DISSERTATION

INFORMATIONELLE SELBSTBESTIMMUNG IM KONTEXT BETRIEBLICHER INFORMATIONSSICHERHEIT

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines
Doktors der Sozial- und Wirtschaftswissenschaften
unter der Leitung von

o.Univ. Prof. i.R. DI Dr. Peter Fleissner
E187
Institut für Gestaltungs- und Wirkungsforschung

eingereicht an der Technischen Universität Wien
Fakultät für Informatik

von

Mag. Josef Heinschink
E9101633
Am Anger 6, 2443 Leithaprodersdorf

Wien, am 18. März 2008

Kurzfassung

Seit einigen Jahrzehnten befindet sich die Wirtschaft in einem weltweiten Transformationsprozeß. Die Globalisierung der Märkte und die Internationalisierung der Produktion sind von raschen Veränderungen im Bereich der Informationstechnologie begleitet. Nur diejenigen Unternehmen, die Veränderungen frühzeitig erkennen, sich flexibel anpassen, werden dem weiter zunehmenden Konkurrenzdruck gewachsen sein und auf Dauer bestehen können. Für die Bereitstellung und Nutzung von Informationen sind immer komplexer werdende Informationssysteme erforderlich. Fehlerhafte Informationssysteme führen schnell zu Produktionsausfällen, verzögerter Bearbeitung oder Datenverlust, folglich zu materiellem bzw. immateriellem Schaden. Ein Hauptgrund für die Ausfälle sind Sicherheitsmängel solcher Systeme. Deshalb kommt dem Management der Informationssicherheit eine steigende strategische und operative Bedeutung zu. Informationssicherheitsmanagement dient dazu, mit diversen Bedrohungen und Risiken umzugehen. Um ein entsprechendes Sicherheitsniveau zu erreichen, genügt es nicht mehr, sich mit einzelnen technischen Maßnahmen zufrieden zu geben. Vielmehr ist ein holistischer Ansatz notwendig: Schaffung eines Rahmenwerkes, in dem technische, rechtliche oder organisatorische Maßnahmen aufeinander abgestimmt werden. Durch die Kombination der richtigen Technologien, Prozesse und Maßnahmen lässt sich eine robuste Infrastruktur aufbauen, die flexibel anpassbar ist und gleichzeitig unter dem Höchstmaß an Informationssicherheit für einen weitgehend unterbrechungsfreien Geschäftsbetrieb sorgt.

Die Vielfalt der Datenverarbeitung führt zu einer sprunghaften Zunahme von personenbezogenen Daten mit hoher Aussagekraft. Sie erlauben, individuelles Verhalten ebenso detailliert nachzuvollziehen wie kollektive Lebensstrukturen. Treibende Faktoren sind vor allem der steigende Einsatz von Internettechnologien in allen Lebensbereichen und die allgegenwärtige Datenverarbeitung. Wenn Datenverarbeitung so funktioniert wie sie soll, agiert sie immer auch als Überwachungstechnologie. Die technischen Konzepte sind entwickelt und es existieren eine Reihe von Services und Tools, die den Kunden eine anonyme bzw. pseudonyme Nutzung ermöglichen oder sie vor unbemerkten Datensammlungen bewahren können. Unter der Voraussetzung eines bestmöglich geschützten Privatbereichs soll dem Benutzer die Hoheit über seine Daten gegeben werden. Dazu notwendig sind *freiheitsfördernde* Architekturen der Informationstechnik, die die Zusammenführung personalisierbarer Daten durch „informationelle Gewaltenteilung“ verhindern.

Identitätsmanagementsysteme stellen solche Architekturen dar. Sie zielen darauf ab, eine einheitliche, systemübergreifende Plattform für die Verwaltung von Benutzern, deren Konten und deren Berechtigungen zu schaffen. Zum einen wird die Entwicklung eines Identitätsmanagementsystem im Kontext von Informationssicherheit dargestellt, zum anderen Ansätze aufgezeigt, wie es Mitarbeitern in Betrieben damit ermöglicht werden kann, ihren Anspruch auf Privatheit zu wahren. Die Möglichkeit zur informationellen Selbstbestimmung muss in einer immer stärker durch Informationstechnologien geprägten Umwelt gewahrt und gestärkt werden.

Motivation

Der Autor dieser Dissertation ist in einem Unternehmen mit mehr als 1000 Benutzern seit 2004 mitverantwortlich für die Planung und Umsetzung eines umfassenden Informationssicherheitsmangementsystems. Eine der dabei zu bewältigenden Herausforderungen besteht in der Realisierung einer unternehmensübergreifenden Zusammenarbeit via Webportal. Dabei soll den Mitarbeitern eine immer größer werdende Anzahl an externen Anwendungen von verschiedenen Institutionen auf Webbasis zur Verfügung gestellt werden. Da die dabei transportierten Daten personenbezogen sind, ist eine entsprechende Sicherheitsinfrastruktur notwendig. Dazu gehört ein Berechtigungskonzept, welches den hausinternen und den externen Anforderungen entspricht. Es existieren viele verschiedene Berechtigungsparameter für viele User mit unterschiedlichen Rechten. Deren Verwaltung hat mit höchster Sorgfalt zu erfolgen. Zudem ist es wichtig, dass alle vom Benutzer getätigten Aktivitäten nachvollziehbar dokumentiert werden.

Die Umsetzung erfolgt in zwei Schritten: Als Basis dient ein derzeit im Aufbau befindliches „Portalverbundsystem“, das den sicheren Austausch von Daten und Berechtigungen zwischen zwei oder mehreren Organisationen ermöglicht. Auf dieser Grundlage soll durch organisatorische und technische Erweiterungen ein holistisches Identitätsmanagementsystem entstehen. Bestrebung ist, ein System zu etablieren, dass neben dem Nutzen für Mitarbeiter und Unternehmen den Aspekt der informationellen Selbstbestimmung für den Anwender in den Vordergrund stellt.

Viele der Erfahrungen aus der täglichen Arbeit des Autors fließen in die Ausführungen mit ein.

Aufbau und Struktur der Arbeit

Die Arbeit besteht aus drei Teilen: Der Rahmen und die Basis werden im ersten Kapitel mit der Abhandlung des Metathemas „Informationssicherheit“ gelegt. Im zweiten Abschnitt wird der Bereich „Digitale Identität und Privacy“ abgeklärt und erläutert, der dritte Teil geht auf den Kern der Überlegungen ein, den Umgang mit Identitäten in Form eines strukturierten „Identitätsmanagements“.

Das sehr breite Thema Informationssicherheit wird mit dem Fokus auf Identitätsmanagement aufgearbeitet. Jene Bereiche, die besondere Relevanz für das Hauptthema haben, werden vertiefend abgehandelt. Der Schwerpunkt liegt auf der betrieblichen Sichtweise. Neben der Datensicherheit ist der Datenschutz elementarer Aspekt einer digitalen Identität. Informationssicherheitsmanagement unter Berücksichtigung von Datenschutzvorgaben ist das Fundament für den Betrieb eines Identitätsmanagementsystems.

Die theoretischen Ausführungen werden mit Beispielen aus der Praxis untermauert. Den dynamischen Entwicklungen und Veränderungen wurde insofern Rechnung getragen werden, dass neu gewonnene Erkenntnisse und Erfahrungen laufend eingearbeitet wurden.

Danksagung

Mein besonderer Dank gilt Herrn Prof. Dr. Peter Fleissner, der diese Arbeit von Anfang an unterstützt und durch eine Vielzahl konstruktiver Anregungen maßgeblich zur ihrem Gelingen beigetragen hat.
Bedanken möchte ich mich bei Studienkollegen und Arbeitskollegen, besonders bei Dipl. Ing (FH) Dragan Simic, MSc, für ihre unzähligen Kommentare und inhaltlichen Beiträge.
Nicht zuletzt danke ich meinen Eltern für ihre Unterstützung und meinen Schwiegereltern für ihre Hilfe und das Korrekturlesen der Dissertation.
Besonders danke ich meiner Frau Sonja und meinen Töchtern Miriam und Hannah, ohne ihren vorbehaltlosen Rückhalt und ihre Geduld wäre diese Arbeit nicht möglich gewesen.

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

Lesehinweis:

Um eine bessere Lesbarkeit zu gewährleisten, wurde auf eine geschlechtsspezifische Differenzierung verzichtet. Entsprechende Begriffe wie beispielsweise Benutzer oder Mitarbeiter gelten im Sinne der Gleichbehandlung stets für beide Geschlechter.

1 INFORMATIONSSICHERHEIT IM PRIVATEN UND BETRIEBLICHEN UMFELD

1.1 PROBLEMSTELLUNG UND HERAUSFORDERUNG

Schon bisher hat das Internet starken Einfluss auf unser Leben genommen, dennoch stehen wir erst am Beginn tiefgreifender Veränderungen. „*Das immer mehr eine universale, digitale Sprache sprechende World Wide Web integriert auf globaler Ebene die Produktion und Distribution von Wörtern, Tönen und Bildern unserer Kultur und passt sie zugleich den individuellen Geschmacksrichtungen und Gemütslagen an. Interaktive Computernetzwerke nehmen exponentiell zu, schaffen neue Formen und neue Kanäle der Kommunikation, formen das Leben und werden zugleich durch das Leben geformt*." [Castells, 2003, S 2].

Im Folgenden sollen zum einen die Auswirkungen des Internets auf die Gesellschaft als Gesamtheit bzw. auf die einzelnen Individuen, zum anderen auf die Unternehmen und Mitarbeiter dargestellt werden. Durch das Internet entstehen neue Formen der Informationsbeschaffung, der Kommunikation und der sozialen Interaktion. Arbeitsabläufe verändern sich, die Arbeit wird mobil, Lernmöglichkeiten werden revolutioniert, wobei vieles, das in der Vergangenheit physische Anwesenheit verlangt hat, durch Virtualität abgelöst wird (z. B.: Bankbesuche, Einkäufe, Reisebuchungen, Behördenwege).

In den letzten Jahren haben sich die Volkswirtschaften der Industrieländer stark gewandelt. Die Liberalisierung der Telekommunikationsmärkte, das rasante Wachstum des Internets und die zunehmende Vernetzung von Wirtschaft und Gesellschaft führten zur sogenannten *Informationsgesellschaft*[1]. Es gibt eine Fülle von Ansätzen, die die Veränderungen der modernen Gesellschaft beschreiben. Ob für die informationstechnologische Revolution der Begriff *Informationszeitalter*, *Wissensgesellschaft*, *Netzwerkgesellschaft* oder eben Informationsgesellschaft verwendet wird, ist eine Frage des persönlichen Geschmacks. *Castells* [Castells, 2003, S 22] bevorzugt den Terminus Informationszeitalter, weil er die verschiedenen Aspekte und Effekte dieser neuen Technologien weitgehend einbezieht. Unstrittig ist jedoch, dass sich die Industriegesellschaft in einem dynamischen Transformationsprozess befindet, der sich insbesondere durch den sprunghaften Anstieg des Einsatzes von Informations- und Kommunikationstechnologien (kurz: IKT) für die Gewinnung, Speicherung, Verarbeitung, Vermittlung, Verbreitung und Nutzung von Informationen manifestiert[2].

„*Die informationelle Wirtschaft ist global.* […] *Eine globale Wirtschaft hat die Fähigkeit, als Einheit in Echtzeit oder gewählter Zeit auf globaler Ebene zu funktionieren. Die notwendige Grundlage dafür ist die neue Infrastruktur, die durch die Informations- und Kommunikationstechnologien bereitgestellt wird. Die Informationstechnik stellt die Infrastruktur für die voranschreitende Globalisierung dar*." [Castells, 2003, S 208f]. Castells Schlussfolgerung ist, dass das Zusammenspiel von Globalisierung, Informationstechnologie und Netzwerktopologie eine neue Gesellschaftsstruktur ergibt, die global

[1] Vgl. http://ec.europa.eu/information_society/index_de.htm [21. März 2007]

funktioniert und auf der Basis von Informatiksystemen weit gehend um ein Netzwerk globaler Finanzströme strukturiert ist [Rolf, 2003, S 7].

Gleichzeitig bedeuten diese Entwicklungen, dass diejenigen, die keinen oder nur begrenzten Zugang zum Internet haben oder die es nicht richtig nutzen können, marginalisiert werden. „*Es kann daher nicht überraschen, dass die Lobeshymnen auf die Möglichkeiten des Internet als Mittel von Freiheit, Produktivität und Kommunikation Hand in Hand mit den Klagen über die „Digital Divide" gehen, jene Trennlinie, zu der es durch die Ungleichheit im Internet gekommen ist.*" [Castells, 2005, S 261].

Die wesentlichsten Chancen dieser Entwicklungen sind[3]:

- ökonomischer Mehrwert durch Schaffung von neuen Berufen und Märkten,
- ökologischer Mehrwert durch elektronischen Transport der Ware „Information",
- Überwindung des Stadt-Land-Gefälles durch elektronische Anbindung der Randregionen an die Zentren,
- globaler Informations- und Wissenstransfer erhöht Potenzial für innovative Lösungen.

Es gibt jedoch auch mögliche Risiken zu bedenken, um entsprechend und effizient gegensteuern zu können:

- unterschiedliche Partizipationschancen für den Einzelnen auf Grund sozioökonomischer und soziokultureller Barrieren (*Digital Divide*),
- Produktionsverlagerung in Billiglohnländer (Verlust von Arbeitsplätzen),
- Gesellschaftliche Konflikte durch Neuorganisation der Produktionsbedingungen (Folgen von Flexibilität, Mobilität etc.),
- Ablehnung neuer elektronischer Dienste durch Konsumenten,
- Verletzung von Persönlichkeits- und Datenschutzrechten.

Die zentrale Basis, die es erlaubt, die Vorteile aus der Nutzung des Internets lukrieren zu können, ist die Verfügbarkeit des Internets und das Vorhandensein entsprechend schneller Verbindungen. Zum einen ist die Verfügbarkeit in den westlichen Ländern bereits hoch, die Tendenz weiterhin steigend – vor allem beim Breitbandzugang [Wirtz, Burda, Beaujean, 2006, S 44ff]. Die technologischen Entwicklungen im *World Wide Web* (kurz: *WWW*) verändern die Art und Weise, mit der digitale Inhalte erzeugt und konsumiert werden. Die Daten[4] des *World Internet Usage Statistics*-Instituts zeigen im Dezember 2007 71 Prozent der Einwohner Nordamerikas als Internetbenutzer, 57 Prozent

[2] Vgl. http://www.bundeskanzleramt.at/site/4544/default.aspx [21. März 2007]
[3] Vgl. http://www.bundeskanzleramt.at/site/4544/default.aspx [21. März 2007];
http://www.politik-digital.de/edemocracy/wissensgesellschaft/nik1.shtml [24. März 2007]
[4] Vgl. http://www.internetworldstats.com/stats.htm [18. Feber 2008]

für Australien und 55 Prozent für die Europäische Union. Laut *Austrian Internet Monitor*[5] (Q3/2007) haben sechs von zehn Österreichern Internetzugang. Zum anderen explodiert das inhaltliche Angebot: die Internettelefonie (*Skype*[6], *Jajah*[7]) feiert einen Siegeszug, der Download von Musik, Filmen und TV-Sendungen ist im Trend und verändert aller Voraussicht nach auf Sicht das Fernsehverhalten und den Werbemarkt. Onlinebanking, Onlineversandhäuser wie *Amazon*[8], Internetauktionshäuser wie *eBay*[9] oder Wettplattformen wie *bwin*[10] sind bei vielen Benutzern (engl. *User*) in Verwendung und erfreuen sich immer größerer Beliebtheit. Internettagebücher (*Blogs*[11]), Foto-Alben wie *Flickr*[12], Musiktauschbörsen wie *Napster*[13], Partnerbörsen, die offene Enzyklopädie *Wikipedia*[14] oder Webplattformen wie *MySpace*[15], *43things*[16] oder *SecondLife*[17] machen das Internet zu einem von Menschen viel benutzten, belebten sozialen Raum. Das alles läßt die *reale* Gesellschaft immer mehr mit der virtuellen Gesellschaft zusammenfließen. Durch das Internet entsteht eine Netzkultur, in der sich Gleichgesinnte in sogenannten *Communities* treffen. Örtliche Begrenzungen werden aufgehoben, so dass Menschen auf der ganzen Welt miteinander kommunizieren und interagieren können. SecondLife (kurz: *SL*) ist ein Beispiel für das Voranschreiten dieser Entwicklungen. Mehr als vier Millionen Menschen weltweit sind bereits virtuelle Bewohner der Online-Welt, bauen sich quasi ein *zweites Leben* auf. Unternehmen eröffnen in SL Büros, verkaufen virtuelle Immobilien oder Waren für virtuelle Menschen, sogenannte *Avatare*[18]. Neben Privatpersonen und Firmen nutzen zunehmend mehr öffentliche Einrichtungen (die Österreich- Repräsentanz im SL ist unter „Erlebniswelt Austria“[19] zu finden) die Plattform für den Aufbau neuer, virtueller Standorte.

Eine Konsequenz aus der Verlagerung realer Handlungen in die *Cyberwelt* ist die Veränderung der Marktmacht. Das Einkaufsverhalten im Internet steht unter einem immer stärker werdenden Einfluss der *Social Networking*-Plattformen. Eine Studie[20] des Marktforschungsunternehmens *Fittkau und Maaß* zeigt, dass die Anwender dort immer mehr Informationen und Bewertungen einzelner Produkte austauschen. Für die Webshopbetreiber bzw. Produzenten und Hersteller bergen diese Entwicklungen

[5] Vgl. http://mediaresearch.orf.at/index2.htm?internet/internet_aim.htm [18. Feber 2008]; http://www.integral.co.at/AIM/business.shtml [17. März 2008]
[6] http://www.skype.com/ [27. Feber 2007]
[7] http://www.jajah.com/ [28. Feber 2007]
[8] http://www.amazon.com/ [27. Feber 2007]
[9] http://www.ebay.com/ [27. Feber 2007]
[10] https://www.bwin.com/ [27. Feber 2007]
[11] Blog oder Weblog (Kunstwort aus Web und Log) ist eine Webseite, die periodisch mit neuen Einträgen versehen wird. Neue Daten stehen an oberster Stelle, ältere folgen in umgekehrt chronologischer Reihenfolge.
[12] http://www.flickr.com/ [27. Feber 2007]
[13] http://www.napster.com/ [27. Feber 2007]
[14] http://www.wikipedia.org/ [27. Feber 2007]
[15] http://www.myspace.com/ [27. Feber 2007]
[16] http://www.43things.com/ [14. Mai 2007]
[17] http://www.secondlife.com/ [11. März 2008]
[18] Ein Avatar ist ein künstlicher Stellvertreter einer realen Person in der virtuellen Welt.
[19] Vgl. http://www.diepresse.at/home/techscience/internet/109069/index.do [20. März 2007]
[20] Vgl. http://www.fittkaumaass.de/ W3B-Studie Jänner 2007 [20. März 2007]

neue Risiken. Es kann passieren, dass eine Marke auf diese Weise in Verruf gerät. Zudem ist es für die Unternehmen schwierig, den Überblick über die Meinungsbildungsprozesse zu bewahren.

Eine zunehmend wichtigere öffentliche Funktion übernimmt der Online-Journalismus (respektive Bürgerjournalismus, engl. *Citizen Journalism*). Das kann beispielsweise beim Wahlkampf für die Präsidentenwahl 2008 in den USA beobachtet werden[21]. Ein Kandidat hatte in einem Gespräch im kleinen Rahmen während eines Vorwahlkampfes einen ausländischen Mitarbeiter eines Konkurrenten mit einem herabsetzenden Schimpfwort bedacht. Das Gespräch wurde per Handy aufgezeichnet und anschließend auf *YouTube*[22] online gestellt. Aufgrund des populären Mediums erreichte diese Aussage Millionen von Menschen und löste so einen Sturm der Entrüstung aus, wodurch die Kandidatur vereitelt wurde. Alle Anwärter auf das Präsidentenamt gaben ihre Kandidatur zuerst im Internet bekannt. Sämtliche Auftritte, Presseaussendungen, Mobilisierungsbotschaften und Spendenaufrufe werden – mit strategischer Streuung – auf populären Online-Plattformen verteilt. Bürger publizieren und nutzen diese öffentlichen Foren zur aktiven oder passiven Meinungsbildung.

Dieses Beispiel, wie auch die verstärkte Zunahme der politischen Diskussion auf diversen Internetseiten[23], zeigt die Veränderung der Beziehung zwischen Politik und Bürger (*E-Democracy*[24]).

Beim alljährlich stattfindenden *Weltwirtschaftsgipfel*[25] im schweizerischen Davos wurden unter dem Titel „*The Shifting Power Equation*“ Machtverschiebungen diskutiert. Zum einen wurde für die traditionelle Geschäftswelt konstatiert, dass sich aufgrund der digitalen Revolution die Macht von den Produzenten hin zu den Konsumenten verschiebt. Zum anderen wurde festgehalten, dass die Staatsmacht zugunsten der Nichtregierungsorganisationen, aber auch der einfachen Staatsbürger und Web-User an Einfluss verliert.

Neben den gesellschaftlichen Folgen erwachsen aus dem steigenden Internetgebrauch für die Individuen neue soziale wie technische Gefahren. In der Literatur sind etliche Abhandlungen[26] zu den psychischen und sozialen Folgen der Vernetzung (Veränderungen der sozialen Beziehungen, der interpersonalen Kommunikationsprozesse, der Identität) – meist unter dem Aspekt der Bedrohung (Pornographie, Internetsucht, Verbreitung rassistischen Gedankenguts) – zu finden.

War es bis vor einiger Zeit noch ausreichend, seinen PC vor Viren zu schützen, ist es nunmehr zwingend notwendig, eine Personal Firewall einzusetzen und das Betriebssystem laufend zu aktualisieren, um Schwachstellen und damit potenzielle unerwünschte Zutrittsmöglichkeiten zu

[21] Vgl. http://www.techpresident.com/ [21. März 2007]
[22] http://www.youtube.com/ [21. März 2007]
[23] Vgl. http://www.wahlkampf-digital.de/ [21. März 2007];
http://www.politik-digital.de/metablocker/plugin/tag/Online+Wahlkampf [21. März 2007];
http://www.politicsonline.com/ [21. März 2007]
[24] Vgl. http://www.e-democracy.org/ [21. März 2007];
http://www.exine.de/netlife/e-democracy.htm [21. März 2007]
[25] Vgl. http://www.weforum.org/en/index.htm [14. März 2007]
[26] Vgl. http://gin.uibk.ac.at/thema/internetsucht/internetsucht.html [21. März 2007];
http://www.psychohelp.at/html4/psychologie_nachrichten/internet/internetsucht.shtml [21. März 2007]

vermeiden. Der sorgsame Umgang mit Zugangsdaten (Benutzernamen, Kennwörter etc.) für Onlinedienste zur Vermeidung von Missbrauch durch Dritte, als gängigstes Beispiel kann hier Onlinebanking (siehe *1.4.1.2 Exkurs: Phishing*) angeführt werden, ist unabdingbar.

Im betrieblichen Umfeld hängt in vielen Bereichen der Unternehmenserfolg vom Funktionieren der Informationstechnologie ab. Die IT tritt nicht mehr nur unterstützend auf, vielmehr werden Geschäftsprozesse digital abgebildet und automatisiert abgewickelt. Längst haben *Enterprise Ressource Planning (*kurz: *ERP)*- oder *Customer Relationship Management* (kurz: *CRM*)-Systeme und eben Internetapplikationen den herkömmlichen IT-Services wie E-Mail, Printing, Filesharing den Rang abgelaufen. Gerade durch die Internetanwendungen öffnen sich die Unternehmen nach außen. Durch *E-Business* oder *E-Government* erhält der Kunde, Partner bzw. Bürger zu einer bislang in sich geschlossenen Umgebung Zugang. Es erfolgt Kommunikation und Interaktion auf informationstechnischem Weg vom und zum Unternehmen. Zudem hat der Einzug des sogenannten *Web 2.0*[27] in Unternehmensnetzwerken Auswirkungen auf den Umgang mit Wissen. Während früher die Mitarbeiter ihr Wissen in statischen Datenbanken abgelegt haben, geht der Trend durch die neuen Social Networking-Werkzeuge in Richtung Informationsbereitstellung und aktivem Wissensaustausch [Bitkom, 2006-2, S 19f]. Technologien wie *Instant Messaging*[28], Web-Konferenzen, Blogs, *Podcasting*[29] oder *Wikis*[30] erleichtern das Ziel, sämtliche Daten und Informationen sowie das gesamte Wissen, das die Mitarbeiter für die Erledigung ihrer Aufgaben benötigen, verfügbar zu machen. Durch die genannten Web 2.0-Technologien werden die virtuelle Zusammenarbeit, der Austausch und die Generierung von Wissen enorm erleichtert.

Die Anforderungen an die Informationssicherheit sind im unternehmerischen Umfeld ungleich höher als im privaten. Genügt es im Haushalt, einen entsprechenden Schutz des PCs zu gewährleisten, bedarf der Schutz der Information im Betrieb eines ganzheitlichen Ansatzes (siehe *1.2 Grundlagen der Informationssicherheit* und *1.8 Unternehmenssicherheit*). Durch die erhöhten Sicherheitsanforderungen und durch die vermehrte Teilnahme am Social Networking kann es innerhalb der Unternehmen zu einer verminderten Arbeitsproduktivität kommen. Zudem werden IT-Systeme und vertrauliche Daten potenziellen Risiken ausgesetzt.

„*Digitalisierung bedeutet für die Ökonomie der Jahrtausendwende zweierlei: eine Rationalisierung der industriellen Produktion und der Arbeitsprozesse im Dienstleistungssektor, für dessen auffälliges Expandieren Computer als wichtiger Faktor gelten*.“ [Betz, Riegler, 2003, S 97]. Der Arbeitsablauf

[27] Web 2.0 ist ein inzwischen etablierter Oberbegriff für die Beschreibung einer Reihe neuer interaktiver Techniken und Dienste des Internets und seiner veränderten Wahrnehmung. Hauptaspekt ist, dass die Benutzer Inhalte selbst erstellen und/oder bearbeiten.

[28] Instant Messaging (kurz: IM) ist ein Dienst, der es ermöglicht, mittels einer Software in Echtzeit mit anderen Teilnehmern zu kommunizieren (engl. chatten).

[29] Podcasting bezeichnet das Produzieren und Anbieten von Audio- oder Videodateien über das Internet.

[30] Ein Wiki ist eine im Internet frei verfügbare Seitensammlung, die von jedem Benutzer nicht nur gelesen, sondern auch online geändert werden kann.

für die Mitarbeiter hat sich demnach durch den Einsatz von Informationstechnologie und Internet verändert. Der Umgang mit der Informationstechnik wird künftig noch stärker zum Rüstzeug fast jeder Tätigkeit gehören. Das hat zur Folge, dass auch immer mehr einfache Arbeiten gute IT-Kenntnisse erfordern [Scheer, 2007, S 19]. Neben einem steigenden Grad an Automatisierung wächst die Mobilität der Mitarbeiter. Sie arbeiten von verschiedenen Arbeitsplätzen aus, von zu Hause oder vom Kunden, Telearbeit nimmt zu (siehe *1.5.1 Arbeitsplatz der Zukunft*).

„*Gleichzeitig verstärken die Potenziale telematischer Vernetzung marktradikale Tendenzen: Als Kontrolltechnologie erlauben Computer verstärkt eine individuelle Feststellung von Arbeitsleistung, was die betriebsinterne Konkurrenz steigert und Formen impliziter Solidarität zwischen Arbeitenden unterschiedlichen Leistungsniveaus schwächt*." [Betz, Riegler, 2003, S 97]. Der Mitarbeiter braucht eine Handhabe, um den Zugriff auf seine Daten kontrollieren zu können. Die Handlungsmöglichkeiten der IT-Abteilung, des Vorgesetzten oder der Personalabteilung, ein vollständiges Mitarbeiterbild (Arbeitszeitkontrolle, Internetsurfverhalten, E-Mail-Kommunikation etc.) generieren zu können, sollen eingeschränkt werden. Solche Systeme sollen nur jene Informationen preisgeben, die vom Benutzer selbst freigegeben werden. Ziel ist es, einen möglichst hohen Grad an „informationeller Selbstbestimmung" (siehe *2.3.2.1 Informationelle Selbstbestimmung*) zu erreichen.

Der Schutz des Benutzers und seiner Daten ist daher für die fortschreitende Nutzung, *Humanisierung des Internets*[31] und Vernetzung der Geschäftswelt unerlässlich.

1.2 GRUNDLAGEN DER INFORMATIONSSICHERHEIT

Informationssicherheit (engl. *Information Security*, oft auch nur *Security*) hat zum Ziel, die Verarbeitung, Speicherung und Kommunikation von Informationen so zu gestalten, dass Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit in ausreichendem Maß sichergestellt werden. Personen, deren Wissen, Daten und Infrastruktur sollen vor Bedrohungen und Gefahren geschützt, Schäden vermieden und Risiken minimiert werden. Zudem sind gesetzliche Auflagen über den Datenschutz zur Wahrung von Persönlichkeitsrechten einzuhalten.

1.2.1 INFORMATION UND INFORMATIONSSICHERHEIT

Nach Rehäuser und Krcmar [Rehäuser, Krcmar, 1996, S 6] bilden die Zeichen die Elementarebene, die durch eine Syntax zu Daten werden. Daten, deren inhaltliche Bedeutung gegeben ist, bilden Information. Wissen ist die von einer Person internalisierte Information.

[31] Vgl. http://www.zeit.de/2005/35/C-Humannetz [27. Feber 2007]

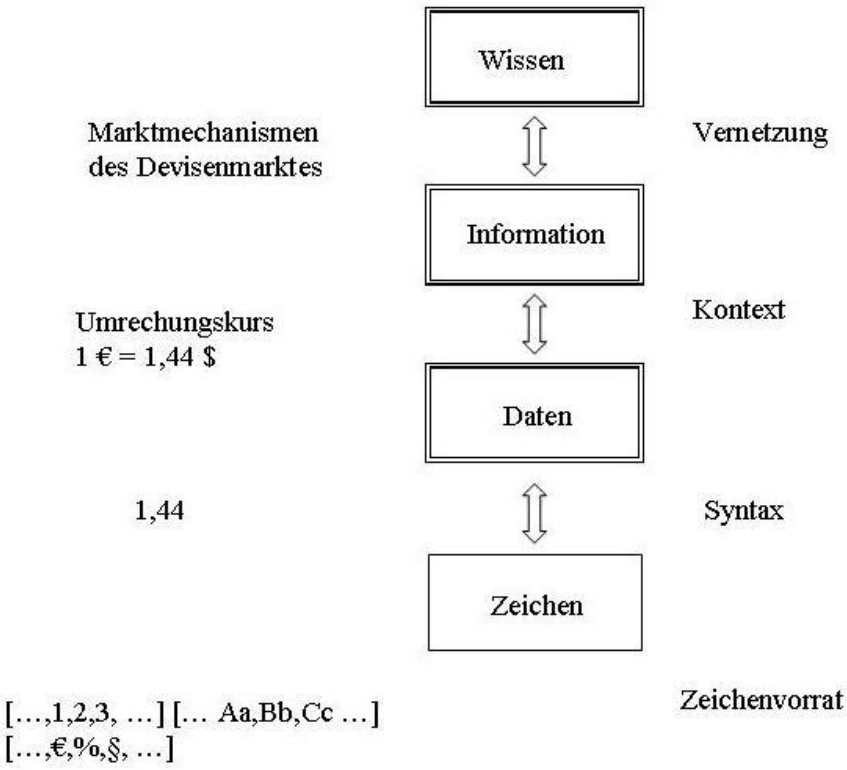


Abbildung 1: Zusammenhang Daten-Information-Wissen

Laut Castells [Castells, 2003, S 17] wird Information als Kommunikation von Wissen definiert. In diesem Sinne wird Information [Holthaus, 2000, S 51ff] als Oberbegriff für Wissen verwendet: betriebliche und private Daten, *Know-how*, Benutzerberechtigungen, Passwörter etc. in analoger und digitaler Form.

Die Diskussion über einen allgemein gültigen Informationsbegriff ist aber bei weitem noch nicht abgeschlossen. In der Literatur hat sich noch kein anerkannter einheitlicher Informationsbegriff durchgesetzt. Übereinstimmung scheint es lediglich darüber zu geben, welche Gebiete dabei involviert sind [Fuchs, Hofkirchner, 2003, S 102]:

- das Gebiet des Erkenntnisgewinns und der Ideenproduktion durch gesellschaftliche Subjekte (Kognition),
- das Gebiet des Austauschs von Erkenntnissen und des Verkehrs gesellschaftlicher Subjekte über Ideen (Kommunikation),
- das Gebiet gemeinsamer Aktionen, zu deren Durchführung die gesellschaftlichen Subjekte Erkenntnisse und Ideen in Einklang bringen müssen (Kooperation).

Der Informationsbegriff kann über die Wissensgebiete hinweg *genau dasselbe*, *nur etwas ähnliches* oder *jeweils etwas ganz anderes* bedeuten („*Capurrosche Trilemma"*). Ein vereinheitlichter Informationsbegriff ist dennoch denkmöglich [Fuchs, Hofkirchner, 2003, S 105 ff].

Information stellt einen Wert dar, den es zu schützen gilt. Die Informationssicherheit (siehe *1.2.2 Anforderungen an die Informationssicherheit*) setzt sich genau das zum Ziel [Holthaus, 2000, S 34], während unter *Safety* die Funktionssicherheit, der Schutz vor Fehlfunktionen verstanden wird. Bei *Privacy* [Windley, 2005, S11] (siehe *2.3 Privacy*) geht es um die Privat- und Intimsphäre, um den Schutz der Daten des Individuums.

Das Bedrohungspotenzial für Informationen ist vielfältig, ständig wachsend und technisch innovativ. Dazu gehören alle Ausprägungen von menschlichem und technischem Versagen, Viren, Spionage, Vandalismus, Diebstahl, aber auch höhere Gewalt wie Blitzschlag, Feuer oder Überschwemmung (siehe *1.3 Taxonomie von Angriffen auf den Wert Information*). Die Computerkriminalität (siehe *1.3.5 Computerkriminalität*) gewinnt bei den Wirtschaftsdelikten immer mehr an Bedeutung.

Private wie öffentliche Unternehmen sind in ihrer Geschäftstätigkeit auf IT-Systeme naturgemäß weit mehr angewiesen als Privatpersonen. Da neben der Abhängigkeit vom Funktionieren der IT auch die Risiken für Betriebe in aller Regel größer sind als für private Haushalte, wird Informationssicherheit – im Sinne eines strukturierten, umfassenden Vorgehens – daher ausschließlich in Unternehmen betrieben (siehe *1.8 Unternehmenssicherheit*). Zudem gibt es entsprechende Verpflichtungen, die sich aus den verschiedenen Bestimmungen und Gesetzen zum Handels-, Gesellschafts-, Haftungs-, Datenschutz-, E-Government-, Verbandsverantwortlichkeits- (in Kraft seit 1.1.2006) oder Bankenrecht ableiten (siehe *1.7.3 Gesetzeslage*). International spielen Vorschriften wie *Basel II*[32], *Sarbanes-Oxley Act*[33] oder *Health Insurance Portability and Accountability Act*, kurz *HIPAA*[34], eine wichtige Rolle (siehe *1.8.4 Informationssicherheitsstandards und -Vorschriften*).

Während im betrieblichen Umfeld die ganze Themenbreite der Informationssicherheit Beachtung findet, gilt für die Privatanwender primär der Schutz vor Viren oder Spyware (siehe *1.7.1.3 Grundsätze im Umgang mit PCs zum Schutz vor Malicious Code*).

Häufig wird Informationssicherheit auf IT-Sicherheit reduziert und damit der technologische Aspekt in den Vordergrund gerückt. Zahlreiche Untersuchungen und Erfahrungen zeigen einerseits die Bedeutung der Technik, andererseits aber auch die häufige Vernachlässigung der organisatorischen, wirtschaftlichen und rechtlichen Aspekte. Generell umfasst Information Security analoge wie digitale Daten ebenso wie den Schutz von Personen und Infrastruktur (Gebäude, technische Anlagen etc.). Informationssicherheit ist aus unternehmerischer Gesamtsicht Teil des Risikomanagements.

[32] http://www.basel-ii.info/ [26. Feber 2008]
[33] http://www.sarbanes-oxley.com/ [26. Feber 2008]
[34] http://www.hipaa.org/ [26. Feber 2008]

Die Quintessenz aus den Ergebnissen der Marktuntersuchungen ist, dass Störfälle, welche die Informationssicherheit betreffen, überdurchschnittlich zunehmen und daher Informationssicherheit zu einem bestimmenden Qualitätsthema in einem Unternehmen geworden ist.

Aus einem Marktreport[35] von *NextiraOne* geht hervor, dass allein im Jahr 2004 weltweit schon rund 700 Millionen Informationssicherheitsvorfälle aufgetreten sind. Weiters erläutert der Report: „*72 Prozent aller Unternehmen und Organisationen in Europa betrachten die Informationssicherheit als Kernthema unter den betrieblichen Prozessen. Das reflektiert nicht nur die Angst vor Schäden und den damit einhergehenden Verlusten, sondern auch die Tatsache, dass die Informationssicherheit eine Leistungskomponente eines Unternehmens und seiner Dienste und Produkte darstellt, bis hin zu einem Unterscheidungsmerkmal vom Wettbewerb. Gerade im Hinblick auf Prozesse, die über Unternehmen verteilt sind, also Outsourcing und unternehmensübergreifende Arbeitsteilung in jeder Form, kommt dem Thema Informationssicherheit eine überragende Bedeutung zu.*"

KPMG[36] untersuchte Ende 2004 die Datensicherheit in österreichischen Betrieben: „[…] *bei 80 Prozent der Unternehmen laufen die Prozesse IT-unterstützt ab. Gleichzeitig sind für 63 Prozent der Befragten die IT-gestützten Unternehmensinformationen streng vertraulich zu behandeln. 56 Prozent der Unternehmen gaben an, dass es zu einer erheblichen Geschäftsunterbrechung kommen würde, wenn auf die Daten nicht zugegriffen werden könnte bzw. Daten nicht mehr vorhanden wären. Eine Manipulation der unternehmensinternen Daten stellt einen drastischen Eingriff in den Geschäftsalltag dar und zieht für knapp ein Drittel der Befragten eine wesentliche Unterbrechung der Geschäftsprozesse nach sich. Entsprechend werten 67 Prozent die Informationssicherheit als hohe Priorität im Unternehmen und Entscheidungen rund um die IT entwickeln sich zunehmend zur Chefsache: Bei 80 Prozent der befragten Unternehmen ist die Geschäftsführung bei strategischen Entscheidungen im Bereich der Informationssicherheit involviert."*

Zusammenfassend kann – quer über alle Branchen hinweg – festgehalten werden, dass die Informationstechnologie zum unabdingbaren Bestandteil für die Durchführung der Geschäfte geworden ist. Die verstärkte Einbindung der Geschäftsführung in Fragen und Entscheidungen zur Informationssicherheit zeigt das gesteigerte Bewusstsein um die Bedeutung dieser Thematik für den Unternehmenserfolg.

„Das Bewusstsein für Informationssicherheit spiegelt sich aber zu wenig in den intern getroffenen Maßnahmen wider: So sind für rund die Hälfte der befragten Unternehmen Probleme mit Computerviren alltäglich. Mehr als ein Drittel beklagt eine schlechte Anpassungsfähigkeit ihrer Anwendungen an sich ändernde Geschäftsprozesse und Marktbedingungen. Bei 34 Prozent der Unternehmen ist das System zeitweilig nicht verfügbar, damit kann auf wichtige Daten nicht zugegriffen werden. 82 Prozent der Befragten haben darüber hinaus angegeben, dass sie über kein

[35] Vgl. http://www.nextiraone.de/ „Störfälle bei der IT-Sicherheit nehmen zu" [27. Feber 2007]

Kontrollsystem bzw. Intrusion Detection System verfügen, welches interne Datenbewegungen dokumentiert."

Dem Risiko von Funktionsstörung und Datenverlust wird in vielen heimischen Unternehmen trotz verstärkter Maßnahmen in den letzten Jahren noch immer zu wenig entgegen gewirkt (Anm.: Dieser Umstand zeigt sich auch international. Laut dem „*Global Security Survey 2007*"[37] haben nur 63 Prozent der Befragten eine Strategie für Informationssicherheit). Obwohl die Notwendigkeit erkannt wird, gibt es auf Grund zu geringer Budgets Mängel im Management der Informationssicherheit. *„Zwei Drittel der Unternehmen verwenden weniger als zwei Prozent ihres Umsatzes für die IT, davon 42 Prozent sogar nur bis zu einem Prozent. Im internationalen Vergleich liegt man damit weit unter dem Durchschnitt. Gartner*[38] *weist in der Studie „IT Spending and Staffing Survey 2003" den durchschnittlichen Anteil der IT-Kosten am Umsatz mit 2,79 Prozent aus.*"

Unternehmen setzen meist auf kurzfristige Maßnahmen, obwohl Erfahrungen zeigen, dass es wirtschaftlicher ist, in Konzepte und Systeme mit längerfristigem Nutzen zu investieren. *„*[…] *für viele Unternehmen (43 Prozent) die Kosten-Nutzen-Aspekte nicht transparent sind. Hohe Komplexität und fehlende Entscheidungshilfen sind weitere Gründe, warum Sicherheitsrisiken nicht erkannt oder einfach verkannt werden. Die Konsequenz daraus ist, dass die eingesetzten Maßnahmen nicht entsprechend auf die Erfordernisse abgestimmt sind."*

Die Empfehlung von KPMG lautet: *„Der erste Schritt zu einem professionellen Risikomanagement im Bereich Informationssicherheit ist daher die Festlegung von klaren, systematischen Vorgaben hinsichtlich der Geschäftsprozesse und ihrer methodischen Umsetzung im Unternehmensalltag. Erst dann können sinnvoll maßgeschneiderte Sicherheitsmaßnahmen getroffen werden. Effizientes Sicherheitsmanagement ist vor allem auch ein kontinuierlicher Prozess: die Strategien und Konzepte in der Informations- und Kommunikationstechnologie sind hinsichtlich ihrer Leistungsfähigkeit und Wirksamkeit ständig zu überprüfen, um Informationssicherheit für die unternehmensinternen Daten auch langfristig zu garantieren.*"

1.2.2 ANFORDERUNGEN AN DIE INFORMATIONSSICHERHEIT

Unternehmen müssen sowohl durch ihr Verhalten (siehe *1.8.3.1.2 Exkurs: Unternehmenskultur*) und ihre Aufbauorganisation als auch durch ihre Prozesse und Infrastruktur sicherstellen, dass die Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit der Informationen sowie der Infrastruktur gewährleistet sind.

Gerade die Vernetzung der Geschäftsprozesse erhöht die Risiken des unbefugten Zugriffs auf – geschäftskritische – Informationen und des Datendiebstahls immens. Das Öffnen bislang

[36] Vgl. http://www.kpmg.at/ „Wie sicher sind die Daten in Österreichs Unternehmen?" [11. März 2008]
[37] Vgl. http://www.deloitte.com/dtt/research/0,1015,cid%253D170582,00.html [11. März 2008]
[38] http://www.gartner.com/ [27. Feber 2007]

abgeschotteter IT-Infrastrukturbereiche gegenüber dem Internet bringt neue Eindringmöglichkeiten trotz hoher Perimetersicherheit[39] (siehe *1.7.2.4 Perimetersicherheit*). Vor allem im E-Business und E-Government ist das Funktionieren von Security deshalb eine wesentliche Säule. Kunden, Bürger und Unternehmen nehmen nur dann am elektronischen Geschäftsverkehr teil, wenn sie darauf vertrauen können, dass die übertragenen und gespeicherten Daten vor Missbrauch geschützt sind.

Ein Unternehmen sollte nicht nur den Zugang und die Kommunikation von und zu externen Personen und Institutionen ermöglichen, sondern ebenso den eigenen Mitarbeitern entsprechende Mobilität gestatten. Es ist in vielen Branchen bereits seit längerem üblich, Inter- und Intranet, E-Mail, Dateien etc. orts- und zeitungebunden zur Verfügung zu stellen. Damit sind auch die entsprechenden Zugangsmöglichkeiten zu den nach außen gerichteten Unternehmensressourcen rein theoretisch für jedermann erreichbar und bilden somit ein Bedrohungspotenzial. Mittels Notebook respektive *Personal Digital Assistant* (kurz: *PDA*) wird über eine meist durch *Virtual Private Network* (kurz: *VPN*) gesicherte Leitung eine Verbindung zum Firmennetzwerk hergestellt.

Innovationen technischer wie organisatorischer Natur stellen laufend neue Anforderungen an die Informationssicherheit. Hinzu kommt die Entwicklung zur Systemheterogenität, indem die unternehmensinterne IT-Infrastruktur nunmehr vielfach auf verteilten Client/Server-Strukturen basiert, die im Gegensatz zur früher dominierenden Zentralrechnerwelt zahlreiche Angriffspunkte beinhalten und entsprechend komplexere Sicherheitsanforderungen haben. Softwareseitig hingegen geht es in Richtung Homogenität: während viele Unternehmen lange Jahre ihre Anwendungen selbst programmiert haben, wird heute zunehmend auf standardisierte Software zurückgegriffen. Damit ist aber auch die Angriffsfläche für *Malware*[40] (siehe *1.3.4 Computer Anomalien/Malicious Code*) enorm gewachsen.

Dies alles sowie gesetzliche und regulative Bestimmungen bedingen verlässliche Sicherheitslösungen für IT-Systeme, Netze, Datenbanken und Anwendungen. Ähnlich anderen Leistungen eines Unternehmens müssen Informationssysteme nicht nur die quantitativen Anforderungen, sondern auch die qualitativen Bedürfnisse ihrer internen Benutzer und externen Kunden befriedigen.

[39] Unter Perimetersicherheit werden die Schutzmaßnahmen (Firewall, Webfilter, Virenscanner etc.) am Übergang zwischen dem Internet und dem Unternehmensnetz verstanden. Ein Beispiel für Perimeterschutz ist die so genannte Demilitarized Zone (kurz: DMZ), die durch Firewallsysteme getrennt von außen und innen erreichbar ist, eine Direktverbindung durch die DMZ ist jedoch nicht möglich.

[40] Unter Malware werden Computerprogramme mit Schadfunktion verstanden;
http://malware.bul-online.de/av_weltkarte.php [12. März 2008];
http://www.cert.org/ [12. März 2008];
http://www.viruslist.com/de/ [12. März 2008]

Im Wesentlichen gibt es vier Sachziele [Österreichisches Sicherheitshandbuch, 2004, S 84ff] [Janowicz, 2006, S 3] [Piller, 2005-1, S 8f], die es zu erreichen gilt:

- Integrität: „Information nicht verändert“
  Unter Integrität wird die Gewährleistung der Unversehrtheit und Korrektheit von Daten verstanden und kann durch *Hash*–Verfahren (siehe *1.7.2.1.4 Hash-Verfahren*) sichergestellt werden.
- Verbindlichkeit: „Kein Abstreiten möglich“
  Hierunter wird Verbindlichkeit im Sinne der Zurechenbarkeit verstanden. Authentizität wird der Verbindlichkeitsanforderung zugerechnet, die etwa durch einen Zeitstempel oder ein Zertifikat (siehe *1.7.2.1.6 Digitale Zertifikate*) erfüllbar ist.
- Verfügbarkeit: „Information wie vereinbart zugänglich“
  Verfügbarkeit bedeutet, dass die Systeme wie die Informationen und Zugänge vereinbarungsgemäß zur Verfügung stehen. Angegeben wird die *Uptime* eines Systems in Prozenten, zum Beispiel bedeuten 99,5 Prozent 44 Stunden Ausfallszeit pro Jahr bei einem 24x7–Ganzjahresbetrieb. Vereinbart wird das Verfügbarkeitsniveau typischerweise in *Service Level Agreements* (kurz: *SLA*’s). Erreicht wird Verfügbarkeit durch redundante Systeme: Cluster, Ausfallsrechenzentrum und dgl. (siehe *1.3.2.2 Gegenmaßnahmen*).
- Vertraulichkeit: „Information in den *richtigen* Händen“
  Unter Vertraulichkeit ist die Sicherstellung des Zugangs zu Informationen nur für Berechtigte zu verstehen. Verschlüsselung (siehe *1.7.2.1 Kryptologie*) ist ein geeigneter Weg, diese Eigenschaft zu erfüllen.

Weitere Ziele bzw. Subziele sind:

- Abrechenbarkeit: „Protokollieren“
  Umgesetzt durch Protokollierung und Logging.
- Anonymität (siehe *2.2.3 Anonymität*): „Information keiner Person zuordenbar“
  Realisierbar durch Proxytechniken und Remailersysteme (siehe *2.4 Maßnahmen zum Schutz der Privacy*).
- Authentizität (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*): „Information der *richtigen* Person zuordenbar“
  Technisch ermöglicht werden kann das durch die digitale Signatur (siehe *1.7.2.1.7 Elektronische Signatur*).
- Pseudonymität (siehe *2.2.2 Pseudonymität*): „Information keiner Person direkt zuordenbar“
  Eine Möglichkeit ist die Verwendung von *Nicknames*.

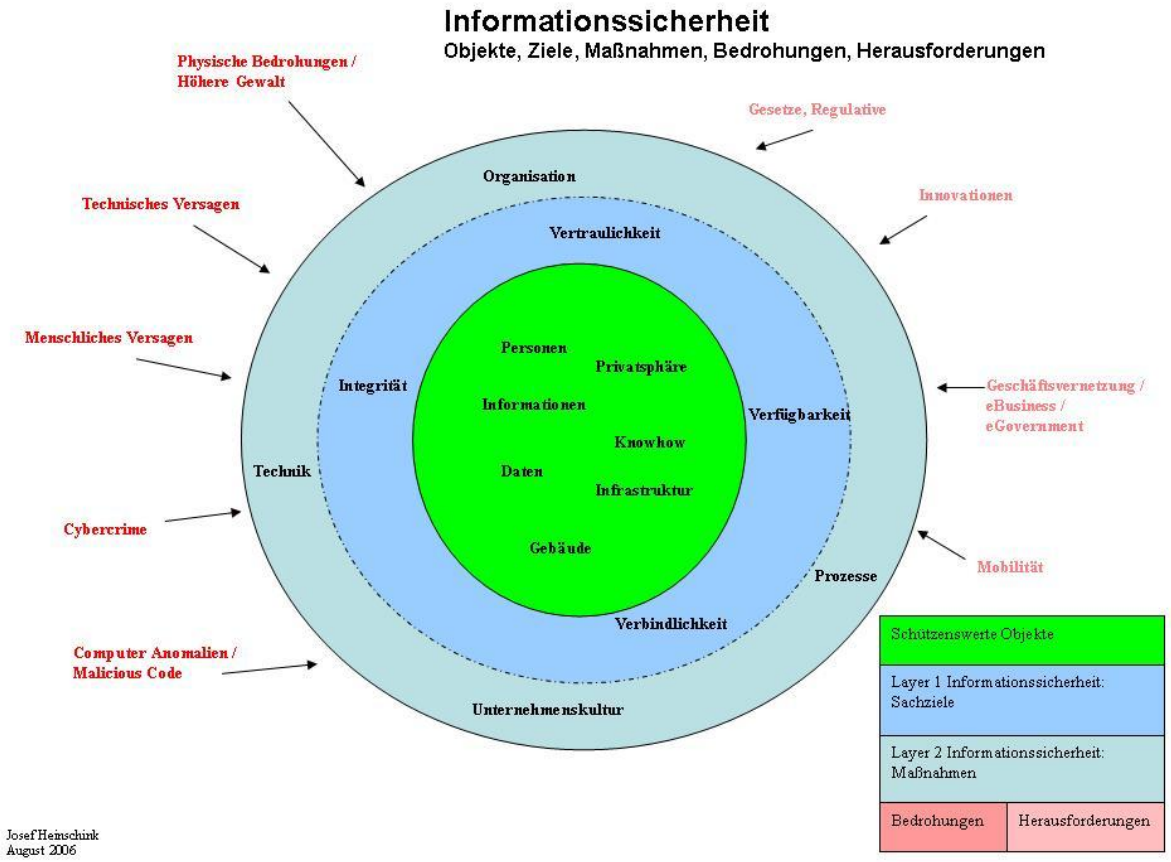


Abbildung 2: Objekt, Ziele, Maßnahmen und Herausforderungen der Informationssicherheit

1.3 TAXONOMIE VON ANGRIFFEN AUF DEN WERT INFORMATION

Eine häufig vorgenommene Unterscheidung der Bedrohungen ist deren Ausgangspunkt. Dabei wird in Organisationen zwischen internen Bedrohungen und externen Bedrohungen unterschieden.

Weitere Unterteilungen gelten sowohl für interne wie externe Bedrohungen: höhere Gewalt (z. B.: Feuer, Hochwasser), Bedrohungen technischen (z. B.: Hardwarefehler, Problem bei Internet Service Provider) und menschlichen Ursprungs (z. B.: Anwenderfehler, Hacker). Einer Studie der *Steria Mummert Consulting AG*[41] zufolge werden 60 Prozent aller deutschen Unternehmen angegriffen, davon kommen zwei Drittel der Angriffe aus dem eigenen Unternehmen; 85 Prozent der Unternehmen haben Erfahrung mit Datenverlust. Das US-Marktforschungsinstituts *ICM Research* hat in einer Studie[42] (Juli 2007) erhoben, dass pro Woche neun vertrauliche Dokumente deutsche Büros auf tragbaren Geräten verlassen. Etwa 19 Prozent der befragten Mitarbeiter gaben an, regelmäßig

[41] http://www.steria-mummert.de/ „Angriff auf IT-Sicherheit: Störfälle nehmen zu“ Oktober 2005 [27. Feber 2007]
[42] http://www.securitymanager.de/magazin/artikel_1484_computerforensik.html [11. März 2008]

Unternehmensdaten mit Dritten auszutauschen. IDC[43] stellt in der Untersuchung „*Worldwide Outbound Content Compliance 2005-2009 Forecast and Analysis: IT-Security Turns Inside Out"* fest, dass für die befragten IT-Verantwortlichen in den kommenden Jahren eine ihrer dringendsten Herausforderungen darin besteht, ihre Mitarbeiter anzuhalten, die firmeninternen Sicherheitsrichtlinien zu befolgen. Folglich stellt der Faktor Anwender per se eine der größten Sicherheitsgefahren für ein Unternehmen dar (siehe *1.8.3 Der Faktor Mensch*).

1.3.1 PHYSISCHE BEDROHUNGEN/HÖHERE GEWALT

1.3.1.1 Problembeschreibung

Katastrophen lassen sich in natürliche (wie Feuer, Blitz, Überschwemmung oder Erdbeben) und nicht-natürliche Bedrohungen (wie Flugzeugabsturz, Bombenanschlag, Einbruch, Stromausfall oder Sabotage) unterteilen.
Katastrophen und physische Störungen größeren Ausmaßes können zur Nichtverfügbarkeit von ganzen IT-Systemen und zum kompletten Datenverlust führen. Beispiele in jüngster Vergangenheit gibt es national wie international allein durch Hochwasserschäden zur Genüge. Bestehen keine Notfall- und Wiederanlaufpläne, kann das – in vielen Branchen im *worst case* – Existenz bedrohend sein. *Business Continuity Management* soll ein strukturiertes, effizientes Vorgehen im Krisenfall gewährleisten. Es beinhaltet einen *Disaster Recovery*-Plan ebenso wie die Einbindung und Integration des Business, sprich der Fachabteilungen.

1.3.1.2 Gegenmaßnahmen

Zur Sicherung der Verfügbarkeit müssen sowohl organisatorische, personelle, technische als auch bauliche Maßnahmen getroffen werden. Konkret bedeutet das Redundanz im Personal-, Daten- und Infrastrukturbereich. Aus wirtschaftlicher Sicht ist festzuhalten, dass fehlertolerante, redundante Systeme an verschiedenen Standorten einen enormen Kostenfaktor darstellen. Es ist daher für viele Betriebe a priori nicht oder nur schwer möglich, einen nahezu unterbrechungsfreien Betrieb im Notfall zu gewährleisten.
Die wesentlichste organisatorische Maßnahme ist die Erstellung eines Notfallplans. Dieser sollte alle erdenklichen Eventualitäten für den Krisenfall vorsehen und für die Beteiligten exakte Handlungsanweisungen enthalten. Um im Ereignisfall möglichst effizient reagieren zu können, sind darüber hinaus regelmäßige Übungen – typischerweise einmal jährlich – erforderlich. Auf diesem Weg lassen sich auch eventuelle Schwachstellen im Notfallplan identifizieren und ausmerzen.

[43] http://www.idc.com/ „Worldwide Outbound Content Compliance 2005-2009 Forecast and Analysis: IT-Security Turns Inside Out" November 2005 [27. Feber 2007]

Für die Mitarbeiter sollte eine Vertreterregelung Pflicht sein, weiters sollten sie laufend über technische Änderungen informiert und regelmäßig geschult werden.
Die baulichen Maßnahmen umfassen die Wahl eines geeigneten Rechenzentrumstandorts, die Beachtung der notwendigen Vorschriften (Brandschutz, Klimatisierung etc.) und geeigneter Zutrittsmöglichkeiten. Lokale Ausweichlösungen sind meist nicht ausreichend, aus diesem Grund ist ein Ausfallsrechenzentrum in entsprechender Entfernung erforderlich, das die notwendigen Aufgaben übernehmen kann.
Zu den technischen bzw. organisatorischen Maßnahmen gehören die Bereitstellung von Ausweicharbeitsplätzen für besonders kritische Tätigkeiten und die sorgfältige Auswahl des Internet Service Providers.

1.3.2 TECHNISCHES VERSAGEN

1.3.2.1 Problembeschreibung

Hierunter werden Anomalien im Zusammenhang mit Hardware, Software, Netzwerken oder Leitungen verstanden.
Während Hardwaredefekte meist auf Fabrikationsfehler, altersbedingten Verschleiß oder Überbeanspruchung zurückzuführen sind, begründet sich das „Nichtfunktionieren“ von Softwarekomponenten durch Programmierfehler bzw. Änderungswünsche der Geschäftsbereiche/Fachabteilungen. Meist handelt es sich dabei um schon länger im Einsatz befindliche Programme, die noch dazu meist relativ schlecht dokumentiert sind.
Beim Ausbringen von Standardsoftware sollte zumindest auf das Erscheinen der ersten Systemaktualisierungen (engl. *Updates* oder *Patches*) gewartet werden.
Aufgrund der starken informationstechnischen Vernetzung der Geschäftsprozesse können selbst kleinere technische Störungen erhebliche Auswirkungen bzw. Stillstandszeiten zur Folge haben.

1.3.2.2 Gegenmaßnahmen

Neben einer regelmäßigen Datensicherung, bei der die Sicherungen an einem entfernten Ort erfolgen sollten, ist vor allem der Einsatz von fehlertoleranten Technologien erforderlich. Diese reichen von redundanten Datenspeicherlösungen bis hin zu redundanten Rechnersystemen, dabei sollten einzeln auftretende Fehlerstellen (engl. *Single Point of Failures)* vermieden werden. Bei *Cluster*-Lösungen laufen mindestens zwei Rechner im Verbund, die so konzipiert und ausgelegt sind, dass das andere System die Aufgaben des ausgefallenen binnen Millisekunden übernimmt, sobald ein System ausfällt. Ein Trend geht zur Abstrahierung der Betriebssysteme und Applikationen weg von der Hardware.

Diese als *Virtualisierung*[44] bezeichnete Methode erlaubt eine bessere Auslastung der Ressourcen und erhöht die Flexibilität der Einsetzbarkeit.

1.3.3 MENSCHLICHES VERSAGEN

1.3.3.1 Problembeschreibung

Menschen agieren entweder unabsichtlich oder absichtlich (vorsätzlich). Während unabsichtlichen Handlungen meist unbewusste Nachlässigkeit (z. B.: das irrtümliche Herausziehen eines Netzsteckers) oder Unwissen (z. B.: Fehleingabe) zu Grunde liegen, ist Absichtlichkeit mit bewusst nachlässigem Handeln verbunden. Im Gegensatz zu diesen beiden Kategorien liegt bei einer Vorsätzlichkeit Schädigungsabsicht vor. Derartige Handlungen können durch Unzufriedenheit oder Racheabsichten – etwa nach Entlassung oder Bereicherungsgedanken – ausgelöst werden.
In vielen Branchen – vor allem im IT-Bereich – ist es üblich, temporär Externe zu beschäftigen, die als Mitarbeiter von Unternehmensberatungen, Personalleasingfirmen oder als freiberufliche Arbeitnehmer – oft vollen – Zugriff auf interne Unternehmensressourcen haben. Aufgrund ihrer räumlichen Präsenz innerhalb des Unternehmens können auch sie den internen Bedrohungen zugeordnet werden, da sie im Gegensatz zu den externen Angreifern wesentliche Schutzmechanismen nicht mehr überwinden müssen.

1.3.3.2 Gegenmaßnahmen

Viele Angriffe sind auf die Unwissenheit der Anwender zurückzuführen. Bewusstseinsbildung und Schulungen (siehe *1.8.2.5.2 Sensibilisierung und Schulung* und *1.8.3 Der Faktor Mensch*) können das Sicherheitsniveau mit vergleichsweise geringem Aufwand beträchtlich erhöhen. Technische Abhilfe kann etwa durch Plausibilitätsabfragen in der eingesetzten Software oder durch klare Rechtevergabe und -verwaltung geschaffen werden.

1.3.4 COMPUTER ANOMALIEN/MALICIOUS CODE

1.3.4.1 Problembeschreibung

Die ersten Computerviren waren noch relativ harmlos und dienten lediglich dem Aufzeigen diverser Schwachstellen von Computersystemen, wobei der *spielerische* Gedanke im Vordergrund stand. Die Fähigkeiten der Schädlinge haben sich rasant weiterentwickelt: vom Löschen von Dateien über das Ausspionieren von Daten und Passwörtern (siehe *1.3.4.7 Spyware*) bis hin zum Öffnen des Systems für entfernte Benutzer durch *Backdoor*-Komponenten (siehe *1.4.3.2 Backdoor/Rootkit*). Mittlerweile existieren im Internet fertige Baukästen, die neben einer Anleitung auch alle notwendigen Bestandteile

[44] Vgl. http://www.vmware.com/de/virtualization/ [3. März 2007]

für die Erstellung einfacher Viren liefern. *MessageLabs*[45], Anbieter von integrierten Messaging- und Websecurity-Services für Unternehmen, berichtet von einem „Geschäftsmodell" russischer Cracker. Dabei geht es um ein Service für Schadsoftware, welches mit einem kommerziellen Preismodell versehen ist. Nach Bedarf kann entweder einmalig oder im Rahmen eines Servicevertrages Schadsoftware (Trojaner, Keylogger, Spyware, Rootkits etc.) bezogen werden. Der Kunde kann aus einem Pool die gewünschte Software auswählen und wird im Rahmen des Vertrages mit Updates versorgt.

Wurde bis vor einiger Zeit noch zwischen verschiedenen Arten von Schädlingen (Virus, Wurm, Trojanisches Pferd etc.) unterschieden, besitzen die meisten heute vorkommenden Schädlinge eine Kombination von Attributen unterschiedlicher Ausprägungen.

Schadsoftware (engl. *Malware* oder *Malicious Code*) ist der Überbegriff für alle Computerprogramme, welche vom Benutzer unerwünschte, schädliche Funktionen ausführen. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die Kompromittierung der Sicherheitseinrichtungen (Firewall, Antivirenprogramm) eines Computers sein. Bis zum Auftreten des hundert tausendsten Schädlings im Jahr 2004 hat es 18 Jahre gedauert, der zweihundert tausendste Schädling[46] wurde bereits zwei Jahre später im August 2006 entdeckt. Interessant ist der Umstand, dass im Jahr 2006 laut Sicherheitsexperten *McAfee*[47] kein einziger Massenausbruch verzeichnet wurde. Die Angreifer gehen gezielt vor, es zählt nicht (mehr) der Grad der Bekanntheit, im Vordergrund stehen finanzielle Faktoren.

Die größer werdende Zahl an Schadsoftware stellt Hersteller wie User vor neue Probleme. Auf der einen Seite müssen die Hersteller danach trachten, möglichst „schlanke" Schutzapplikationen und Datenbanken zu programmieren. Auf der anderen Seite leiden die Benutzer unter immer größer werdenden Geschwindigkeitsverlusten, weil die Schutzprogramme am PC nach immer mehr und verschiedenen verseuchten Codes in immer größer werdenden Datenbanken suchen müssen. Erfahrungsgemäß verschlingt ein Standardschutzpaket (Antivirus, Firewall) bis zu 15 Prozent der Systemressourcen eines PCs, vor allem im Arbeitsspeicherbereich.

1.3.4.1.1 Exkurs: Botnet

Botnets[48] entstehen durch die Verseuchung von PCs mit Malware. Diese Netzwerke werden (von kriminellen Organisationen) für *Spam*-Verbreitung (siehe 1.6 *Exkurs: E-Mail/Spam*) oder *Denial of Service (DoS)*-Attacken (siehe *1.4.3.7 Denial of Service*) verwendet, ohne dass die Benutzer der missbrauchten PCs dessen gewahr werden. Große Botnets können aufgrund ihrer Bandbreitensumme durch Senden von entsprechenden Datenmengen beispielsweise die Leitungen eines attackierten

[45] Vgl. http://www.messagelabs.com/ „Intelligence Report" Juni 2006 [11. März 2008]
[46] Vgl. http://news.softpedia.com/news/McAfee-200-000-virus-definitions-28896.shtml [26. März 2007]
[47] http://www.mcafee.com/ [27. Feber 2007]

Internet Service Provider (kurz: ISP) überlasten (Anm.: meist ist ein Kunde des ISP das Ziel des Angriffs).

Grundsätzlich gilt, je verbreiteter ein Programm, desto höher ist konsequenterweise das Gefährdungspotenzial. Produkte von Microsoft[49] sind demnach aufgrund ihrer Marktpräsenz das beliebteste Angriffsziel. Hierzu passend ein Bericht[50] vom IT-Medienberichterstatter *IDG*: „*Hackers hunting for unpatched Microsoft computers. Hackers are actively using exploit code to target a flaw in Microsoft Corp's software that generated a special warning from the U.S. government last week. The problem involves a networking function called Windows Server services within the Windows operating system that is used for file sharing and printing. Microsoft last week issued Patch MS06-040 for the problem, which affected several Microsoft operating systems. Security experts warned then that exploit code had been detected and could be used more widely. The SANS Institute reported other names given to the exploit code by security vendors. Symantec Corp. calls it W32.Wargbot and Trend Micro Inc. has named it Worm.IRCBOT.JK. McAfee Inc. goes by IRC.Mocbot and F-Secure Corp. refers to the malware as IRCBOT-ST.*“

Durch diesen *Bug*[51] kann ein System auch als Bot missbraucht werden: *„The malware is a bot, a class of malicious code that allows a hacker to take remote control over a computer. Once on an infected machine, the bot contacts remote servers in China over Internet Relay Chat. It can send messages through a user's AOL LLC Instant Messenger account, an activity that could be used to trick other users into downloading the bot. The U.S. Department of Homeland Security highlighted the MS06-040 vulnerability a day after Microsoft issued a patch, saying it "could impact government systems, private industry and critical infrastructure, as well as individual and home users." Microsoft issued a total of twelve fixes this month on what's known as Patch Tuesday.*“

Eine im Jänner 2008 publizierte Analyse des US-Sicherheitsunternehmens *Marshal Limited*[52] besagt, dass rund 85 Prozent der weltweit verschickten Spam-Mails aus nur sechs verschiedenen Botnets stammen. „Srizbi“ stellt mit 30 Prozent des verschickten Spams das größte Netzwerk dieser Art dar, gefolgt von „Rustock“ mit 20 Prozent und „Mega-D“ mit 11 Prozent. Als Hauptquelle weist die Analyse die USA mit einem Anteil von rund zwölf Prozent am Gesamtaufkommen aus.

Messagelabs [Messagelabs, 2007] berichtet von einer Weiterentwicklung der Botnets: „*2007 was the year when botnets came of age. Greater levels of technical ingenuity have led to the traditional botnets evolving from a simple command-and-control channel structure to more devolved and discreet botnets that have greater levels of agility and functionality and are much more difficult to disrupt.“*

[48] Unter einem Botnet versteht man ein durch das Internet fernsteuerbares Netzwerk aus PCs.
[49] http://www.microsoft.com/ [28. Feber 2008]
[50] Vgl. http://www.idg.net/ „Hackers hunting for unpatched Microsoft computers“ 14. August 2006 [27. Feber 2007]
[51] Als Bug wird ein Programm- oder Softwarefehler bezeichnet.
[52] http://www.marshal.com/ [11. März 2008]

Sicherheitsspezialisten veröffentlichen periodisch Berichte [Symantec, 2007] [McAfee, 2007] [Messagelabs, 2007] über die Veränderungen im Angriffsverhalten und den Einsatz neuer Techniken. Weltweit zeichnet sich ein Trend zu mehr Konvergenz ab. Zum einen verschmelzen E-Mail, Instant Messaging und Internet als Verbreitungskanäle für Malware, zum anderen gehen Techniken mit unterschiedlichem Ziel wie Viren, Trojaner oder Spyware zunehmend ineinander über. Bedrohungen durch große, weit verbreitete Internetwürmer haben kleineren, gezielten Angriffen Platz gemacht, die auf Betrug, Datendiebstahl und andere kriminelle Aktivitäten abzielen:

Abbildung 3: Anzahl der gezielten Attacken im Zeitverlauf

Das *SANS Institute*[53] präzisiert die zu erwartenden Sicherheitsbedrohungen für 2008:

- Website-Angriffe auf Sicherheitslücken im Browser und deren Plug-Ins. Speziell Plug-Ins werden als lohnende Angriffsziele gesehen, da diese beim Browser Update nicht automatisch gepatcht werden.
- Verbesserte Botnet-Massenangriffe.
- Verstärkte Spionage. Auffallend ist, dass Organisationen in China in diesem Umfeld immer mehr in Erscheinung treten.
- Bedrohungen gegen Mobiltelefone, insbesondere Apples *iPhone*[54], Googles *Android*[55] und Voice-over-IP.
- Identitätsdiebstahl durch Bots und Spyware.
- Ausnutzung von Sicherheitslücken in Webanwendungen, beispielsweise durch Cross-Site-Scripting.
- Social Engineering (z. B.: gefälschte Jobangebote von bekannten Jobbörsen) und *Event*-Phishing (US-Präsidentenwahl, Fußball-Europameisterschaft, Olympische Spiele etc.).

Der Bericht „*Privatanwender im Visier von Cyberkriminellen/Mit gezielten Attacken zu finanziellem Gewinn*“[56] (Zeitraum Jänner bis Juli 2006) hält fest, dass Heimanwender mit 86 Prozent die am häufigsten angegriffene Gruppe (der Finanzsektor folgt mit 14 Prozent) aller gezielten Internet-

[53] http://www.sans.org/ [11. März 2008]
[54] http://www.marshal.com/ [11. März 2008]
[55] http://code.google.com/android/ [11. März 2008]

Attacken weltweit sind. Angreifer sehen private Computer als das schwächste Glied in der Sicherheitskette. Während private und öffentliche Unternehmen in der Regel über entsprechende Schutzmaßnahmen verfügen, sind die privaten PCs meist schlechter geschützt. Heimcomputer stellen eine lukrative Zielgruppe für den Diebstahl sensibler Daten dar. Die Angreifer setzen dabei zunehmend bösartigen Code ein, der Ausweichtechniken nutzt (siehe *1.4.3.2 Backdoor/Rootkit*), um der Entdeckung durch Schutzprogramme und Intrusion Detection/Prevention-Systeme (siehe *1.7.2.4.4 Intrusion Detection Systeme und Intrusion Prevention Systeme*) zu entgehen. Symantec verzeichnete mehr als 4,6 Millionen aktive Botnet-Computer im Halbjahr 2006, das sind durchschnittlich 57.717 gekaperte Computer täglich, zudem wurden 6.110 DoS-Angriffe pro Tag registriert. Bei anderen Angriffen wird modularer Schadcode verwendet. Dieser ist zunächst mit limitierten Funktionen ausgestattet, kann sich aber nach der Installation auf dem Computer über das Internet selbständig mit zusätzlichen Schadfunktionen aufrüsten. 79 Prozent der 50 häufigsten Schädlinge im Untersuchungszeitraum funktionierten nach diesem Baukasten-Prinzip.

1.3.4.1.2 Verbreitungsmöglichkeiten

Die noch immer – neben der herkömmlichen Übermittlung via klassischer Datenträger (Diskette, CD, Band, USB[57]-Stick) – gebräuchlichste Verbreitungsform ist das Mitschicken von Malware in Anhängen (engl. *Attachments*) von Mails. Inzwischen steigt auch die Anzahl der direkt auf Webseiten (Foren, Weblogs etc.) platzierten Schadprogrammen. Der unerwünschte Download von Schadsoftware allein durch das Anschauen einer Webseite wird als *Drive-by-Download* bezeichnet. Ein bekanntes Beispiel dafür ist die sogenannte *JPEG-Lücke*[58]: Das bloße Betrachten eines verseuchten JPEG[59]-Bildes mit dem Microsoft *Internet Explorer* reicht(e) aus, um den Rechner zu verseuchen.

Schädlinge nützen Sicherheitslücken rund um den PC aus: Betriebssystemschwachstellen, Sicherheitslücken in Scripts (*ActiveX Controls*, *Java Applets* usw.), Verbindungsprotokollfehler etc. Ein *Exploit* ist ein Programm, das Schwächen bzw. Fehlfunktionen eines anderen Programms ausnutzt. Exploits nutzen den Umstand, dass Systeme nicht zwischen Programmcode und Daten unterscheiden. Das wohl bekannteste seiner Gattung ist das sogenannte *Zero-Day-Exploit*. So wird ein Exploit genannt, das am selben Tag erscheint, an dem die Sicherheitslücke publik wird. Das Tempo macht die Gefährlichkeit dieser Exploits aus, weil kaum ein Schutzprogrammhersteller so schnell in der Lage ist, die Sicherheitslücke entsprechend zu schließen.

[56] Vgl. http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20060925_01 [11. März 2008]
[57] USB steht für Universal Serial Bus und ist eine Schnittstelle bzw. Bussystem zum Verbinden von Computern mit Zusatzgeräten.
[58] Vgl. http://www.tecchannel.de/client/windows/402397/ [3. März 2007]
[59] JPEG steht für Joint Photographic Experts Group; ein gängiges Format für digitale Bilder.

Eine empirische Untersuchung (siehe Symantec-Bericht) hat ergeben, dass ein *ungepatchter* (sinngemäß für nicht geschlossene Programmlücken) PC mit Microsoft *Windows XP*-Betriebssystem[60] mit einer fünfzigprozentigen Wahrscheinlichkeit innerhalb von zwölf Minuten mit schädlicher Software infiziert wird, vor allem PC‘s mit Breitbandzugang sind hier besonders exponiert. Das Zeitfenster (engl. *Time-to-Patch),* das sich zwischen dem Auftauchen einer Schwachstelle und der Erhältlichkeit eines geeigneten Patch auftut, hat bei Unternehmen im Jahr 2006 durchschnittlich 28 Tage (50 Tage im zweiten Halbjahr 2005) betragen.
Eine Untersuchung[61] des Internet-Sicherheitsunternehmens *Websense*[62] konstatiert immer ausgefeiltere Methoden, um Würmer und Trojaner über das Internet zu verteilen. So stellt mittlerweile sogar der Besuch eines Weblogs eine Gefahr dar. Websense konnte im Rahmen der Untersuchung mehrere hundert Websites ermitteln, die virenverseuchte Weblogs enthielten. Angreifer suchen sich einen viel besuchten Weblog-Anbieter aus, dort wird ein Weblog angelegt und mit *Spyware* wie *Keyloggern*[63] versetzt. Mittels Spam oder *Instant Messaging*[64], in denen der Link zum betreffenden Blog enthalten ist, werden dann Benutzer auf die präparierten Seiten gelockt.
Neben Weblogs bieten praktisch alle Kommunikationsarten Verbreitungsmöglichkeiten für Malware – keine Technik und Technologie ist davor gefeit: *Voice over IP*[65], *Peer to Peer*[66], Chats (Instant Messaging), Skype etc.

1.3.4.2 Protokoll- (Un) Sicherheiten

Das Funktionieren des Internets wird durch rund 500 Protokolle sichergestellt. Eine übersichtliche Strukturierung findet sich im *Open Systems Interconnection Reference Model (kurz: OSI)-Schichtenmodell*[67]. Das OSI-Modell dient zur Kommunikation informationsverarbeitender Systeme auf Basis vereinheitlichter Verfahren und Regeln. Die Standardisierung erfolgte durch die *International Organization for Standardization* (kurz: *ISO*)[68]. Die folgende Grafik gibt die wichtigsten Internetprotokolle auf der Basis des Schichtenmodells wieder:

[60] http://www.microsoft.com/germany/windowsxp/default.mspx [3. März 2007]
[61] http://www.zdnet.de/security/news/0,39029460,39132319,00.htm „Websense: Blogs sind Virenschleudern“ [26. März 2007]
[62] http://www.websense.com/ [27. Feber 2007]
[63] Keylogger sind Programme, die sämtliche Tastaturanschläge eines Users registrieren, speichern und an Dritte weiterleiten.
[64] Unter Instant Messaging wird das Kommunizieren in Echtzeit über Intra- bzw. Internet verstanden.
[65] Das Telefonieren über Computernetzwerke wird als Voice over IP bezeichnet.
[66] Ein Peer to Peer (P2P)-Netzwerk ist das Gegenteil des Client/Server-Prinzips, das heißt alle Computer sind gleichberechtigt und können sowohl Dienste in Anspruch nehmen, als auch Dienste zur Verfügung stellen.
[67] http://www.iso.org/ ISO/IEC 7498-1:1994 [27. Feber 2007]
[68] ISO ist die internationale Vereinigung von Normungsorganisationen und erarbeitet internationale Normen (engl. Standards).

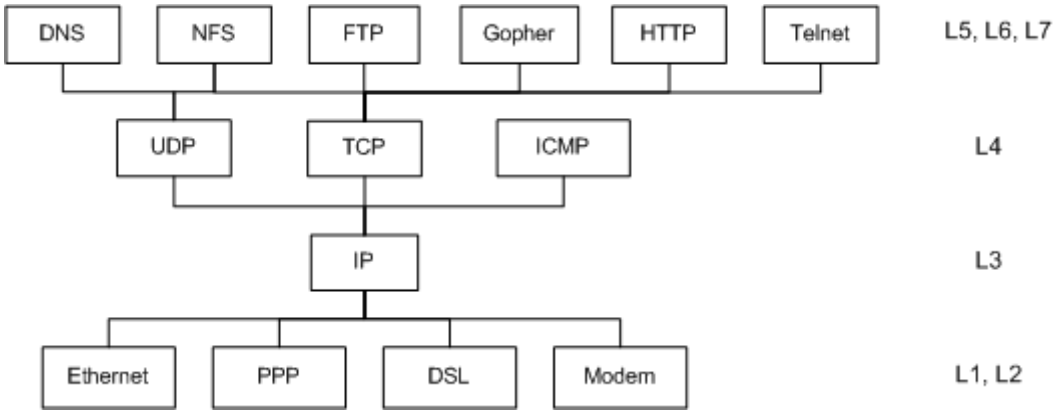


Abbildung 4: Protokolle des OSI-Schichtenmodells

1.3.4.2.1 TCP/IP-Sicherheit

TCP/IP steht für zwei Protokolle: *Transmission Control Protocol* (kurz: TCP) und *Internet Protocol* (kurz: IP). TCP/IP ist die Standardmethode zur systemübergreifenden Datenkommunikation. Sie bildet die Basis für das Verbinden unterschiedlicher Betriebssysteme bzw. Netzwerkkomponenten und ermöglicht die wichtigsten Dienste: E-Mail, Dateitransfer, Nachrichtendienst und den Zugriff auf das World Wide Web (kurz: WWW).

Der große Funktionsumfang des Protokolls bringt einige Sicherheitsrisiken mit sich, die durch folgende Angriffsmöglichkeiten [Weippl, 2004, Protocol Security (1), S 1ff] ausgenützt werden könnten: *SYN-Attacks, SYN-Cookies, IP-Spoofing, TCP-Sequence Number Guessing, Source-Routing, Connection-Hijacking, RIP-Attacks, ICMP-Attacks, Smurf-Attacks, insecure UDP* oder *ARP-Spoofing*. Ein DoS (siehe *1.4.3.7 Denial of Service*) wird durch eben diese Attacken aufgrund von Problemen (Abbrechen des Vorgangs in einem gewissen Zustand) in der *TCP-state machine*[69] ermöglicht. Bei *IPv6* wurde beim Design weit mehr auf Sicherheit bedacht genommen als bei *IPv4*.

1.3.4.2.2 DNS-Sicherheit

DNS steht für *Domain Name System* und ist für die Auflösung von Namen in IP-Adressen verantwortlich. So wird beispielsweise *www.tuwien.ac.at* in 128.130.102.130 aufgelöst. Ziel von Attacken wie *DNS-Packet Interception* oder *DNS-Cache poisoning* ist ein DoS (siehe *1.4.3.7 Denial of Service*) oder eine Manipulation durch *Masquerading* (eine IP-Adresse und Port-Nummer wird in einem Datenpaket durch andere ersetzt). *DNSSec* nutzt eine Verschlüsselung für die DNS-Kommunikation, die Authentizität und Integrität sicherstellt.

[69] Vgl. http://research.umbc.edu/~jeehye/cmsc491b/lectures/tcpstate/sld001.htm [27. Feber 2007]

1.3.4.2.3 HTTP-Sicherheit

Das *Hypertext Transfer Protocol* dient zur Übertragung von Daten über ein Netzwerk. Es wird eingesetzt, um Webseiten aus dem Internet in einen Webbrowser zu laden. HTTP hat in der Version 1.0 eine aus heutiger Sicht schwache Authentifizierung. Abhilfe wird durch Version 1.1 bzw. *HTTPS* geschaffen.
Durch *Request Smuggeling* wird es möglich, Firewall und Intrusion Prevention/Detection-Systeme (siehe *1.7.2.4.4 Intrusion Detection Systeme und Intrusion Prevention Systeme*) zu umgehen.

1.3.4.2.4 FTP-Sicherheit

File Transfer Protocol ist ein gängiges Protokoll, das Dateiübertragungen in TCP/IP–Netzwerken ermöglicht. FTP verfügt über eine schwache Authentifizierung, was anhand des vielerorts verwendeten *anonymous* FTP-Dienstes gesehen werden kann. FTP kann aufgrund des unverschlüsselten Passworts relativ leicht missbraucht werden. *FTPS* sorgt durch Verbindungsverschlüsselung für ein entsprechendes Mindestmaß an Sicherheit.

1.3.4.2.5 SSL/TLS-Sicherheit

Transport Layer Security (kurz: *TLS*) dient zur Verschlüsselung für Datenübertragungen im Internet. TLS ist die Weiterentwicklung von *Secure Socket Layer* (kurz: *SSL*). SSL/TLS wird als Verschlüsselung für HTTP (→ HTTPS), VPN, SMTP (→ SMTPS), FTP (→ FTPS) etc. verwendet und soll diese Protokolle bzw. Daten vor Lauschangriffen, Verfälschung oder Identitätsdiebstahl schützen. Ältere Implementierungen von SSL/TLS erreichen mit 40 Bit eine relativ schwache Schlüssellänge, die *brute-force*-Attacken (siehe *1.4.3.4 Passwort-Attacken)* erleichtert.

1.3.4.2.6 IPSec-Sicherheit

IP-Security (kurz: *IPsec*) ist ein Sicherheitsstandard für die verschlüsselte Kommunikation über IP-Netzwerke. IPsec soll durch Techniken [Weippl, 2004, Protocol Security (2), S 52ff] wie *Encapsulating Security Payload (ESP), Authentication Header (AH) und Internet Key Exchange (IKE)* die Sachziele Vertraulichkeit, Authentizität und Integrität gewährleisten. Am häufigsten findet IPSec bei Virtual Private Networks (VPN)-Verbindungen Verwendung. Trotz der niedrigen Netzwerkschicht (Layer 3 OSI-Schichtenmodell) gibt es einige Schwachstellen. IPSec wird sowohl in der Literatur als auch in der Praxis nach wie vor als bestmöglicher Schutz von IP gesehen.

1.3.4.2.7 Wireless LAN-Sicherheit

WLAN (siehe *1.5.4 Local Area Network*) bezeichnet allgemein ein drahtloses, lokales Funknetz im Standard *IEEE 802.11x*[70]. Ein Verschlüsselungsstandard ist *Wired Equivalent Privacy (WEP),* welcher auf dem *RC4-Algorithmus* basiert. *Bit-Flipping, Statistical Attacks, Known Plaintext Attacks* und *Authentication Forging* sind die gebräuchlichsten Angriffsformen [Weippl, 2004, Wireless LAN Security, S 5ff]. Mit Tools wie *WEPCrack*[71] oder *NetStumpler*[72] ist es relativ einfach, in ein WLAN „einzubrechen".

Aus diesem Grund sind technische Ergänzungen und Weiterentwicklungen wie *WEPplus, WPA, 802.11i/802.X, Extensible Authentication Protocol (EAP), Protected Extensible Authentication Protocol (PEAP)* [Weippl, 2004, a.a.O.] notwendig geworden. Dennoch bleibt ein Restrisiko bestehen, da jede einzelne Technologie Schwachstellen hat.

Es gibt jedoch alternative Sicherungsmöglichkeiten für drahtlose Netze: die Verschlüsselung kann auf die IP-Ebene verlegt werden. Der Datenverkehr wird dann etwa durch IPSec oder VPN geschützt. Möglich ist auch die Zuhilfenahme der *RADIUS*-Technologie, wo mittels Hardwareidentifikation Sicherheit geschaffen wird. Hiermit wird beispielsweise nur ein mobiles Gerät mit einer dem RADIUS-Dienst bekannten *MAC-Adresse* (siehe *1.4.3.6 Spoofing*) bzw. weiteren eindeutigen, frei wählbaren Clientmerkmalen für ein WLAN zugelassen.

Eine weitere Möglichkeit ist die Absicherung von WLAN durch einen „elektronischen Fingerabdruck". Forscher an der kanadischen *Carleton University*[73] haben festgestellt, dass die Funkelektronik jedes WLAN-Moduls eine eigene Charakteristik aufweist. Mittels des von Gerät zu Gerät unterschiedlichen „elektronischen *Fingerprints"* lassen sich die WLAN-Geräte eindeutig identifizieren [Hall, Barbeau, Kranakis, 2005].

1.3.4.3 Virus

Ein Virus ist ein nicht-selbständiges Programm, das sich in andere Programme, Dateien, Skripts, Makros und Bootsektoren (*Wirtsysteme)* „einnistet" und diese verändert. Auf diese Weise erfolgt – meist unbemerkt – die Infizierung. Charakteristisch für Viren sind die Selbstreplizierung und die Schadfunktion (engl. *payload*). Klassifiziert wird in der Literatur typischerweise nach *Boot-, Programm-* und *Makroviren.* Erwähnenswert ist die Selbstschutzfunktion von einzelnen Viren in Form von *Polymorph-* und *Stealthviren.*

Der beste Schutz vor Viren kann durch aktuell gehaltene Virenschutzprogramme erreicht werden[74].

[70] http://standards.ieee.org/getieee802/802.11.html [27. Feber 2007]
[71] http://wepcrack.sourceforge.net/ [27. Feber 2007]
[72] http://www.netstumbler.com/ [27. Feber 2007]
[73] Vgl. http://www.scs.carleton.ca/ [2. Mai 2007]
[74] Vgl. http://www.bsi.bund.de/av/texte/hinweise.htm [11. März 2008];
http://www.virenschutz.info/ [11. März 2008]

1.3.4.4 Wurm

Ein Wurm ist ein selbständiges Programm, das sich typischerweise über Netzwerke ausbreitet. Die Versendung erfolgt über infizierte E-Mails, Peer to Peer, Instant Messaging oder Dateifreigaben. Würmer für Handys und andere vergleichbare Geräte können sich über *Bluetooth*[75]- oder infizierte *MMS*[76]-Nachrichten verbreiten. Ein Wurm ist im Gegensatz zu Viren aktiv, das heißt, er wartet nicht passiv auf eine Weitergabe durch infizierte Dateien, sondern versucht selbst über verschiedene Wege PCs zu infizieren, zudem muss er nicht unbedingt eine spezielle Schadensroutine enthalten. Da ein Wurm sowohl auf den infizierten als auch auf den zu infizierenden Systemen Ressourcen bindet, kann er alleine dadurch Schaden anrichten.

Ein Beispiel über die Funktionsweise und -vielfalt bzw. Verbreitungsmöglichkeit eines Wurms (August 2006)[77]: „*Das Sicherheitsunternehmen Symantec berichtet über einen neuen Wurm, der eine Sicherheitslücke im Serverdienst von Windows ausnutzt. Der Wurm W32.Randex.GEL beherrscht eine Reihe von Methoden, sich weiter im Internet zu verbreiten. Microsoft hat mittlerweile ein Sicherheitsupdate zur Verfügung gestellt, wodurch die Lücke geschlossen wird. Der Wurm verbreitet sich mit Hilfe der Instant Messenger von AOL, ICQ, MSN und Yahoo und nutzt Netzwerkfreigaben, Microsoft SQL-Server sowie vier bekannte Sicherheitslücken in Windows. Der Schädling legt eine Kopie von sich als „javanet.exe" im Systemverzeichnis von Windows ab und trägt diese als neuen Dienst in die Registry ein. Zudem sorgt er dafür, bei jedem Neustart geladen zu werden. W32.Randex.GEL öffnet eine Hintertür ins System, indem er auf dem TCP-Port Kontakt mit einem IRC-Server (Internet Relay Chat) aufnimmt. Sobald er seine Vorbereitungen abgeschlossen hat, ist der Wurm auf Standby und wartet auf Kommandos. So wird er beispielsweise angewiesen, Dateien herunter zu laden, laufende Prozesse zu stoppen, DoS-Angriffe zu starten oder Tastatureingaben zu protokollieren. Es können auch Anmeldedaten für Onlinebanking, eBay, PayPal und andere Dienste ausspioniert werden.“*

Schutzmaßnahmen gegen Würmer sind zum einen das Patchen von Systemen und Programmen (siehe *1.7.1.2.2 Patchmanagement*), zum anderen Virenschutzprogramme und (Personal) Firewallsysteme.

1.3.4.5 Trojanisches Pferd

Als Trojanisches Pferd (kurz: Trojaner) wird ein Programm bezeichnet, das neben seiner eigentlichen Funktion eine dem Anwender unbekannte Funktion ausführt. Trojaner können in verschiedenen

[75] Bluetooth ist ein Industriestandard (IEEE 802.15.1) für die drahtlose Vernetzung von Geräten (Mobiltelefone, PDAs, Computer, Peripherie) über kurze Distanzen. Solche Netzwerke werden als Wireless Personal Area Network (WPAN) bezeichnet.

[76] Multimedia Messaging Service bietet die Möglichkeit, multimediale Nachrichten an andere mobile Endgeräte oder an E-Mail-Adressen zu schicken.

[77] Vgl. http://www.pressetext.at/pte.mc?pte=060824039 [3. März 2007]

Varianten[78] auftreten: als versteckte Funktionalität in einem vordergründig nützlichen Programm, als modifizierte Programmkopien oder als eigenständiges Programm.
Diese kann von der Beschädigung von Systemressourcen über das Ausspionieren von Informationen bis hin zur Fernsteuerung eines Rechners reichen: Dateioperationen (Upload/Download/Löschen von Dateien), Erstellen von Netzwerkfreigaben, Spionagefunktionen (Passwörter, Aufzeichnung von Tastatureingaben, Screenshots, laufende Übertragung der Bildschirmausgabe) oder Fernsteuerungsfunktionen (Übernahme von Tastatur und Maus, Beendigung von Programmen, Abmelden des Benutzers, Herunterfahren des PCs).
Die folgenden Beispiele sollen die Bandbreite der Anwendungsmöglichkeiten illustrieren:

- Überwachung des Datenverkehrs mithilfe von Sniffern (siehe *1.4.2.4 Sniffing*),
- Ausspähen von Daten (Passwörter, Kreditkartennummern, Kontonummern etc.),
- Fernsteuerung des Rechners etwa für kriminelle Zwecke, zum Beispiel zum Versenden von Werbe-E-Mails oder der Durchführung von DDoS-Attacken (siehe *1.4.3.7 Denial of Service*),
- Installation von Dialer[79]-Programmen für die heimliche Einwahl auf Mehrwertrufnummern,
- Benutzung der Systemressourcen zur Ablage von illegalen Dateien,
- Einblendung unerwünschte Werbung-Popups[80] oder Umleitung auf ungewollte Webseiten.

In der Regel werden Trojaner durch den Benutzer gestartet, wodurch sie dessen Berechtigungen erhalten, gleiches gilt für alle Schadprogramme, welche die Trojaner auf dem Computer installieren.
Rechner können sich mit einem Trojaner über Datenträger, durch Downloads aus dem Internet (bei Besuch von Diskussionsforen oder Blogs) oder durch den E-Mail-Verkehr infizieren. Gängige Verteilmethode ist das Anbieten von falschen Updates für bekannte Software. So wurden beispielsweise im Laufe des Jahres 2006 Trojaner zum Download bereitgestellt, die vorgegeben haben, ein Update von Skype[81] bzw. *Firefox*[82] zu sein. Die Verbreitung des Trojaners erfolgt somit oft durch den Anwender selbst, technisch gesehen in einer Kombination aus Wurm und Trojaner.
Die Infektion erfolgt durch eine Veränderung eines Programms: die bestehende Datei, meist in einer ausführbaren (engl. *executable*, kurz: *exe*) Form, wird mit einem Trojaner versehen (*Huckepackprinzip*) und zu einer neuen exe-Datei gemacht. Zudem wird beim erstmaligen Aufrufen der Trojaner so im System verankert, dass er mit jedem Rechnerneustart wieder aufgerufen wird. Damit eröffnen sich dem Angreifer einige Möglichkeiten zur Kontrolle des vereinnahmten PCs. Viele der Funktionen erfordern eine synchrone Kommunikation zwischen Angreifer und Angriffsziel. Diese kann durch den Einsatz von Firewalls, mit der Verwendung interner und externer IP-Adressen sowie

[78] Vgl. http://www.trojaner-info.de/beschreibung.shtml [3. März 2007]
[79] Dialer sind Computerprogramme zur Verbindungsherstellung mit dem Internet über das analoge Telefonnetz.
[80] Popups sind visuelle Elemente einer Software, um beispielsweise Werbung in einem Browser anzuzeigen.
[81] Trojaner „IRCBot“

dem Schließen von ungenutzten Ports unterbunden werden. Aus diesem Grund verlagern sich die Angriffe häufig auf (vertraute) Kommunikationspartner des Angriffsziels. Dies können einerseits die Kunden sein, andererseits auch die Mitarbeiter, die sich von außen in das Unternehmensnetz einwählen. So konnten beispielsweise vor einigen Jahren Cracker ins Firmennetz von Microsoft gelangen, indem per E-Mail in den Heimrechner eines Mitarbeiters ein Trojaner eingeschleust wurde, der in weiterer Folge die notwendigen Zugangsinformationen ausspähte.

Mögliche Gefahr für Kunden durch Trojaner droht im Onlinebanking (siehe *1.4.1.2 Exkurs: Phishing*) beim PIN/TAN-Verfahren. Von den im Zeitraum April-Juni 2006 von *Panda Software*[83] registrierten Schädlingen waren knapp die Hälfte Trojaner, im Speziellen sogenannte *Bankfraud*-Trojaner. Wurden im Jahr 2006 9.042 Bankfraud-Trojaner von Panda gezählt, gab es im Jahr 2007 einen Anstieg von 463 Prozent auf 88.165. Zahlen aus dem Jahr 2008 zeigen täglich rund 10.000 neue Schädlinge. Davon sind ein Drittel Trojaner, knapp 5 Prozent Bankfraud-Trojaner. Gelingt es dem Angreifer, einen Trojaner auf den Kundenrechner zu platzieren und eine Onlinebanking-Session zu überwachen, so kann er die Onlinebanking-Anwendung respektive den Webbrowser nach der Eingabe, aber vor dem Absenden der einmaligen TAN beenden. Der Angreifer ist nun im Besitz der PIN und des noch ungenutzten TAN und kann mit diesen eine Transaktion durchführen.

Eine neue Generation von Trojanern kommuniziert nicht mehr direkt mit dem Angreifer, sondern asynchron über E-Mail, indem sie die Funktionalitäten des Microsoft *Message Application Programming Interface* (kurz: *MAPI*) ausnutzen, das von einem Großteil der weltweit eingesetzten Mailsysteme verwendet wird. Damit ist es möglich, versteckte Mailordner anzulegen, wodurch der Mailverkehr transparent wird. Der Trojaner erzeugt durch das Anlegen eines versteckten Ordners einen unsichtbaren Kommunikationskanal, über den er per E-Mail seine Befehle erhält und die gewonnenen Ergebnisse verschickt. Da E-Mail zum Standardmedium geworden und in dieser Richtung nicht kontrollierbar ist, besteht kein Schutzmechanismus, derartige Angriffe zu unterbinden.

Der österreichische Antivirenhersteller *Ikarus*[84] hat im Jahr 2006 eine starke Zunahme an Trojanern beobachtet: Alleine im August 2006 wurden bei Ikarus über 16.000 neue Trojaner registriert – mit nach wie vor steigender Tendenz. Dies wird durch einen Report von Panda für den Monat Feber 2008 bestätigt. Mit einem Anteil von 23,70 Prozent haben Trojaner die meisten Infektionen verursacht. Die Verbreitung erfolgt nicht mehr nur via E-Mail, sondern über präparierte Webseiten bzw. FTP und die darüber genutzten Dienste. Von kostenlosen *Countern* in Webseiten über Erotikseiten bis hin zu aktuellen Download-Videos reicht die Palette der Malware-Quellen. Zudem können auch *Microsoft Office*-Applikationsdateien[85], wie *Word*-Dokumente oder *Excel*-Sheets, Bilddateien oder PDF-Dateien

[82] Trojaner „FormSpy“, „DownloaderAXM“
[83] Vgl. http://www.pandasoftware.com/ „Panda Software advises on how to avoid Internet bank fraud“ September 2006 [26. März 2007]
[84] Vgl. http://www.ikarus-software.at/portal/index.php September 2006 [27. Feber 2007]
[85] http://office.microsoft.com/de-de/default.aspx [4. März 2007]

Links auf verseuchte Webseiten enthalten. Trojaner bleiben auch aufgrund neuer Methoden unentdeckt. So werden beispielsweise eigens entwickelte Komprimierungsprogramme verwendet, um den Schutzprogrammen den Blick in das Datenpaket zu erschweren oder Trojaner sind so programmiert, dass sie die Statusfenster der Personal Firewall oder des Virenscanners schließen können.

Trojaner werden aufgrund ihrer Funktionsvielfalt als gefährlicher eingestuft als Viren und Würmer. Viren und Würmer können lediglich die ihnen bei der Erstellung implementierten Fähigkeiten entfalten, wogegen Trojaner den Angreifenden mit Informationen über das befallene System versorgen, sodass der Angriff dem spezifischen Umfeld angepasst werden kann. Zudem können Trojaner mit Selbstverbreitungsmechanismen ausgestattet sein. Da Trojaner versteckt operieren, bleibt ihre Existenz den Schutzprogrammen meist verborgen (siehe *1.4.3.2 Backdoor/Rootkit*).

Als Schutz vor Trojanern bieten sich zunächst Virenscanner[86] an. Aufgrund der Konsistenz von Trojanern verfehlen diese meist die bei Viren gewohnte Wirkung (siehe *1.4.3.8 Hacking, Beispiel 2*). Hilfe versprechen Werkzeuge zur Integrationsüberprüfung (engl. *Integrity Checker*), die für die wichtigsten Systemdateien Prüfsummen erstellen, so dass Veränderungen durch Neuberechnungen entdeckt werden könnten. Weiters ist die Überprüfung von Anschlüssen[87] (engl. *Ports*) ein probates Mittel. Dies kann mit Programmen geschehen oder mit dem in Windows enthaltenen Befehl „netstat“. Dazu ist in der Eingabeaufforderung die Befehlszeile „netstat -a“ einzugeben. Es erscheinen die aktiven Verbindungen (Beispiel):

Proto	Lokale Adresse	Remoteadresse	Status
TCP	_:31337	0.0.0.0:45178	ABHÖREN
UDP	_:31337	*:*	

In dem Beispiel wartet ein Programm an Port 31337 auf eine Verbindung. Der erfahrene Anwender kann über den Port auf das Programm schließen, 31337 steht für *Back Orifice*[88], einen bekannten Trojaner.

1.3.4.6 Adware

Als Adware, ein Kunstwort aus *Advertising* (engl. für Werbung) und Software, bezeichnet man – üblicherweise kostenlose und meist *heimlich* installierte – Software, die dem Benutzer Werbebanner oder Popups anzeigt. Diskutiert wird, ob Adware als Spyware zu bezeichnen ist. Fest steht, dass auch Adware meist Informationen über das Surfverhalten der Benutzer zurückliefert, damit Werbung gezielter präsentiert werden kann.

[86] Vgl. http://www.trojaner-info.de/ [27. Feber 2007]
[87] Ports sind in Netzwerkprotokollen eingesetzte Adresskomponenten, um Datensegmente den richtigen Diensten zuzuordnen.
[88] http://www.tcp-ip-info.de/trojaner_und_viren/backorifice.htm [4. März 2007]

Diese Bedrohungen, die bislang nur als eine Gefahr für die Heimanwender eingestuft wurden, sind laut dem Sicherheitslösungsanbieter *Fortinet*[89] zunehmend auch für Unternehmen und Behörden relevant. Verdacht auf Adware besteht, wenn der PC langsamer arbeitet als sonst oder wenn am Bildschirm Popups und Werbung angezeigt werden, auch wenn keine Verbindung zum Internet besteht. Die Installation von Adware-Schutz an der Netzwerkperipherie (siehe *1.7.2.4 Perimetersicherheit*) ist die beste Lösung, um solche Applikationen zu identifizieren und unschädlich zu machen, noch bevor sie den Rechner des Endbenutzers erreichen.

1.3.4.7 Spyware

Als Spyware wird Software bezeichnet, die persönliche Daten eines PC-Benutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software bzw. an Dritte sendet oder dazu genutzt wird, dem Benutzer direkt Produkte anzubieten.

Die gelieferten Daten dienen im positiven Sinn etwa zur Bekämpfung von Softwarepiraterie, Bekämpfung von illegalen Tätigkeiten, im Negativen zur Generierung von Benutzerprofilen, Überwachung von Mitarbeitern am Arbeitsplatz (siehe *2.3.3.2.9 Angriff auf Informationssicherheit und die Verwendung von Malicious Code*), Daten- bzw. Identitätsdiebstahl (siehe *1.3.5.3 Identitätsdiebstahl*), Erpressung oder Industriespionage.

Spionage kann durch Software wie auch Hardware erfolgen: von Trojanern über *Cookies*[90] (siehe: *2.3.3.2.3 Cookie*), ActiveX[91] bis hin zu Keyloggern und Netzwerksniffern (siehe *1.4.2.4 Sniffing*). Spyware findet sowohl im privaten wie auch unternehmerischen Umfeld Einsatzmöglichkeiten.

Beim Erstellen von Profilen werden Daten über die Gewohnheiten der User gesammelt, um diese beispielsweise für Werbezwecke zu nutzen. Auf diese Weise werden Webseiten so personalisiert, dass jene Produkte angezeigt werden, für die sich der Benutzer schon einmal interessiert bzw. die er via Webshop bezogen hat. Technisch ermöglicht wird das etwa durch Cookies bzw. *Webbugs*[92] (*siehe 2.3.3.2.4 Webbug*). Beim Herunterladen der Software wird ein Cookie zum Wiedererkennen des PCs für den erneuten Besuch der Website hinterlegt. Das Cookie enthält eine Kennung, unter der die

[89] Vgl. http://www.fortinet.com/ „Top-Ten-Guide zur Erkennung von Greyware“ Juni 2005 [27. Feber 2007]

[90] Ein Cookie ist ein Eintrag in einer Datenbank und dient dem Austausch oder der Archivierung von Informationen. Webbrowser stellen eine Cookie-Datenbank zur Verfügung: der Webserver kann dort Informationen von einer besuchten Webseite in Form von HTTP-Cookies hinterlegen und bei einem Wiederbesuch der Seite auslesen.

[91] ActiveX sind Softwarekomponenten von Microsoft für Anwendungen, Makros und Entwicklungsprogramme aktiven Inhalts. Bei der Programmierung und beim Einsatz von ActiveX-Komponenten in Webbrowsern müssen bestimmte Regeln eingehalten werden (Anm.: in der Praxis nicht immer der Fall), um Sicherheitslücken zu vermeiden.

[92] Als Webbugs bezeichnet man kleine, meist unsichtbare Grafiken in HTML-E-Mails oder auf Webseiten, die Aufzeichnungen ermöglichen. Mit dem Öffnen einer Webseite wird dieser Grafik von einem Server im Internet geladen. Der Betreiber des Servers kann somit sehen, wann und wie viele Benutzer diesen Webbug benutzten respektive ob und wann eine E-Mail geöffnet oder eine Webseite besucht wurde. Sofern Standards eingehalten werden, ist es sogar möglich, folgende Informationen über die Besucher zu erhalten: Gültigkeit der E-Mail-Adresse, Betriebssystem, Webbrowser, IP-Adresse.

gefundenen Daten beim Anbieter gespeichert werden. Durch die Registrierung gelangen Daten über den Benutzer zum Anbieter. Alle bei erneuten Besuchen anfallenden Daten können den bereits vorhandenen zugeordnet werden.

Beliebte Ziele bei der Datenspionage (siehe *1.3.5.2 Datendiebstahl und Spionage*) sind naturgemäss Benutzerkonten, Passwörter, Kreditkartennummern (siehe *1.4.1.2 Exkurs: Phishing*) oder auch *PGP*[93]-Schlüssel bzw. Informationen zur Aufbau- und Ablauforganisation (siehe *1.4.1 Möglichkeiten der Informationsbeschaffung*).

Überwacht werden Personen sowohl in der eigenen Familie als auch im Unternehmen. Während im Familienkreis meist Eltern bewusst die Tätigkeiten ihrer Kinder überwachen wollen, liegt es im betrieblichen Umfeld am Arbeitgeber, ob er über die ohnehin vorhandenen Daten (z. B.: Stammdaten) des Arbeitsnehmers hinaus noch aktiv und gezielt nach Informationen sucht. In einem Unternehmen gibt es viele Möglichkeiten, Mitarbeiter zu überwachen bzw. auszuspionieren. So können die Einlogzeiten am PC und der Besuch von Webseiten mit protokolliert, Zeiterfassungs- und Personalstammdaten analysiert werden. Ein nächster Schritt ist der Einsatz von speziellen Überwachungsprogrammen. Damit ist es möglich, Tastatureingaben aufzuzeichnen, die Zwischenablage zu speichern, den Mailverkehr mitzulesen, Chats mitzuschneiden und ähnliches mehr.

Die Gefahr für Unternehmen, Opfer von Spywareschäden zu werden, nimmt enorm zu. Dem „*State of Spyware"*-Report[94] des Softwarespezialisten *Webroot*[95] zufolge ist die Zahl der Spyware-Programme auf Firmen-PCs allein in den Monaten April bis Juni 2005 um 19 Prozent gestiegen. Ein viel benütztes „Einfallstor" sind Anhänge in E-Mails. Motivation zu immer neuen Zielen und Methoden, um Computer mit Spionageprogrammen zu verseuchen, ist das Streben nach Profit. Von den Spionageangriffen sind jedoch nicht nur Unternehmen betroffen, sondern auch die privaten Anwender. Insgesamt sind rund 80 Prozent der Privatrechner mit Spyware verseucht, im Durchschnitt befinden sich darauf mehr als 25 Spyware-Programme, die meist aus den USA kommen.

Ein Problem stellt die oft unklare Grenze zwischen legaler Werbung und illegaler Spyware dar. Um mögliche rechtliche Probleme zu vermeiden, kennzeichnen viele Antispyware-Programme die ermittelten Softwarekomponenten als unerwünschte Software.

[93] Pretty Good Privacy (kurz: PGP) ist ein weit verbreiteter Algorithmus zur Verschlüsselung von Daten.
[94] Vgl. http://www.antyspyware.pl/state-of-spyware/2006-q1-sos.pdf August 2006 [26. März 2007]
[95] Vgl. http://www.webroot.com/ [27. Feber 2007]

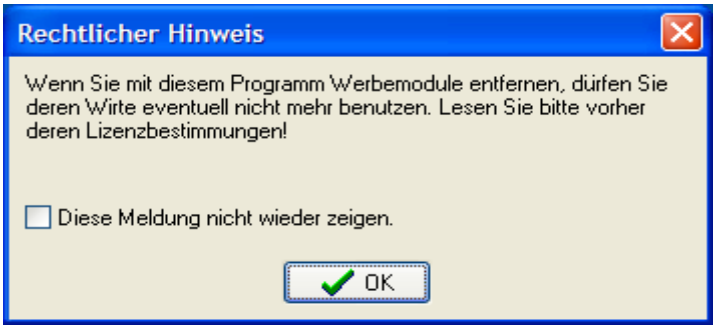


Abbildung 5: Rechtlicher Hinweis Spyware-Schutz

Die amerikanische Verbraucherorganisation *Consumer Reports*[96] hat im Bericht „*State of the Net*“ bilanziert, dass Verbrauchern in den Vereinigten Staaten von 2004 bis 2005 durch Angriffe aus dem Cyberspace über acht Milliarden US-Dollar Schaden entstanden ist. Auf die Kategorie „Spyware“ entfiel Schaden von 2,6 Milliarden US-Dollar bei Kosten von $ 100 pro Vorfall: „*Despite a decline in the incidence of spyware, its resulting problems remain epidemic. In the previous six months, spyware infections prompted nearly a million U.S. households to replace their computer*.” In der Ausgabe dieses Reports für 2007 werden folgende Fakten festgehalten: “*In the first half of 2007, spyware infections prompted 850,000 U.S. households to replace their computers. 1 out of every 11 surveyed had a major, often costly problem due to spyware. The economic fallout per incident was $100, with damage totalling $1.7 billion*.“

Eine Umfrage von *Computerworld*[97] bei 577 IT-Managern zum Thema Spyware in Unternehmen hat ergeben, dass 79 Prozent der Befragten Probleme mit Spyware hatten. Im Speziellen rühren die Probleme von Einbußen in der Geschwindigkeit der PCs (engl. *Desktop-Performance-Issues*) und durch Trojaner bzw. Backdoor ermöglichten „Einbruch“ (engl. *Break-In*) her. 99 Prozent der befragten Verantwortlichen sehen Spyware als Möglichkeit für Daten- und Identitätsdiebstahl.

Spyware-Software kann so programmiert sein, dass sie sich gegen das Löschen schützen kann, indem mehrere Prozesse gleichzeitig laufen. Wird ein Prozess davon beendet, genieren die anderen einen neuen. Durch Spyware können zusätzliche Sicherheitslöcher in einem System erzeugt werden, die dann sicherheitsrelevante Softwareupdates verhindern. Diese Selbstschutzmechanismen machen es privaten, selbst versierten, Benutzern und IT-Administratoren schwer, sich der Spyware zu entledigen. Zum einen bieten Sicherheitssoftware-Hersteller lokale Lösungen (privat: *Ad-Aware*[98], Spybot-S&D[99], *Spyware Doctor*[100], betrieblich [Forrester, 2006]: *CA*[101], Symantec, *Sunbelt*[102], *Tenebril*[103], *Trend*

[96] Vgl. http://www.consumerreports.org/ „State of the Net“-Report [11. März 2008]
[97] Vgl. http://www.computerworld.com/ „IT Management Survey Spyware“ Dezember 2005 [27. Feber 2007]
[98] http://www.lavasoft.de/ms/ [27. Feber 2007]
[99] http://www.safer-networking.org/microsoft.en.html [27. Feber 2007]
[100] http://www.pctools.com/ [27. Feber 2007]
[101] http://www.ca.com/ [27. Feber 2007]
[102] http://www.sunbelt.com/ [27. Feber 2007]

Micro[104]) am PC gegen Spyware an, zum anderen gibt es Ansätze für Unternehmen im Perimeterbereich (siehe *1.7.2.4 Perimetersicherheit*): *File Attachment Blocking*, Intrusion Detection, *Web Content Filter etc.* Zudem werden am Markt Dienstleistungen wie *Employee Computing Risk Assessment (ECRA)*[105] angeboten, mit Hilfe derer ergänzend zur Spywarediagnose noch eine Reihe weiterer Risiken überprüft werden, die sich aus dem Surfverhalten der User ergeben (Bandbreitenverluste, Haftungsfragen, Produktivitätsminderungen). *Sophos*[106] schlägt in seinem Strategiepapier „*Solving the spyware problem*“[107] vor, Mitarbeiter entsprechend zu sensibilisieren, restriktive Sicherheitspolicies einzuführen und aktuell gehaltene Technologien – auf verschiedenen Ebenen – einzusetzen. Den Rahmen der Gegenmaßnahmen bildet die *Anti-Spyware Coalition*[108]. Diese Allianz, bestehend aus verschiedenen Interessensgruppen und Technologiefirmen, unterstützt die laufenden Bestrebungen gegen Spyware. In ihrem „*Risk Modeling Document*“ finden sich *best practice*-Ansätze zum Schutz und zur Bekämpfung von Spyware.

1.3.4.8 Erkennung von Malicious Code

Eine Infizierung durch Malware könnte vorliegen, wenn eines oder mehrere der folgenden Symptome auftreten:

- der PC startet oder funktioniert langsamer als sonst, besonders beim Surfen im Internet,
- bestimmte Aktionen am PC sind nicht mehr ausführbar,
- Symbole sehen nicht mehr so aus wie früher,
- der Zugriff auf bestimmte Dateien dauert lange,
- der Internet Explorer öffnet Werbefenster, die in keinem erkennbaren Zusammenhang zu den besuchten Websites stehen,
- die Webbrowser-Startseite wurde geändert,
- im Favoritenordner stehen Links, die nicht vom Benutzer gespeichert wurden,
- der PC verbindet sich selbständig mit dem Internet,
- die Firewall meldet Versuche von Programmen, die eine Verbindung zum Internet herstellen wollen.

[103] http://www.tenebril.com/ [27. Feber 2007]
[104] http://de.trendmicro-europe.com/ [27. Feber 2007]
[105] Vgl. http://www.bacher.at/index.php?aID=163 [27. Feber 2007]
[106] http://www.sophos.com/ [27. Feber 2007]
[107] http://www.zdnet.de/itmanager/whitepapers/0,39026292,39002442q,00.htm Feber 2007 [26. März 2007]
[108] http://www.antispywarecoalition.org/ [27. Feber 2007]

1.3.5 COMPUTERKRIMINALITÄT

Unter Computerkriminalität (engl. *Cybercrime*) werden Straftaten im Zusammenhang mit Computern verstanden. Cybercrime wird aufgrund der monetären Intentionen der Wirtschaftskriminalität zugeordnet.

Definitionen von Cybercrime (*Österreichisches Bundeskriminalamt*[109]):

„*The use of ICT to commit or further a criminal act against a person, property, organisation or the networked computer system.“*

„The criminal use of any computer network or system on the internet; attacks or abuse against the systems and networks for criminal purposes; crime and abuse from either existing criminals using new technologies, or new crimes that have developed with the growth of the internet.“

Interpol[110] publiziert auf seiner Webseite einen Straftatenkatalog, der den breiten Umfang an möglichen Delikten wiedergibt (ein Auszug):

- illegales Abhören von Datenverkehr,
- datenbezogene Wirtschaftsspionage,
- Diebstahl,
- Trojanische Pferde, Viren, Würmer,
- computerbezogener Betrug,
- Missbrauch von Geldausgabesystemen,
- Fälschung von DV-Mitteln,
- Input- und Output-Programmmanipulationen,
- (Telefon-) *Phreaking*[111],
- unautorisierte Vervielfältigung von Software (Raubkopien),
- Hardware-Sabotage,
- Software-Sabotage,
- missbräuchliche Verwendung von Nachrichtensystemen, Computern und Netzwerken zu Speicherung, Austausch oder Verteilung von strafrechtlich relevantem Material.

In der Literatur[112] weiters zu finden sind das Ausspähen von Daten, *Reverse Engineering*[113] (siehe *1.4.1 Möglichkeiten der Informationsbeschaffung*), *Cracking*, *Hacking* (siehe *1.4.3.1 Exkurs: Script*

[109] Vgl. http://www.bmi.gv.at/kriminalpolizei/ [4. März 2007]
[110] Vgl. http://www.interpol.int/Public/FinancialCrime/Default.asp [4. März 2007]
[111] Illegale Manipulation von Telefonsystemen
[112] Vgl. http://www.computerbetrug.de/ [11. März 2007]
[113] Hardwarenachbau durch spezielle Analysemethoden; Rückgewinnung des Quellcodes von einem ausführbaren Programm; Herausfinden der Regeln eines Kommunikationsprotokolls aus der Beobachtung der Kommunikation

Kiddie/Hacker/Cracker), Modifizierung von Programmen (siehe *1.3.5.4 Manipulation von Daten*), *Spamming* (siehe *1.6 Exkurs: E-Mail/Spam*) und *Cyberstalking*[114].

Price Waterhouse Coopers[115] hat eine weltweit umfassende Studie[116] über Wirtschaftskriminalität gemacht, in der belegt wird, dass der digitale Anteil im Sinne von Cybercrime deutlich an Gewicht gewinnt. Im Jahr 2005 wurden dabei 3.600 Unternehmen in 34 Ländern befragt. Einige der Ergebnisse:

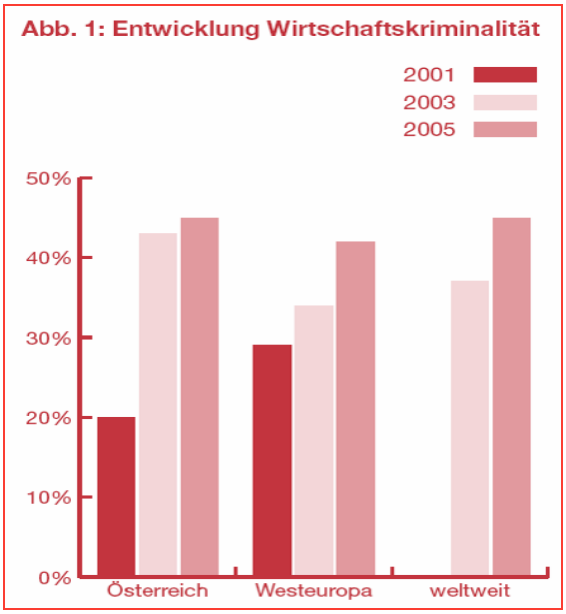


Abbildung 6: Entwicklung Wirtschaftskriminalität Österreich/Westeuropa/weltweit

- 45 Prozent der österreichischen Unternehmen wissen, dass sie in den letzten zwei Jahren durchschnittlich in sechs Fällen Opfer eines Wirtschaftsdelikts geworden sind,
- mit 30 Prozent entdeckter Fälle von Produktpiraterie und Industriespionage liegt Österreich über dem westeuropäischen (27 Prozent) und dem weltweiten (25 Prozent) Durchschnitt.

[114] http://www.cyberstalking.at/ [4. März 2007]
[115] http://www.pwc.com/ [5. Mai 2007]
[116] Vgl. http://www.pwc.com/ „Global Economic Crime Survey 2005 Österreich“ Dezember 2005 [27. Feber 2007]

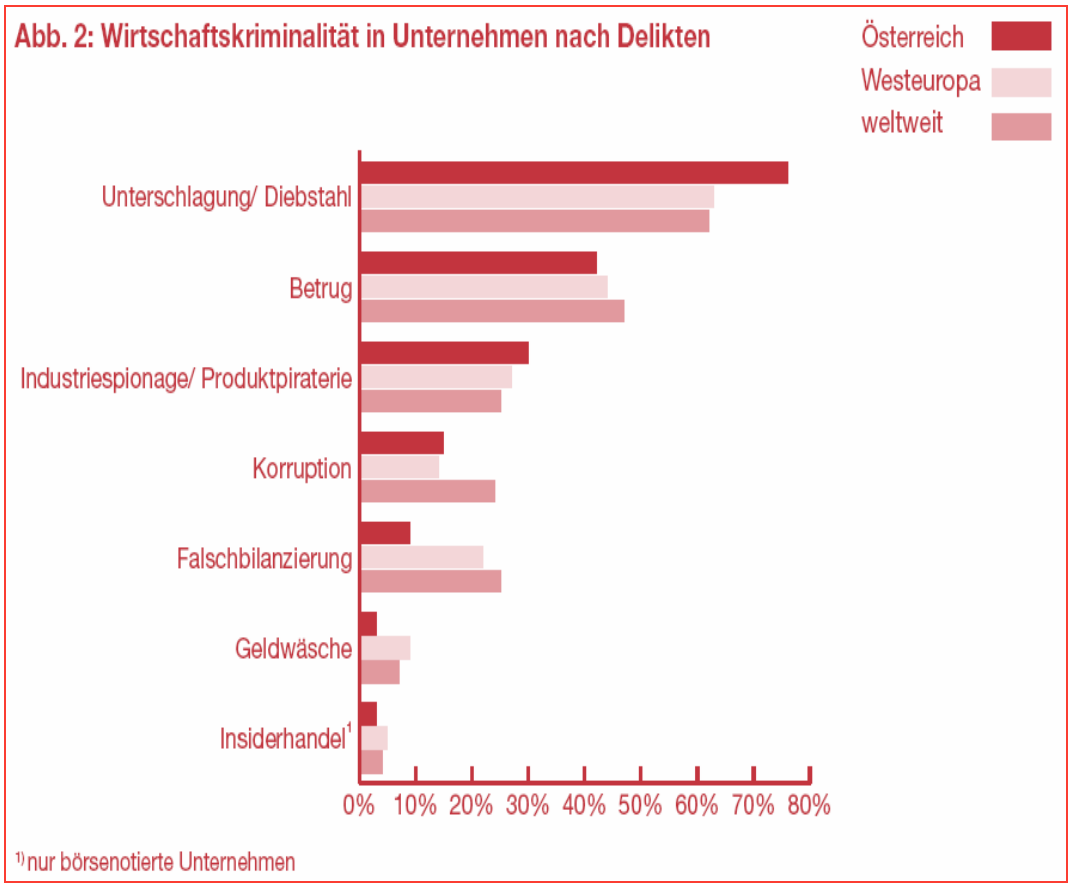


Abbildung 7: Wirtschaftskriminalität Österreich/Westeuropa/weltweit nach Delikten

Materieller Schaden

- 14 Prozent der befragten österreichischen Unternehmen erlitten einen Schaden zwischen einer und zehn Millionen Euro (Durchschnitt für Westeuropa: 11 Prozent),
- in 69 Prozent der berichteten Fälle lag der finanzielle Schaden zwischen 10.000 und 250.000 Euro (Westeuropa und weltweit 50 Prozent),
- der durchschnittliche Schaden pro geschädigtem Unternehmen betrug 3,4 Millionen Euro.

Immaterieller Schaden

- Imageverlust wiegt in Österreich schwerer als im Ausland,
- nur in 13 Prozent der berichteten Fälle erfuhr niemand außerhalb des Unternehmens von der Tat (Westeuropa 23 Prozent, weltweit 22 Prozent),
- 40 Prozent der Geschäftspartner (Westeuropa 31 Prozent, weltweit 35 Prozent) wussten, dass das Unternehmen Opfer von Wirtschaftskriminalität wurde.

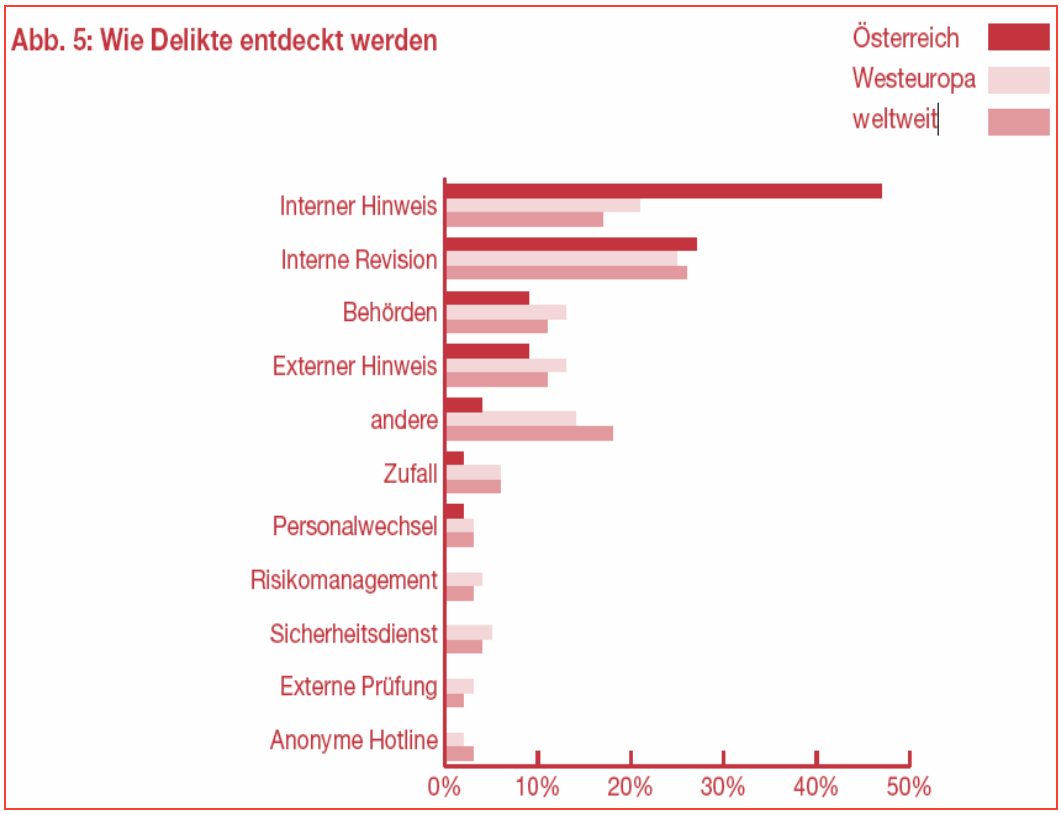


Abbildung 8: Aufdeckung Österreich/Westeuropa/weltweit der Delikte

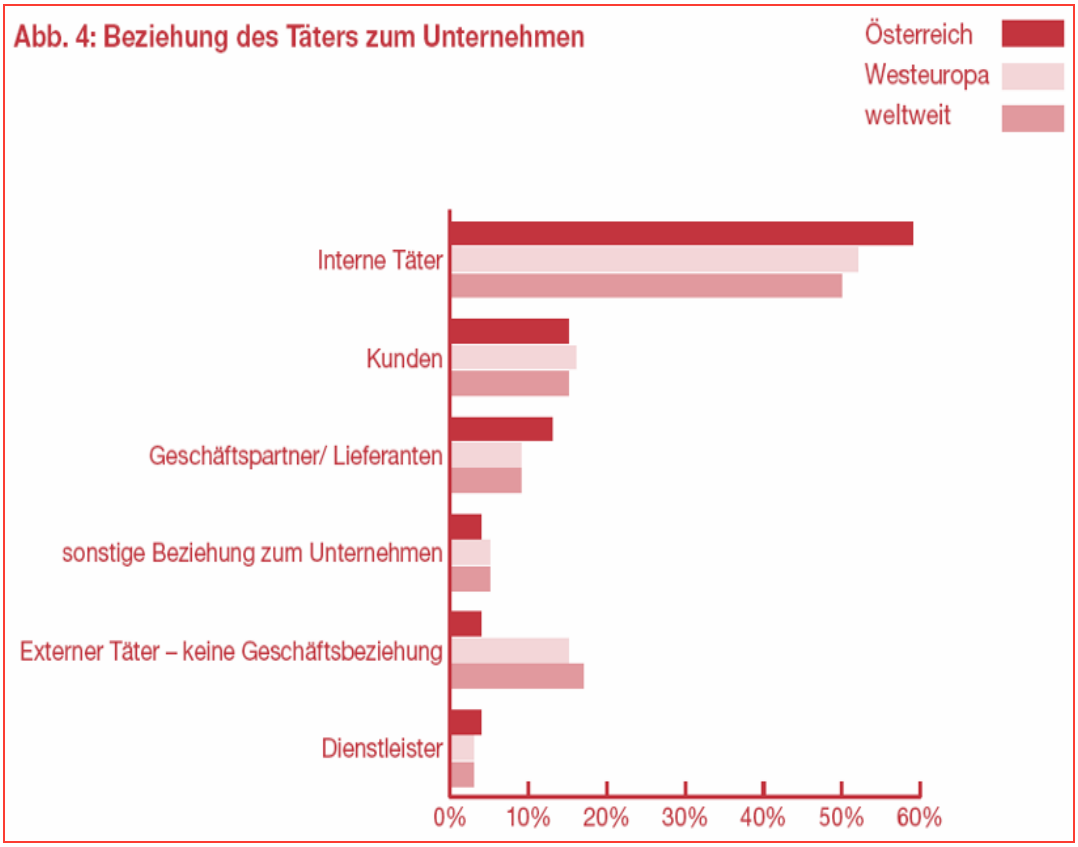


Abbildung 9: Beziehung Täter/Unternehmen Österreich/Westeuropa/weltweit

Profil des Täters:

- 60 Prozent der Täter kommen aus dem eigenen Unternehmen (Westeuropa 52 Prozent),
- 64 Prozent davon aus Topmanagement und mittlerem Management (Westeuropa 41 Prozent),
- Der typische Täter ist männlich (93 Prozent), zwischen 31 und 50 Jahre alt (73 Prozent) und überdurchschnittlich gebildet.

Motivation des Täters:

- mangelndes Werte- und Unrechtsbewusstsein,
- leichte Verführbarkeit,
- aufwendiger Lebensstil,
- unzureichende interne Kontrollen.

Der Täter ist sozial unauffällig, schwer zu identifizieren und vertrauenswürdig.

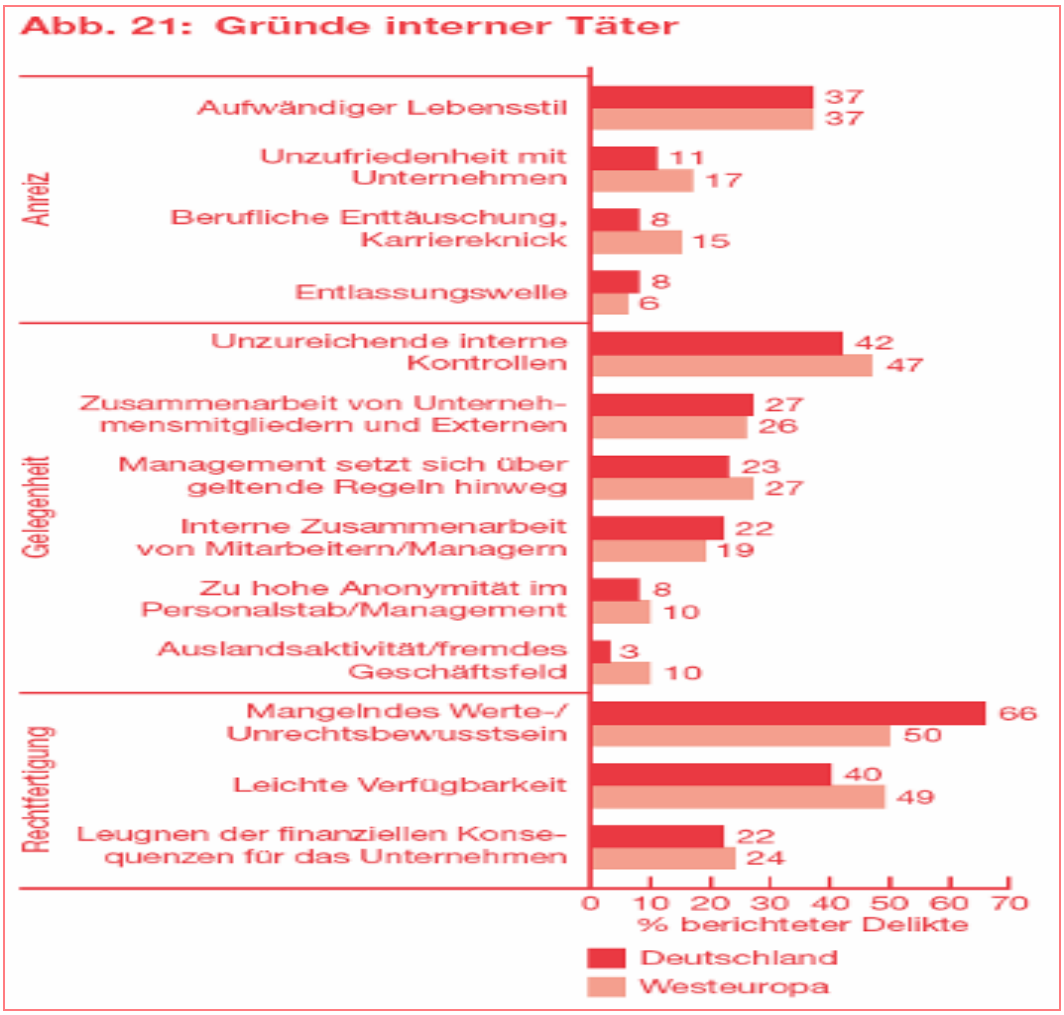


Abbildung 10: Motivation interner Täter Deutschland/Westeuropa

Daten von Cybercrime-Fällen des deutschen *Bundeskriminalamtes*[117]:

Bundeskriminalamt			
Straftaten	**erfasste Fälle**		
	2004	**2003**	**2002**
Computerkriminalität Gesamt	*66,973*	*59,691*	*57,488*
Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	36,088	35,954	36,969
Computerbetrug -§263a StGB-	14,186	11,388	9,531
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	7,357	7,003	5,902
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB-	570	237	228
Datenveränderung, Computersabotage -§§ 303a/b StGB-	3,130	1,705	1,327
Ausspähen von Daten	1,743	781	806
Softwarepiraterie (private Anwendung z.B. Computerspiele)	2,782	2,053	1,947
Softwarepiraterie in Form gewerbsmäßigen Handelns	1,117	570	780

Abbildung 11: Entwicklung der Cybercrime-Fälle in Deutschland

Um der Ausbreitung von Cybercrime entgegen wirken zu können, bedarf es internationaler Zusammenarbeit. Das Österreichische Bundeskriminalamt arbeitet vernetzt in Kooperation mit *Europol*[118], *ENFSI*[119], *Interpol* und *FBI*[120].

1.3.5.1 Rechtlicher Rahmen

1.3.5.1.1 International und Europäische Union

Maßgebend ist hier die am 23. November 2001 in Kraft getretene *Convention on Cybercrime*[121] (*Council of Europe, ETS No. 185, Budapest, 23.XI.2001*). Die Konvention ist der erste internationale Vertrag, welcher sich gegen Verbrechen über das Internet richtet [Proksch, 2006, Crime, S 12]. Dieser enthält insbesondere Bestimmungen zu

- Urheberrechtsverletzungen,
- Computerbetrug,

[117] Vgl. http://www.bundeskriminalamt.de/ [27. Feber 2007]
[118] http://www.europol.europa.eu/ [4. März 2007]
[119] http://www.enfsi.org/aboutenfsi/ [27. Feber 2007]
[120] http://www.fbi.gov/ [4. März 2007]

- Kinderpornographie,
- Netzwerksicherheitsverletzungen.

Der Vertrag enthält eine Reihe von Bestimmungen zum Verfahren respektive zu Überwachungsrechten, ebenso zur Durchsuchung und Überwachung von Computernetzen. Ergänzt wird die Konvention durch ein Zusatzprotokoll, das die Veröffentlichung fremdenfeindlicher und rassistischer Propaganda im Internet unter Strafe stellt. Das Ziel der Konvention ist in der Präambel wie folgt festgehalten: „*to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation*." Wesentliche Bestimmungen des Vertrages sind in folgenden Artikeln niedergeschrieben:

- *Article 2 – Illegal access,*
- *Article 3 – Illegal interception,*
- *Article 4 – Data interference,*
- *Article 5 – System interference,*
- *Article 6 – Misuse of devices,*
- *Article 7 – Computer-related forgery,*
- *Article 8 – Computer-related fraud,*
- *Article 9 – Offences related to child pornography,*
- *Article 10 – Offences related to infringements of copyright,*
- *Article 11 – Attempt and aiding or abetting,*
- *Article 12 – Corporate liability.*

1.3.5.1.2 Österreich

Der rechtliche Rahmen in Österreich wird im Wesentlichen in einzelnen Paragraphen der angeführten Gesetze, insbesondere im Strafrecht, abgesteckt [Proksch, 2006, Crime, S 6f].

- *Staatsgrundgesetz* (kurz: *StGG*)[122],
- *Zugangskontrollgesetz* (kurz: *ZuKG*)[123]: *§10,*
- *E-Commercegesetz* (kurz: *ECG*)[124]: *§§13ff ECG Providerhaftung, §18 Mitwirkungspflicht,*
- *Datenschutzgesetz* (kurz: *DSG 2000*)[125]: *§51 und §52,*
- *Urheberrechtsgesetz* (kurz: *UrhG*)[126]: *§§91 ff,*
- *Telekommunikationsgesetz* (kurz: *TKG*)[127]: *§89 TKG Mitwirkungspflicht,*

[121] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [11. Feber 2007]
[122] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: STGG [11. Feber 2007]
[123] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Zugangskontrollgesetz §10 [11. Feber 2007]
[124] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: ECG §13, §19 [11. Feber 2007]
[125] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: DSG §51, §52 [11. Feber 2007]

- *Strafgesetzbuch* (kurz: *StGB*)[128]:
  - *§118a StGB Widerrechtlicher Zugriff auf Computersysteme,*
  - *§119 StGB Verletzung des Telekommunikationsgeheimnisses,*
  - *§119a StGB Missbräuchliches Abfangen von Daten,*
  - *§126a StGB Datenbeschädigung,*
  - *§126b StGB Störung der Funktionsfähigkeit eines Computersystems,*
  - *§126c StGB Missbrauch von Computerprogrammen oder Zugangsdaten,*
  - *§148a StGB Betrügerischer Datenverarbeitungsmissbrauch,*
  - *§225 StGB Fälschung von Computerdaten (Identitätsbetrug).*

1.3.5.2 Datendiebstahl und Spionage

Gegenstand dieser Bedrohungen sind nur für autorisierte Personen bestimmte Informationen, die in nicht berechtigtem Besitz Gefahr von Missbrauch bergen. Dazu gehören beispielsweise Daten wie Kontenangaben bzw. Informationen über bevorstehende Fusionen oder neue Produkte. Aus den vom deutschen Bundeskriminalamt erfassten Daten (siehe *Abbildung 11: Entwicklung der Cybercrime-Fälle in Deutschland*) geht hervor, dass beim „Ausspähen von Daten“ 2004 ein Wachstum von 223 Prozent zu verzeichnen ist: während im Jahr 2003 781 Fälle erfasst wurden, steigerte sich die Zahl im Jahr 2004 auf 1.743. Mit Trojanern (siehe *1.3.4.5 Trojanisches Pferd*) sowie Sniffer- (siehe *1.4.2.4 Sniffing*) und Spoofing- (siehe *1.4.3.6 Spoofing*) Technologien gibt es einige Möglichkeiten zur Durchführung von Datenspionage. Neuere Daten aus dem Jahr 2006 für Deutschland[129] bestätigen einen weiteren Anstieg der Datenspionage gegenüber 2005 von 26,4 Prozent. Hinzu kommen über 2,6 Millionen Diebstahldelikte, zu denen auch gestohlene elektronische Geräte mit teilweise brisanten, vertraulichen Informationen gezählt werden.

Ein Bericht[130] der *Universität von Washington*[131] besagt, dass 2007 allein in den USA zwei Milliarden sensible Daten in *falschen Händen* sind. Als besonders besorgniserregend werten die Forscher zudem den Umstand, dass allein in den Jahren 2005 und 2006 mehr Vorfälle zu verzeichnen waren als die 25 Jahre vorher zusammen. Als Hauptverantwortliche werden nicht Angriffe von Cyberkriminellen, sondern schlichtweg die Nachlässigkeit von Unternehmen und Anwendern identifiziert. Mehr als sechzig Prozent der Vorfälle gehen dabei nicht auf Angriffe von außen, sondern auf Unachtsamkeiten der Datenverwalter zurück. So zählen sowohl das versehentliche Online-Stellen von Daten, das

[126] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Urheberrechtsgesetz §91 [11. Feber 2007]
[127] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: TKG §89 [11. Feber 2007]
[128] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Strafgesetzbuch §118, §119, §126, §148 [11. Feber 2007]
[129] http://www.bmi.bund.de/cln_012/nn_121894/Internet/Content/Broschueren/2007/Polizeiliche__Kriminalstatistik__2006__de.html [27. Mai 2007]
[130] http://jcmc.indiana.edu [10. Juni 2007]
[131] http://www.washington.edu/ [10. Juni 2007]

Verlieren von Hardware und Datenträgern sowie andere Verwaltungsmissverständnisse zu den häufigsten Ursachen für den steigenden Datenverlust.

Es gibt zwei Möglichkeiten: einerseits, dass Personen berechtigten Zugang zu den Informationen haben (z. B.: Mitarbeiter), andererseits sich diesen unberechtigterweise verschaffen. Im ersten Fall ist ein angemessener Schutz schwierig. Eine Umfrage (Mai 2007) im Auftrag des Security-Spezialisten Websense hat ergeben, dass 36 Prozent der Befragten die eigenen Mitarbeiter für den Verlust von Daten verantwortlich machen. *Personal Recruiting*, Mitarbeiterschulung, Maßnahmen im Bereich der Client Security, Berechtigungsvergabe, Verschlüsselung sind hier nahe liegende Schutzvarianten (siehe *1.7 Schutzmaßnahmen und Gegenstrategien*). Gegen externe Angreifer ist physischer und virtueller Zutrittsschutz unerlässlich (siehe *1.7.1 Organisatorische Gegenmaßnahmen* und *1.7.2 Technische Gegenmaßnahmen*).

1.3.5.2.1 Mobile Geräte

Einen Problemkreis stellen mobile Geräte (engl. *Mobile Devices*), wie Notebooks, Personal Digital Assistants (kurz: PDA), aber auch (speicherfähige) Hardware wie USB-Sticks, *MP3*[132]*-Player*, Digitalkameras oder Mobiltelefone dar.

Nach einer Untersuchung des britischen Securityspezialisten *Centennial Software*[133] wird das Risiko, das von USB-Sticks, *iPods* oder anderen tragbaren Speicherlösungen ausgeht, weitgehend unterschätzt. 87 Prozent der befragten Unternehmen prüfen nicht einmal den Einsatz tragbarer Speicher in ihren Büros, obwohl sich über die Hälfte durchaus der Gefahren bewusst sind – angefangen von versehentlich eingeschleppten Viren bis hin zum Datendiebstahl. Wie leicht es ist, große Datenmengen unbemerkt zu entwenden, zeigt das Beispiel eines ehemaligen AOL-Mitarbeiters, der 92 Millionen E-Mail-Adressen von Kunden gestohlen und an Spammer weiterverkauft hatte. Ein einfaches, mit entsprechendem Speicher ausgestattetes Musikabspielgerät reicht, um innerhalb von wenigen Minuten Gigabyte wertvoller und vertraulicher Daten von einem Netzwerk zu stehlen. Während in den technischen Schutz vor Viren, Spam und andere Bedrohungen viel Knowhow und Geld investiert wird, fehlen in den meisten Firmen Richtlinien, die den Gebrauch von externen Speichermedien regeln.

Nach einem Bericht [Landesk, 2005] des Sicherheitsspezialisten *LANDesk*[134] stellen das Eindringen von Malware ins Netzwerk und der Datendiebstahl die größten Sicherheitsbedrohungen für Unternehmen dar. Fast ein Viertel der europäischen IT-Manager beklagt, sie könnten die Benutzung privater mobiler Geräte im Unternehmen nicht unterbinden. Obwohl diese Geräte eine echte

[132] MP3 (steht für: Moving Picture Experts Group (kurz: MPEG oder MP) Audio Layer 3) ist ein Dateiformat zur Audiodatenkompression.
[133] Vgl. http://www.centennial-software.com/company/news/?id=63 Dezember 2005 [27. Feber 2007]
[134] http://www.landesk.de/ [17. März 2008]

Bedrohung darstellen, will bzw. kann sie nur jeder Fünfte (19 Prozent) aus dem Unternehmensnetzwerk verbannen.

In den vergangenen Jahren ist eine deutliche Zunahme der Diebstähle mobiler Geräte zu verzeichnen. Sie enthalten neben wichtigen Geschäftsdaten oft auch Zugangsinformationen für das interne Netzwerk.

Ein Bericht[135] in der Onlineversion von Computerworld spiegelt die Situation im Bereich Daten- bzw. Gerätediebstahl und die (fehlenden) Konzepte der Unternehmen wider: „*Companies are struggling to protect hardware and data. Loss of confidential data – including intellectual property, business documents, customer data and employee records – is a pervasive problem among U.S. companies. 81 Percent of companies surveyed reported the loss of one or more laptops containing sensitive information during the past 12 months, according to the survey, which queried nearly 500 information security professionals.“*

Einer der Hauptgründe für Datendiebstahl ist demnach*: „*[…] *is because companies don't know where their sensitive or confidential business information resides within the network or enterprise systems. This lack of knowledge, coupled with insufficient controls over data stores, can pose a serious threat for both business and governmental organizations. Moreover, the danger doesn't stop at the network, but includes employees' and contractors' laptop computers and other portable storage devices.“*

Mit „*No idea*“ hat die Mehrheit der Befragten auf „*How long would it take to determine what actual sensitive data was on a lost or stolen laptop, desktop, file server or mobile device?“* geantwortet.

Zusammenfassend stellt das untersuchende Institut fest: *„Corporations are clearly struggling with the challenges of identifying and protecting sensitive data, as well as developing successful strategies for securing confidential information stored among the myriad devices that make up today's data networks. The findings point to the shockingly high risk to both business and consumers of undiscovered confidential data, but the data also serve as a compass to help point organizations toward effective solutions to this vexing problem.“*

Unternehmen ergreifen außergewöhnliche Maßnahmen, indem sogar Prämien ausgesetzt werden, um verloren gegangene Geräte und Daten wieder zu finden[136]: “*Unisys Corp., working with the Office of the Inspector General of the U.S. Department of Veterans Affairs (VA) and the FBI, is offering a reward of up to $50,000 for information leading to the recovery of a missing desktop computer that belongs to the VA. The computer, which contains personal information on 38,000 veterans treated at VA medical facilities in Philadelphia and Pittsburgh, went missing from the Reston, Va., office of Unisys, the subcontractor hired to assist in insurance collection for those facilities.”* oder *“Chevron Corp. is searching for a password-protected laptop stolen from an independent accounting firm*

[135] Vgl. http://www.computerworld.com/ „Survey: 81 Prozent of U.S. firms lost laptops with sensitive data in the past year“ 16. August 2006 [15. März 2008]

working for it. The laptop contained the names and Social Security numbers of an undisclosed number of current and former Chevron employees. Chevron is taking steps to avoid any recurrence, including reviewing and enhancing our security procedures for sharing information with outside accounting firms. "

1.3.5.3 Identitätsdiebstahl

Definition[137]:

„*Identity theft or identity fraud is the taking of the victim's identity to obtain credit, credit cards from banks and retailers, steal money from the victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file bankruptcy or obtain a job using the victim's name. The Impersonator steals thousands of dollars in the victim's name without the victim even knowing about it for months or even years. Recently criminals have been using the victim's identity to commit crimes ranging form traffic infractions to felonies."*

Identitätsdiebstahl (engl. *Identity Theft*) ist eine spezielle Form des Datendiebstahls. Als Identitätsdiebstahl wird die unerlaubte Aneignung und missbräuchliche Verwendung personenbezogener Daten durch Dritte bezeichnet. Bei einem Identitätsdiebstahl eignet sich der Täter persönliche Daten wie Name, Anschrift, Sozialversicherungs-, Bankkonto-, Kreditkartennummer oder Zugangsdaten an, um eine Identitätsabfrage zu umgehen oder diese zu fälschen. Identitätsdiebstahl ist eine der am stärksten zunehmenden Kriminalitätsformen in hoch technisierten Ländern. Die am häufigsten auftretenden Formen sind Kreditkartenbetrug und Kontenraub. Insbesondere im E-Commerce, etwa beim Durchführen von Transaktionen bei eBay, kann Identitätsdiebstahl erhebliche Auswirkungen haben. Geschädigte durch Identitätsdiebstahl wehren sich nach Bekanntwerden der Straftat am effektivsten durch eine Strafanzeige – typischerweise – „gegen Unbekannt" bei der Polizei. Angreifer manipulieren durch Zuhilfenahme von Techniken wie Phishing (siehe *1.4.1.2 Exkurs: Phishing*), Pharming (siehe *1.4.1.2.1 Pharming*) oder Spoofing (siehe *1.4.3.6 Spoofing*) die Computer der jeweiligen Zielpersonen und bemächtigen sich damit deren Identität (Benutzerkennung, Passwort). Mit dieser gestohlenen Identität verschaffen sie sich Zugang zu diversen Diensten und Webseiten, um die gewonnenen Daten selbst zu nutzen bzw. Interessierten zukommen zu lassen oder zu verkaufen.

Das amerikanische *Department of Justice* (deutsch: Justizministerium)[138] berichtet, dass im Jahr 2004 in den USA ein geschätzter Schaden von 6,4 Milliarden Dollar durch Identitätsdiebstahl entstanden ist. 3,6 Millionen (3 Prozent) der amerikanischen Haushalte haben demnach im ersten Halbjahr 2004 finanziellen Schaden durch Identitätsdiebstahl erlitten. Beinahe die Hälfte dieser Fälle ging der Statistik zufolge auf Missbrauch von Kreditkartendaten zurück. Bei 25 Prozent der Opfer habe das

[136] Vgl. http://www.computerworld.com/ „Unisys offers $50,000 reward for missing VA computer" 16. August 2006 [2. März 2008]
[137] Vgl. http://www.identitytheft.org/ [2. März 2008]

Erschleichen von Onlinebanking-Daten eine Rolle gespielt. Das *Department of Justice* befragte dafür rund 42.000 amerikanische Haushalte (Hinweis: In dem seit 30 Jahren erscheinenden Report wurde erstmalig Identitätsdiebstahl als eigenständige Deliktkategorie aufgenommen).

In einem Report[139] (Jänner 2007) der Sicherheitsexperten von McAfee wird von einem starken Anstieg beim Identitätsdiebstahl berichtet. Allein zwischen Jänner 2004 und Mai 2006 habe sich die Zahl der gemeldeten Phishing-Alarme und Keylogger verhundertfacht.

Während die Diebstahlszahlen in den USA auf hohem Niveau sind, steht in Österreich ein Anstieg der Schadensfälle noch bevor. „*Im Jahr 2006 waren nach unseren Schätzungen etwa 3.000 Österreicher Opfer eines Identitätsdiebstahls*“, erklärt ein Vertreter von *Arge Daten*[140].

Der folgende Artikel schildert den Sachverhalt eines Identitätsdiebstahls und die Rechtsfolgen am Beispiel eBay Deutschland vom 28.11.2005[141]:

„*Am 16. November 2005 hat das Brandenburgische Oberlandesgericht in einer Entscheidung (Az. 4 U 5/05) die Berufung der eBay International AG gegen ein Urteil des Potsdamer Amtsgerichts (AG) zurückgewiesen. Dabei ging es um die Verpflichtung der Marktplatzbetreiber, Maßnahmen gegen Identitätsdiebstahl zu treffen. Damit konnte eBay seine Rechtsauffassung, nach der das übliche Verfahren bei der Anmeldung neuer eBay-Accounts bereits ausreichende Sicherheit vor Missbrauch biete, auch in der zweiten Instanz nicht durchsetzen.“*

Die Chronologie des Falls sieht wie folgt aus: *„*[…] *Mitte November 2003 stellte ein eBay-Teilnehmer fest, dass unter seinem Namen, aber mit einem fremden Account Pullover auf der Online-Handelsplattform feilgeboten und Kunden mit mangelhafter Ware oder gänzlichem Ausbleiben von Lieferungen über den Tisch gezogen wurden. Der Inhaber der missbrauchten Daten sah seine Namensrechte sowie seine allgemeinen Persönlichkeitsrechte durch den Accountmissbrauch verletzt und machte die mangelnde Identitätsüberprüfung bei der Einrichtung neuer eBay-Accounts für die bereits mehrfach in den Medien gemeldete Form des Online-Auktionsbetrugs mit Fake-Accounts mitverantwortlich. Er forderte eBay daher auf, Maßnahmen zu treffen, die mögliche Wiederholungen unterbinden sollten. Mit einer Abmahnung vom Januar 2004 forderte der eBay-Nutzer die Abgabe einer strafbewehrten Unterlassungserklärung. Die Plattformbetreiber wiesen das jedoch von sich, woraufhin er beim AG Potsdam im Februar 2004 eine einstweilige Verfügung gegen eBay erwirkte, die dasselbe Gericht im Dezember 2004 mit einem Urteil im Hauptsacheverfahren bestätigte. Die Berufung der Plattformbetreiber gegen das AG-Urteil führte zum zweitinstanzlichen Verfahren vor dem OLG.“*

[138] http://www.ojp.usdoj.gov/bjs/cvict.htm [27. Feber 2007]
[139] Vgl. http://www.harvard.de/pressemeldungen/McAfee/2007/6-avert-id-thft-001-0107s_DE.pdf Jänner 2007 [26. März 2007]
[140] Vgl. http://www.argedaten.at/ [4. März 2007]
[141] Vgl. http://www.heise.de/newsticker/meldung/66719 [4. März 2007]

eBay setzte sich zur Wehr: *„*[…] *da der letzte bekannt gewordene Versuch des Identitätsdiebstahls gescheitert ist, zeige, dass die ergriffenen Maßnahmen zur Missbrauchsverhinderung effektiv seien.* […] *§11 des Teledienstegesetzes neuer Fassung ist anzuwenden, der sicherstelle, dass es für Betreiber von Telediensten keine vorbeugenden Prüfpflichten gebe. Dieses Haftungsprivileg befreit Provider von der Verantwortung für fremde rechtswidrige Informationen, die sie unwissentlich speichern und verfügbar machen.“*

Konter und Replik des Gerichts: *„*[…] *diese Regelung ist auf den vorliegenden Fall nicht anwendbar.* […] *die Haftung des Diensteanbieters muss sich entsprechend §8 Abs. 1 Teledienstegesestz nach den allgemeinen Gesetzen richten: dass bedeutet, dass die Such- und Überwachungspflicht an bestimmte Voraussetzungen gebunden ist. Der von eBay zugelassene mehrfache Identitätsklau verletze das Namensrecht des Klägers. Die Betreiber der Handelsplattform hat seine Prüfungspflicht verletzt, dadurch müsse das Unternehmen haften.“*

Es gibt viele Bestrebungen und Überlegungen, Identitätsdiebstahl so schwer wie möglich zu machen. Die US-Bundesbehörde *Federal Bureau of Investigation* (kurz: FBI) startete etwa im Herbst 2006 eine Operation namens *„Identity Shield“*[142]. Das Projekt widmet sich der Bekämpfung von Identitätsdiebstahl, insbesondere durch Phishing. Interessant ist dabei, dass das FBI offensiv auf die Hacker zugeht und diese zur Kooperation auffordert. Die Sensibilisierung für das Thema Identitätsdiebstahl ist noch nicht ausreichend vorhanden und muss weiter forciert werden.

1.3.5.4 Manipulation von Daten

Während die Daten beim Diebstahl unverändert bleiben, finden bei der Manipulation Veränderungen statt.

Die Motive für derartige Handlungen reichen von Bereicherung über Schädigung bis hin zur Zerstörung. Ein mögliches Schadensszenario ist der Geldtransfer von einem fremden auf ein eigenes Konto. Bei Vorfällen mit Bereicherungsmotiv ist es zuweilen möglich, den Täter zu identifizieren. Schwieriger ist dies bei Schädigungs- oder Zerstörungsmotiven. Frustration aufgrund Entlassung oder pure Zerstörungslust können hier Antriebsfedern sein. Mit Zerstörungen sind in aller Regel Löschvorgänge verbunden. Eine technische Methode stellen sogenannte *logische Bomben* dar: hier werden Programme in ein System eingeschleust, die im Falle eines bestimmten Ereignisses (z. B.: markantes Datum) ihre Zerstörungskraft entfalten.

[142] http://www.computerworld.com/ „Black Hat: New industry-FBI initiative targets identity theft“ 2. August 2006 [12. März 2008]

1.3.5.5 Exkurs: Computer Forensik

Bei der Computer Forensik[143] geht es um die Untersuchung und Beweismittelsicherung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen bzw. der darauf gespeicherten Daten. Dabei werden „digitale Spuren“ analysiert und ausgewertet, um den Sachverhalt festzustellen.
Die zunehmende Computerkriminalität hat zu einem Anstieg von Gerichtsprozessen geführt, in denen digitale Daten als Beweismittel eine zentrale Rolle spielen. Gerichte stehen vor dem grundlegenden Problem, in welcher Form digitale Daten als strafrechtlich relevante Beweismittel zu sichern sind.
Damit die Ergebnisse anerkannt und verwertbar werden, gilt es gewisse Prinzipien zu beachten:

- Protokollierung,
- Datenverluste minimieren,
- Sicherstellen der Beweismittelintegrität durch ein forensisch korrektes Abbild der elektronisch gespeicherten Daten,
- Analysen nur auf Kopien durchführen,
- Rechtmäßigkeit der Untersuchungsmittel und -methodik,
- Vieraugenprinzip,
- neutrale, sachlich fundierte und nachvollziehbare Berichterstattung .

Die Ziele einer forensischen Analyse nach einem Übergriff (Cracker, Computersabotage, Datendiebstahl etc.) bzw. zivilrechtlichen Verfahren (Zivilstreitigkeiten, Scheidung, Konkursverfahren, medizinische Fehlentscheidungen, Nachlassregelungen etc.) sind

- die Identifikation des Angreifers, Täters oder Betroffenen,
- das Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch oder der Straftat geführt haben könnte,
- die Ermittlung des entstandenen Schadens nach einem Systemeinbruch bzw. anderen (strafbaren) Handlungen,
- die Sicherung der Beweise und Daten für weitere juristische Aktionen (siehe oben).

1.4 UNBERECHTIGTE INFORMATIONSBESCHAFFUNG UND UNBERECHTIGTER ZUGRIFF

1.4.1 MÖGLICHKEITEN DER INFORMATIONSBESCHAFFUNG

Zur Vorbereitung eines Angriffs auf ein System ist es zunächst notwendig, Informationen darüber zu sammeln. Je mehr Informationen ein Angreifer über ein System erlangt, umso höher ist die Wahrscheinlichkeit für einen erfolgreichen Angriff.

Es gibt viele Möglichkeiten, an Daten zu kommen. So können Angreifer beispielsweise über Veröffentlichungen in der Fachpresse, durch die Analyse der HTML-Quelltexte der Unternehmenswebseite oder *Hintergehen* von Menschen Informationen gewinnen. Besonderes Augenmerk gilt dem Ausspähen von Zugangsdaten für Onlinegeschäfte, im Speziellen für den Bankenbereich.

1.4.1.1 Social Engineering

Unter *Social Engineering* wird das Ausnutzen der „Schwachstelle Mensch“ verstanden, um an wesentliche Informationen zu kommen. Das Ziel ist, die getäuschte Person zu einer bestimmten Handlung zu bewegen, die dem Angreifer beispielsweise den Zugang zu einem geschützten Computersystem ermöglicht [Feiler, 2006, S 1].

Ein derartiger Angriff könnte darin bestehen, sich als EDV-Administrator auszugeben und den Mitarbeiter aufzufordern, seine Logindaten bekannt zu geben.

„*Die Menschen sind die großen Schwachstellen im Sicherheitsmanagement. Ein guter Hacker braucht kein großer Techniker zu sein. Es genügt, wenn er ein guter Lügner ist. (Anm.: frei nach Kevin Mitnick, einen der berühmtesten Vertreter der Hackergemeinschaft)*“, stellt der *Chief Information Security Officer* (kurz: *CISO*) *Johannes Mariel*[144] vom *Österreichischen Bundesrechenzentrum*[145] fest. Täter machen sich oft die Hilfsbereitschaft und Ahnungslosigkeit von Mitarbeitern zu Nutze. Besonders perfid ist das *Reverse Social Engineering*, bei dem Angreifer in das System eindringen, Fehler produzieren und danach als „rettende Engel“ auftreten.

Die Verwendung der Social Engineering-Technik hat wesentlich zum „Erfolg“ des „*LoveLetter*“-Virus[146] im Mai 2000 beigetragen. Die Betreffzeile „*I Love you*" verleitete – mitten im Frühling – die Empfänger dazu, die vermeintliche Liebesbotschaft zu öffnen. Einige erfolgreiche Nachfolger des LoveLetter-Virus (z. B.: *Sober*[147]) waren durch die Verwendung der Reizwörter „Gratis WM-Tickets“ (Anm.: Fußballweltmeisterschaft 2006 in Deutschland) oder „Klassentreffen“ ähnlich erfolgreich.

Das Sozialportal MySpace wurde mit einem alten Trick gehackt[148]: „[…] *Two teenagers were arrested here on Long Island for hacking into a female acquaintance's MySpace account.* […] *Using an old social engineering ruse, they sent the victim an E-Mail stating that another „user" had a similar MySpace page to hers and that the victim's pictures and info were on it. In their E-Mail they conveniently sent her a "link" (bogus, of course) that she could clicked on to take her to the fake MySpace login page. At that point once she entered her login information the two teens were able to*

[143] Vgl. http://www.computerforensik.org/ [27. Feber 2007]
[144] Vgl. Persönliche Notizen von der Konferenz „Sicherheitsmanagement mit Schwerpunkt Identity Management“ [10.11.2004, BRZ, Wien]
[145] http://www.brz.gv.at/ [27. Feber 2007]
[146] Vgl. http://www.bsi.bund.de/av/vb/ll_beschr.htm [7. März 2007]
[147] Vgl. http://www.bsi.bund.de/av/vb/soberq10062005.htm [7. März 2007]

capture her password data and with it they logged into her account and posted inappropriate material on her real page. Social engineering attacks are hard to combat and all the security in the world will not help when you open the door and invite the hacker in!"

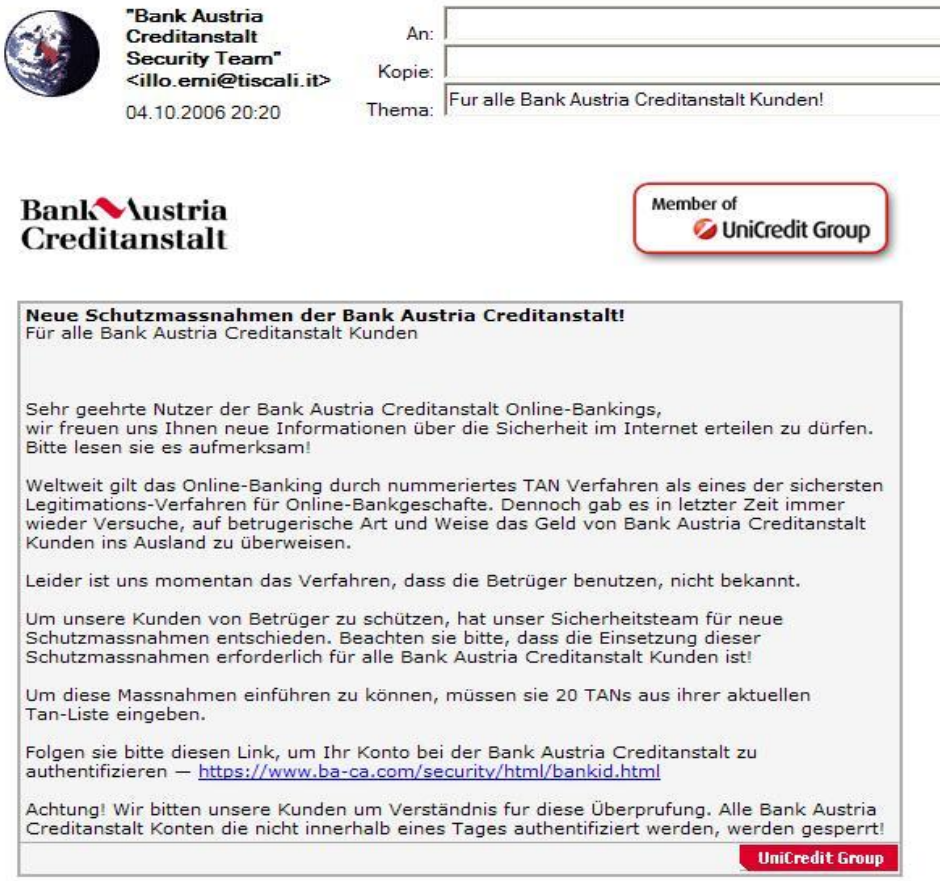
Die Sensibilisierung der User (siehe *1.8.3 Der Faktor Mensch*) ist der geeignetste Weg, Informationsverlust durch Social Engineering zu verhindern.

1.4.1.2 Exkurs: Phishing

Phishing[149] (Kunstwort zusammengesetzt aus „*Password*" und „*fishing*") steht für eine Form der Täuschung und des Onlinebetrugs mit dem Ziel, Informationen (Zugangsdaten, Kreditkartendaten etc.) zu stehlen. Dabei werden Social Engineering-Techniken eingesetzt, der Empfänger soll durch vertrauensbildende Maßnahmen oder emotionale Einbindung zur Herausgabe von Zugangsdaten bewegt werden. Verwendung findet diese Art des Diebstahls beim Onlinebanking, bei Bezahlportalen, Versandhäusern oder Internet-Auktionshäusern. Übermittelt der gutgläubige Benutzer Daten an den Betrüger, kann dieser die Identität seines Opfers übernehmen (siehe *1.3.5.3 Identitätsdiebstahl*) und mit den *gephisten* Zugangsdaten eine Geldüberweisung oder eine Warenbestellung zu Lasten des Opfers durchführen. Durch den Missbrauch der persönlichen Daten können beträchtliche Schäden in Form von Vermögensverlust oder Rufschädigung entstehen.

Es gibt eine Reihe von internationalen wie auch nationalen Phishing-Attacken. Als Beispiel wird eine Attacke auf die *Bank Austria Creditanstalt (BA-CA)*[150] vom Oktober 2006 beschrieben. Der Zeitpunkt war optimal gewählt, nachdem einige Tage zuvor die BA-CA mit dem Thema „Reduzierung des Sicherheitsrisikos beim Onlinebanking durch Beschränkung der Höhe einer Online-Transaktion auf 1.500 Euro" prominent in den Medien[151] vertreten war. Oft bleibt den Betroffenen nur der Hinweis auf „BA-CA", „Sicherheit" und „Onlinebanking" in Erinnerung. Unter den Bedingungen, dass man Kunde bei der Bank ist, diese Information aus den Medien im Hinterkopf hat und nicht allzu sehr auf Security sensibilisiert ist, erscheint folgende E-Mail formal und inhaltlich plausibel (Anm.: nahezu fehlerfrei, Logo, Absender etc.):

[148] Vgl. http://www.computerworld.com/blogs/node/3239 [10. März 2008]
[149] Vgl. http://www.securityinfo.ch/phising.html [7. März 2007];
http://www.bsi-fuer-buerger.de/phishing/index.htm [7. März 2007]
[150] http://www.ba-ca.com/ [6. März 2007]
[151] Vgl. http://futurezone.orf.at/it/stories/141197/ [6. März 2007]


"Bank Austria Creditanstalt Security Team" <illo.emi@tiscali.it>
04.10.2006 20:20
An:
Kopie:
Thema: Fur alle Bank Austria Creditanstalt Kunden!

Bank Austria Creditanstalt

Member of UniCredit Group

Neue Schutzmassnahmen der Bank Austria Creditanstalt!
Für alle Bank Austria Creditanstalt Kunden

Sehr geehrte Nutzer der Bank Austria Creditanstalt Online-Bankings,
wir freuen uns Ihnen neue Informationen über die Sicherheit im Internet erteilen zu dürfen.
Bitte lesen sie es aufmerksam!

Weltweit gilt das Online-Banking durch nummeriertes TAN Verfahren als eines der sichersten Legitimations-Verfahren für Online-Bankgeschafte. Dennoch gab es in letzter Zeit immer wieder Versuche, auf betrugerische Art und Weise das Geld von Bank Austria Creditanstalt Kunden ins Ausland zu überweisen.

Leider ist uns momentan das Verfahren, dass die Betrüger benutzen, nicht bekannt.

Um unsere Kunden von Betrüger zu schützen, hat unser Sicherheitsteam für neue Schutzmassnahmen entschieden. Beachten sie bitte, dass die Einsetzung dieser Schutzmassnahmen erforderlich für alle Bank Austria Creditanstalt Kunden ist!

Um diese Massnahmen einführen zu können, müssen sie 20 TANs aus ihrer aktuellen Tan-Liste eingeben.

Folgen sie bitte diesen Link, um Ihr Konto bei der Bank Austria Creditanstalt zu authentifizieren — https://www.ba-ca.com/security/html/bankid.html

Achtung! Wir bitten unsere Kunden um Verständnis fur diese Überprufung. Alle Bank Austria Creditanstalt Konten die nicht innerhalb eines Tages authentifiziert werden, werden gesperrt!

UniCredit Group

Abbildung 12: Beispiel eines Phishing-Mail

Der Empfänger wird dazu verleitet, dem auf eine gefälschte Webseite führenden Internetlink zu folgen. Werden auf dieser Seite die vertraulichen Kontodaten eingegeben, „fischen“ die Betrüger diese Informationen ab und greifen selbst auf das Konto zu.

Eine vom *Bundesministerium für Soziales und Generationen*[152] in Auftrag gegebene Studie [ARGE Daten, 2007] über die Onlinebanking-Angebote österreichischer Banken bestätigt deren sicherheitstechnische Absicherungsmaßnahmen mit dem gleichzeitigen Appell für deren Verbesserung. Problematisch sehen die Studienautoren die Qualitätsunterschiede bei den verwendeten TAN-Verfahren. Viele Banken verwenden noch heute (Dezember 2006) ein veraltetes, damit technisch unsicheres TAN-Verfahren. Kritisch werden auch die Aufklärungsarbeit und die Vorgangsweise vieler Banken gesehen, das Risiko im Zweifelsfall an ihre Kunden weiterzugeben.

Der bislang größte (publizierte) Online-Bankraub hat in Schweden stattgefunden[153]. Von 250 Kunden der *Bank Nordea*[154] wurden mittels Phishing-Attacken über einen Zeitraum von 15 Monaten rund

[152] http://www.bmsg.gv.at/ [5. Mai 2007]
[153] Vgl. http://www.pressetext.at/pte.mc?pte=070122017 [26. März 2007]
[154] http://www.nordea.com/ [27. Feber 2007]

900.000 Euro erbeutet. Die Bank hat die Fakten von sich aus im Jänner 2007 veröffentlicht, um eine weitere Sensibilisierung bei den Usern zu erreichen.

Den meisten Benutzern ist inzwischen bewusst, dass sie Passwörter und sensible Informationen nicht via E-Mail senden sollten. Deshalb wird in derartige E-Mails ein Link eingebaut, der auf die vermeintliche Bankseite verweist (siehe am Beispiel *Phishing-Attacke Bank Austria*). Um die Benutzer zu täuschen, werden ganze Webseiten nachgebaut, die mit den originalen optisch identisch sind. Der Benutzer wähnt sich auf der Originalseite und gibt dort sorglos seine Daten ein. Nachdem seit 1.3.2004[155] auch Umlaute in URLs verwendet werden können, sind neue Möglichkeiten der Adressnamenverfälschung entstanden. Beispielsweise könnte eine Originaladresse auf *http://www.schoellerbank.at/* lauten und die Fälschung auf *http://www.schöllerbank.at/*. Die beiden Namen erscheinen in der Wahrnehmung des Users gleich, technisch sind sie allerdings unterschiedlich. Ebenso schwer zu erkennen ist die Verwendung von Buchstaben aus anderen Alphabeten. So unterscheidet sich etwa das kyrillische „а“ optisch in keiner Weise vom lateinischen „a“. Um beim Beispiel der Bank zu bleiben wird das „а“ in http://www.schoellerbank.at/ in kyrillisch dargestellt, somit ist die Adresse unterschiedlich und der nichts ahnende User wird auf die falsche Seite gelinkt.

Aus einem Bericht [Symantec, 2006-1] (erstes Halbjahr 2006) des Herstellers Symantec geht unter anderem hervor, dass Phisher versuchen, Filtertechnologien zu umgehen, indem sie zahlreiche verschiedene Varianten von Phishing-E-Mails erzeugen und verteilen. In dem Zeitraum wurden 157.477 unterschiedliche Phishing-Kampagnen dokumentiert, das ist eine Zunahme von 81 Prozent gegenüber dem Vergleichszeitraum zweites Halbjahr 2005. Nicht überraschend ist, dass der Finanzsektor am stärksten davon betroffen ist: 84 Prozent aller Phishing-Angriffe, die vom Symantec „*Phish Report Network“* und „*Brightmail AntiSpam“* registriert wurden, zielen auf Banken und andere Finanzdienstleister ab.

Symantec [Symantec, 2007] berichtet in diesem Zusammenhang von der Professionalisierung der Methoden, die sich in einem enormen Anstieg von Phishing-Toolkits zeigt. Dabei handelt es sich um eine Reihe von Skripts, die einem Angreifer die automatische Einrichtung von Phishing-Webseiten ermöglichen. Damit ist es ein Leichtes, Webseiten von bekannten Unternehmen inklusive der zugehörigen *Corporate Identity* (z. B.: Logo) vorzutäuschen. Parallel dazu lassen sich über solche Skripts korrespondierende Phishing-Mails generieren, um den Anwender auf die Webseite zu locken. Im Berichtszeitraum Jänner bis Juli 2007 stammten 86 Prozent der weltweiten Phishing-Webseiten von lediglich 30 Prozent der erfassten Absender IP-Adressen.

[155] Vgl. http://www.nic.at/de/service/technische_informationen/idn/zeichentabelle_konverter/ [1. März 2008]

Das britische Finanzkontrollorgan *Financial Services Authority*[156] (kurz: *FSA*) berichtet im Dezember 2006, dass die Anzahl der Phishing-Fälle in Großbritannien von 2004 bis 2006 um 8.000 Prozent zugenommen hat. Laut FSA hat sich Phishing in den vergangen Jahren quasi zu einem industriellen Zweig entwickelt.

Neuere Daten [Messagelabs, 2007] vom dritten Quartal 2007 bestätigen, dass durch das gestiegene Angebot an Phishing-Toolkits und die zunehmende Nutzung aggressiver Phishing-Techniken wie *Rock*-Phishing[157] sowohl die Zahl als auch die Schwere der Angriffe weiter gestiegen ist. Im Beobachtungszeitraum versuchte eine von 87 E-Mails Zugangsdaten auszuspionieren.

Schutzmaßnahmen gegen Phishing können beispielsweise E-Mail-Filtersysteme oder Features in Internet-Browsern sein. Ab der Version 7[158] des Microsoft Internet Explorers ist ebenso ein Schutz gegen Phishing integriert wie im *Mozilla Firefox*[159].

Speziell beim Onlinebanking bestehen einige Möglichkeiten, die Transaktionen sicherer zu gestalten. Eine Variante ist der Schutz durch indizierte TAN-Listen (kurz: *iTAN*). Damit schreibt die Bank die Verwendung einer bestimmten TAN vor. Im Gegensatz dazu war es bisher üblich, die nächste oder eine beliebige TAN zu nehmen. Im Oktober 2006 stellte jedoch der Sicherheitsspezialist *Sabre Labs*[160] in einer Analyse einiger TAN-Listen der *Citibank*[161] fest, dass ein potenzielles Sicherheitsrisiko durch die bankinterne Systematik der TAN-Erzeugung entsteht. Angreifern ist es mit mathematischen Modellen unter bestimmten Voraussetzungen auf Grundlage bereits verwendeter und somit ungültiger TANs möglich, weitere Transaktionsnummern zu berechnen. Eines der Hauptprobleme wird darin gesehen, dass potenzielle Phishing-Opfer ihren bereits verbrauchten TANs keine weitere Bedeutung und Vertraulichkeit zumessen. Die Empfehlung der Sicherheitsexperten ist eine Überarbeitung des Verfahrens zur Erstellung der TAN-Listen.

Die *Deutsche Gesellschaft für Informatik*[162] kritisiert in einer Aussendung[163] (März 2007) ebenfalls die Unsicherheit des iTAN-Verfahrens im Onlinebanking. Nach Auffassung der Experten hat das vor zwei Jahren eingeführte iTAN-Verfahren das Sicherheitsniveau kaum verbessert, weil die grundsätzliche Schwachstelle aller webbasierten Transaktionsverfahren bestehen bleibt. Empfohlen wird, dass die Benutzer das vom Browser angezeigte Zertifikat der Bank-Webseite überprüfen. Dies ist der Nachweis, dass die https-Verbindung tatsächlich mit der gewünschten Bank hergestellt ist. Wenn die

[156] Vgl. http://www.fsa.gov.uk [27. Feber 2007]
[157] Beim Rock-Phishing wird ein Phishing-Toolkit verwendet, das einem einzigen kompromittierten Computer innerhalb eines Botnets ermöglicht, mehrere Phishing-Sites gleichzeitig zu hosten.
[158] Releasedatum: 10. Oktober 2006
[159] http://www.mozilla.com/firefox/ [27. Feber 2007]
[160] Vgl. http://www.sabre-labs.com/ [6. März 2007];
http://www.phenoelit.net/lablog/ [27. März 2007]
[161] http://www.citibank.de/ [6. März 2007]
[162] http://www.gi-ev.de/ [5. Mai 2007]
[163] Vgl. http://www.gi-ev.de/aktuelles/meldungsdetails/meldung/152/ [8. März 2008]

Verschlüsselung zwischen Bankserver und Kunden-PC funktioniert, ist ein *Man in the Middle*-Angriff (siehe *1.4.3.4 Passwort-Attacken*) wirkungslos.

Manche Bankinstitute bieten mit dem *Transaktionscode-Key* (kurz: *TAC-Key*, auch unter *M-TAN* in der Literatur zu finden) eine zusätzliche Komponente, die mittels SMS auf ein vom Kunden autorisiertes Mobiltelefon übertragen wird. Der TAC-Key besteht aus einem vierstelligen numerischen Code und ist an die laufende Session gebunden. Die Verwendung eines vom Internet unabhängigen Kommunikationskanals (Mobiltelefon) erhöht die Sicherheit.

Der beste Ansatz ist die Verwendung der digitalen Signatur (siehe *1.7.2.1.7 Elektronische Signatur*), die außerhalb des Webbrowsers die Datenverschlüsselung vornimmt.

erhöhtes Risiko relativ geringes R. äusserst geringes R.	Risiko gegenüber Diebstahl von Zugangscodes (Phishing, etc)	Risiko gegenüber Angriffen über das Netz (Man in the Middle)	Risiko gegenüber Angriffen am Benutzer-PC (Trojanische Pferde)	Risiko bei strikter Einhaltung der Benutzer-Policies
Benutzername & Passwort				
PIN/TAN Verfahren				
PIN/iTAN Verfahren				
PIN/mTAN (TAC) Verfahren				
Authentifizierung mittels Signatur				
Signatur über Inhalte				
Bürgerkarte				

Abbildung 13: Onlinebanking-Sicherheit

Der österreichische Softwareentwickler *IdnWebshield*[164] hat ein Service entwickelt, mit dem es Unternehmen möglich ist, Schutzprofile gegen Phishing-Angriffe für wichtige Domains und Links anzulegen. Die Fälschungsmethoden zielen in erster Linie darauf ab, eine hohe Ähnlichkeit mit der Originaladresse zu erreichen. Durch die Kombination verschiedener Fälschungstechniken lassen sich Phishing-Adressen erzeugen, die einen hohen Grad an Verwechselbarkeit aufweisen und damit für den gutgläubigen, unerfahrenen Internetbenutzer zu einer Gefahr werden können. Betroffen von Phishing – im Konkreten Subdomain-Attacken – war beispielsweise die deutsche *Volksbank*[165]. Dabei wird die

[164] Vgl. http://www.idnwebshield.com/ [27. Feber 2007]
[165] http://www.volksbank.de/ [27. Feber 2007]

Domain *volksbank.de* als Subdomain einer beliebigen anderen *.com* eingerichtet. Für die Benutzer ist das kaum zu erkennen. Das von den IdnWebShields eingesetzte Schutzprofil verhindert, dass eine Adresse mit Subdomain volksbank.de überhaupt angesteuert werden kann, selbst wenn diese verschachtelt ist.

Ein hundert prozentiger Schutz gegen Phishing existiert nicht: Es gibt einfach zu viele Möglichkeiten, derartige Angriffe im Internet zu platzieren. Neben den erläuterten technischen Maßnahmen (siehe auch *1.7.2.7 Sicherheitsmaßnahmen von Microsoft*) kann durch eine Sensibilisierung der User und dem Bereitstellen von Verhaltensratschlägen die Sicherheit spürbar erhöht werden[166]. Unterstützung im Kampf gegen Phishing bietet zudem eine von der *Anti-Phishing-Group*[167] angebotene Datenbank (Juli 2007) zum gegenseitigen Informationsaustausch über Phishing-Attacken.

1.4.1.2.1 Pharming

Pharming[168] (Kunstwort zusammengesetzt aus Server*farm* und Phishing) ist – ähnlich dem Phishing – eine weitere Betrugsmethode im Internet. Sie basiert auf der Manipulation von DNS-Anfragen (beispielsweise durch DNS-Spoofing, siehe *1.4.3.6 Spoofing*), um die Benutzer auf gefälschte Webseiten umzuleiten. Eine Methode dabei ist die Veränderung der *Hosts*-Datei[169]. Dabei wird – etwa mit einem Trojaner – ein System so manipuliert, dass von diesem nur noch gefälschte Webseiten abgerufen werden können, selbst wenn die Adresse korrekt eingegeben wurde.

1.4.1.2.2 SMiShing

Bei *SMiShing*[170] (Kunstwort zusammengesetzt aus SMS und Phishing) wird per SMS eine Art „Abobestätigung" verschickt. Darin wird eine Webadresse zur Abmeldung genannt. Bei Besuch dieser Seite wird versucht, einen Trojaner einzuschleusen.

1.4.1.2.3 Vishing

Vishing[171] (Kunstwort zusammengesetzt aus *Voice* und Phishing) steht für Betrug im Bereich Voice over IP- (kurz: *VoIP*) Telefonie. Dabei wird per Telefonanruf – über das kostengünstige VoIP –

[166] Vgl. https://www.a-i3.org/content/view/932/203/ [8. März 2007]
[167] http://www.antiphishing.org/ [27. Mai 2007]
[168] Vgl. http://www.pharming.org/index.jsp [9. März 2007];
http://www.zeit.de/online/2007/08/internet-betrug-pharming?page=2 [9. März 2007]
[169] Die hosts-Datei ist eine lokale Textdatei, die der Zuordnung von Hostnamen zu IP-Adressen dient.
[170] Vgl. http://www.heise.de/newsticker/meldung/77326 [9. März 2007];
http://www.consumeraffairs.com/news04/2006/11/smishing.html [9. März 2007]
[171] Vgl. http://www.internetnews.com/security/article.php/3619086 [9. März 2007];
http://www.telekom-presse.at/channel_internet/news_24245.html [9. März 2007]

versucht, den Empfänger zu täuschen und zur Herausgabe von Passwörtern oder Kreditkartendaten zu verleiten. Das FBI weist im Jänner 2008 auf einen Anstieg von Vishing-Attacken hin[172].
Eine andere Variante des Vishing ist die, per Spam (siehe *1.6 Exkurs: E-Mail/Spam*) eine Telefonnummer zu verbreiten. Die Nachricht enthält eine Aufforderung, sich bei der angegebenen Telefonnummer zu melden. Ein Tonband verlangt von den Anrufern persönliche Daten. Besonders hinterhältig ist dieses Verfahren deswegen, weil es den Ratschlag und den Hinweis vieler Finanzinstitute ausnutzt, nicht auf E-Mails zu reagieren, sondern telefonischen Kontakt zu suchen.

1.4.1.3 Physischer Einbruch

Hierbei geht es um den klassischen Einbruch in ein Gebäude. Befindet sich der Eindringling im Haus, kann er sowohl analoge wie digitale Daten entwenden (kopieren, stehlen). Da diese Art der Informationsbeschaffung für die Einbrecher ein verhältnismäßig hohes Risiko darstellt, sind die virtuellen Eindringversuche im Vormarsch.

1.4.1.4 Dumpster Diving

Mülltonnen sind oft eine ergiebige Quelle um an Informationen zu gelangen. Gelingt es dem Hacker, Zugang zu weggeworfenen Akten, Plänen, CDs oder Backupmedien bekommen, lassen sich viele wertvolle Daten rekonstruieren (Unternehmenskennzahlen, Accountdaten, Telefonnummern, Anwesenheitslisten etc.)
Die effizienteste Gegenmaßnahme ist das Sensibilisieren der Mitarbeiter, nicht mehr benötigte Daten entsprechend zu archivieren bzw. zu vernichten.

1.4.1.5 Internetsuche

Im Internet ist eine Reihe von Informationen über das „Ziel“ eines geplanten Angriffs zu finden [Weippl, 2004, Threats and Countermeasures, S 4ff]. Der Besuch einer Webseite eines Unternehmens offenbart bereits einige Grunddaten: Kontaktinformation, Geschäftspartner, eingesetzte Technologien etc. Zudem ist vieles mittels Internet-Suchmaschinen zu finden (neues Wort im Sprachgebrauch dafür ist *googlebar*), so lassen sich Informationen über vergangene und künftige Events, Aktivitäten, Berichte über das Angriffsziel in Sekundenschnelle abrufen. Eine ergiebige Quelle können auch *Usenets*[173] oder *Newsfore*n sein. Dort beantworten Mitarbeiter beispielsweise Fragen zu technischen Funktionalitäten eines Produkts oder tätigen Aussagen über Interna ihres Arbeitgebers.

---

172 http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9057918&source=NLT_AM&nlid=1 [21. Jänner 2008]

173 Das Usenet ist ein weltweites, elektronisches Netzwerk, das Diskussionsforen aller Art für jedermann bereitstellt.

1.4.1.5.1 WhoIs

Über das *WhoIs*-Protokoll sind Informationen zu finden, wie etwa, welcher Mitarbeiter für die Organisation des Internets verantwortlich zeichnet.
Plattformen wie *RIPE*[174] bieten einfach zu bedienende Masken zum Suchen von Domain-Informationen.

1.4.1.5.2 DNS

Mittels des Befehls *nslookup* (Windows, Unix) ist es ein Einfaches IP-Adressen oder Domänenzugehörigkeit eines bestimmen Computers herauszufinden (siehe *1.3.4.2.2 DNS-Sicherheit*).
Gegenmaßnahmen sind hier nur schwer möglich, zum einen ist das Exponieren von Unternehmensdaten durch Mitarbeiter im Internet (z. B.: Foren, E-Mail-Verteiler) durch Policies einzuschränken, zum anderen kann das Unternehmen durch technische Maßnahmen (Splitting, Zonentransferrestriktionen) im Bereich des DNS Informationen unterdrücken.

1.4.2 IDENTIFIZIEREN VON ZUGANGSMÖGLICHKEITEN

Nachdem beschrieben wurde, wie man Informationen über das Ziel des Angriffs sammeln könnte, werden nachfolgend einige gängige, elektronische Zutrittsmöglichkeiten aufgezählt [Weippl, 2004, Threats and Countermeasures, S 12ff]. Hierbei werden in der Regel Verletzlichkeiten/Schwachstellen (engl. *Vulnerabilities*) von Datenbanken, DNS etc. ausgenutzt.

1.4.2.1 War Dialing

Unter *War Dialing* wird die systematische Suche nach Telefonnummern verstanden, die in Verbindung mit Modems stehen. Mit Computerprogrammen wie *ToneLOC*[175] und einem Modem werden etwa alle Telefonnummern in einem vorgegebenen Rufnummernbereich automatisch angewählt. Dieser Vorgang wird protokolliert, damit kann dann festgestellt werden, hinter welcher Nummer ein Computer steckt. Der nächste Schritt überprüft, ob der Computer remote erreich- und kompromittierbar ist.
Die Unternehmen vergessen bei den Security-Überlegungen gern auf Modems, die meist schon Jahre im Einsatz sind. Zudem gibt es oft keine Inventarliste (engl. *Inventory*), in der festgehalten ist, wo ein Modem in Verwendung ist. Technisch können Maßnahmen wie *dial-out only* gesetzt werden, organisatorisch ist das Verbot von Modems per Sicherheitsrichtlinie (siehe *1.8.2.4.2 IT-Systemsicherheitspolitik*) ein Ansatz.

[174] http://www.ripe.net/ [27. Feber 2007]
[175] http://www.iss.net/security_center/advice/Countermeasures/Scanners/War_Dialers/ToneLoc/default.htm [9. März 2007]

1.4.2.2 Network Mapping

Das Ziel ist, eine Übersicht über die Netzwerkstruktur zu erhalten. Dazu sollen alle an ein Netzwerk angeschlossenen Systeme identifiziert werden. Mit Systembefehlen wie *traceroute*[176] bzw. Tools wie *Cheops*[177] können wesentliche Komponenten (Router, Firewalls etc.) ausgeforscht werden.
Eine Firewall (siehe *1.7.2.4.1 Firewall*) stellt einen probaten Schutz dar.

1.4.2.3 Scanning

Durch *Scanning* können Informationen wie IP-Adressen von verfügbaren Rechnern, Betriebssystem oder eingesetzte Software mit Versionsangabe (engl. *Release*) gewonnen werden. Diese Technik ermöglicht es, herauszufinden, ob der jeweilige Dienst einen anonymen Login erlaubt bzw. eine Authentifizierung fordert.

1.4.2.3.1 Port-Scanner

Ein Portscanner ist eine Software (z. B.: *NMap*[178]), mit der überprüft werden kann, welche Dienste (Web-, FTP- und Telnetserver) ein System im Netzwerk anbietet. Damit kann meist auch die Funktion des Systems eruiert werden.
Unter Ports werden Adressenbezeichnungen verstanden, die in Netzwerkprotokollen eingesetzt werden, um Datensegmente den richtigen Diensten zuzuordnen. So läuft beispielsweise der Dienst HTTP für das Internet über Port 80, der Port 25 für SMTP (E-Mail). Insgesamt stehen unter TCP/IP (siehe *1.3.4.2.1 TCP/IP-Sicherheit*) 65535 Ports zur Verfügung, die für Dienste genutzt werden können.
Eine gut konfigurierte Firewall bietet durch das Schließen aller nicht gebrauchten Ports einen adäquaten Schutz. Zudem können Intrusion Detection-Systeme (siehe *1.7.2.4.4 Intrusion Detection Systeme und Intrusion Prevention Systeme*) die Vorgänge zumindest dokumentieren.

1.4.2.3.2 Schwachstellen-Scanner

Schwachstellen-Scanner sind Computerprogramme (z. B.: *Nessus*[179]), die Zielsysteme auf Sicherheitslücken und Konfigurationsfehler hin untersuchen. Grundlage der Überprüfung eines Rechners ist ein Port-Scan. Für jeden gefundenen Dienst wird festgestellt, welches Programm in welcher Version diesen Dienst anbietet. Dann wird der jeweilige Dienst automatisch auf Schwachstellen hin getestet. Hierbei wird zum Beispiel auf anonyme Logins bzw. Logins mit Standardbenutzernamen und -passwörtern geprüft. Zudem werden Tests auf Sicherheitslücken

[176] http://www.heise.de/netze/tools/traceroute [9. März 2007]
[177] http://cheops-ng.sourceforge.net/ [9. März 2007]
[178] http://insecure.org/nmap/ [9. März 2007]
[179] http://www.nessus.org/ [21. März 2007]

(Softwarebugs, Konfigurationsfehler, dokumentierte Schwachstellen (engl. *known issues*) bei ungepatchten Systemen) durchgeführt. Des Weiteren gibt es Tests auf bereits bekannte Schwachstellen mittels simulierter Angriffe, zum Beispiel Buffer Overflow-Angriffe (siehe *1.4.3.3 Buffer Overflow-Attacken*) oder Denial of Service-Attacken (siehe *1.4.3.7 Denial of Service*). Die Ergebnisse der Tests werden oft in ausführlichen Dokumentationen über die gefundenen Schwachstellen – auch öffentlich im Internet – sowie Behebungsvorschlägen aufbereitet.

Während Nessus ein frei verfügbares Werkzeug ist, kann der *Internet Security Scanner* der Firma *ISS*[180] nur käuflich erworben werden. Für Systemadministratoren sind solche Scanner eine wichtige Hilfe, um Sicherheitslücken aufzuspüren. Für Angreifer hingegen bieten die mit solchen Tools gewonnen Informationen die Basis, die es überhaupt erst ermöglicht, in ein System einzubrechen.

Technisch sind Firewalls in Verbindung mit Intrusion Detection Systems (siehe *1.7.2.4 Perimetersicherheit*) eine geeignete Schutzmaßnahme gegen Scanning. Zudem ist es erforderlich, nicht verwendete Dienste zu deinstallieren. Eine organisatorische Gegenmaßnahme ist das Durchführen von Audits (siehe *1.7.1.1.3 Audits und Revision*), wo proaktiv Schwachstellen in den Systemen geortet werden können.

1.4.2.4 Sniffing

Unter *Sniffing* wird das Abhören und Auswerten von Datenpaketen im Netzwerk verstanden. Sniffing ist eine wesentliche Methode bei der Diagnose bzw. beim Troubleshooting von Netzwerkproblemen und unterstützt die Administratoren bei der Netzwerkanalyse und dem Entdecken von Anomalien. Es kann aber auch dazu genützt werden, um Datenspionage für einen Angriff zu betreiben. Während beim Scanning der Rechner analysiert wird, fokussiert Sniffing auf den Bereich Netzwerk und Kommunikation.

Ein Sniffer arbeitet in zwei Modi: den *non-promiscuous* und den *promiscuous Mode*. Während im non-promiscuous Mode der ankommende und abgehende Datenverkehr des eigenen Systems (eindeutiges Kennzeichen ist die MAC-Adresse) gesnifft wird, werden im promiscuous Mode die gesamten Daten einer Netzwerkschnittstelle gesammelt.

Für das Sniffing gibt es eine ganze Reihe von freien und kommerziellen Produkten: *Clearsight Analyzer*[181], *Ettercap*[182], *Sniffer*[183], *Ethereal*[184] oder *Tcpdump*[185].

[180] http://www.iss.net/ [27. Feber 2007]
[181] http://www.clearsightnet.com/ [27. Feber 2007]
[182] http://ettercap.sourceforge.net/ [27. Feber 2007]
[183] http://www.networkgeneral.com/ [27. Feber 2007]
[184] http://www.ethereal.com/ [16. März 2007]
[185] http://www.tcpdump.org/ [27. Feber 2007]

1.4.3 ZUGANG

Gegenstand dieses Abschnitts soll die Darstellung der wichtigsten Technologien sein, die Angreifern für einen unberechtigten Zugang zu Informationen zur Verfügung stehen [Weippl, 2004, Threats and Countermeasures, S 21ff]. Der Fokus der Darstellung liegt dabei auf der Beschreibung der Angriffstechniken auf Netzwerk-, Betriebssystem und Applikationsebene, die von externen Angreifern verwendet werden können, aber auch – zumindest teilweise – internen Angreifern zur Verfügung stehen. In der Literatur werden die Angreifer gerne als *Script Kiddie*, *Cracker* oder *Hacker* bezeichnet.

1.4.3.1 Exkurs: Script Kiddie/Hacker/Cracker

Script Kiddie steht als Synonym für eine Person, die – in meist dilettantischer Art – vorgefertigte Programme („Baukastensystem“) benutzt, um Sicherheitsbarrieren zu überwinden. Im Gegensatz zum professionellen Hacker hat ein Script Kiddie nur wenig Wissen darüber, wie eine Schwachstelle auszunutzen ist oder wie sich Sicherheitslücken aufspüren lassen. Angesichts der im Internet zugänglichen, leicht verständlichen Anleitungen zum Hacken und der vielen vorgefertigten, automatisierten Tools, steigt die Zahl der Script Kiddies stetig an.
Ein Hacker ist ein Computerbenutzer mit sehr hohem Fachwissen und technischem Knowhow. Das Wissen wird dazu genutzt, Sicherheitslücken zu identifizieren und durch diese unter Umgehung der Sicherheitsmaßnahmen Zugriff auf ein System zu erlangen. Gearbeitet wird nach einer „Hackerethik“ [Janowicz, 2006, S8f]. Ziel eines Hackers ist es nicht, möglichst viel Schaden anzurichten, sondern einem verantwortungsvollen Umgang mit Computertechnologien Vorschub zu leisten. Dazu werden beispielsweise neue Entwicklungen kritisch beobachtet und untersucht. Hacker dringen zwar in Systeme ein, suchen nach Informationen, richten aber dabei keinen Schaden an. Viele Hacker veröffentlichen sogar die von ihnen gefundenen Sicherheitslücken samt Hilfestellungen und Lösungsansätzen, um ihre Erkenntnisse für die Verbesserung von Sicherheitssystemen nutzbar zu machen. Die Verwendung des Begriffs „Hacker“ ist umstritten, es soll eine deutliche Unterscheidung zur Bezeichnung „Cracker“ geben. Bei Crackern geht es um Zerstörung und Schädigung, es gibt keine ethischen Grundsätze. Die Forderung der Hackergemeinschaft, hier genauer zu differenzieren, wird von den Medien nicht wahrgenommen bzw. ignoriert. Gemeinhin verstehen und verwenden die meisten Menschen den Begriff „Hacker“ für Eindringlinge, unabhängig, ob diese mit guter oder schlechter Absicht agieren.

1.4.3.2 Backdoor/Rootkit

Als *Backdoor* wird ein Teil eines Computerprogrammes bezeichnet, der es Benutzern ermöglicht, unter Umgehung der Standard-Zugriffssicherung („durch die Hintertür“) Zugang zum System zu erlangen.

Unter *Rootkit* werden Softwaretools verstanden, die nach dem Eindringen in ein Computersystem auf dem kompromittierten System installiert werden, um zukünftige Logins, Prozesse und Dateien zu verbergen. Zweck eines Rootkits ist es, Malware vor Schutzprogrammen zu verstecken. Dabei verschleiern Rootkits nicht nur ihre eigene Existenz, sondern auch alle Angreifer-Aktivitäten. Jeder Login des Hackers und jede Aktion werden quasi unsichtbar durchgeführt.

Die Grenze zwischen Rootkit und Backdoor ist fließend. Ein Rootkit versteckt per se Logins und Prozesse, enthält Software, um Daten von Terminals oder Netzwerkverbindungen zu sammeln. Durch Backdoors wird es einfacher, auf das kompromittierte System zuzugreifen.

Rootkits kompromittieren jedoch nicht nur Systeme, sondern haben auch eine positive Seite und können durch die Möglichkeit, in grundlegende Systemfunktionen einzugreifen, sogar zu deren Schutz beitragen.

In der Literatur werden Backdoor/Rootkit gern in Applikation-Backdoors, in traditionelle Rootkits und in *Kernel*-Rootkits aufgeteilt. Bei den Backdoors läuft eine eigenständige Applikation, die dem Angreifer unbemerkt Zugriff ermöglicht. Während bei den traditionellen Rootkits wesentliche Betriebssystemteile verändert oder getauscht werden, wird bei den Kernel-Rootkits der ganze Betriebssystemkernel manipuliert.

Eines der größten Ziele aller Malware-Hersteller ist es, die Anwesenheit von Schadprogrammen in Systemen unsichtbar zu machen. Die Sicherheitsexperten von *Kaspersky Lab*[186] warnen deshalb vor boomender Rootkit-Technologie zur Verbergung von Malicious Code in Systemen. Der steigende Bekanntheitsgrad von Rootkits steht laut Kaspersky in Zusammenhang mit der Verbreitung der Quelltexte dieser Bausätze im Internet. Durch diese fertigen und dokumentierten Module ist es für die Angreifer leichter, die *Geheim*- (engl. *Stealth*) Komponenten in ihren Schadprogrammen zu realisieren. Ein weiterer Aspekt zur Verbreitung von Rootkits ist der Umstand, dass die Mehrheit der Windows-Anwender mit Administrationsrechten arbeitet.

Im Herbst 2005 kam die Firma *Sony BMG*[187] in die Schlagzeilen und musste diverse Musik-CDs zurückrufen, nachdem im Weblog von *Sysinternals*[188] bekannt wurde, dass der Sony-Kopierschutz für Musik-CDs sich mit Methoden eines Rootkits in Windows-Systemen einnistet (siehe *2.3.3.5 Digital Rights Management*).

Auf der Sicherheitskonferenz *Black Hat*[189] im Jänner 2006 wurde ein BIOS-Rootkit vorgestellt, der selbst durch ein Neuformatieren der Festplatte nicht gelöscht werden kann.

Um Rootkits entgegenzuwirken, müssen zunächst Beobachtungen des Systems angestellt werden. Das Verfolgen ungewöhnlichen Verhaltens von Programmen, ausführende Aufgaben beim Systemstart und

[186] Vgl. http://www.kaspersky.com/ [27. Feber 2007];
http://www.viruslist.com/de/analysis?pubid=167889685 [27. März 2007]
[187] http://www.sonybmg.com/ [27. Feber 2007]
[188] Vgl. http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html [27. Feber 2007]
[189] Vgl. http://www.blackhat.com/ [27. Feber 2007]

die registrierten Einträge der Anwender können Hinweise auf Rootkits sein. Zusätzlich gibt es Hilfsprogramme wie *Chkrootkit*[190] oder *Tripware*[191], die beim Aufspüren der Stealth-Tools hilfreich sind. Die Schutzmaßnahmen reichen von Antivirensystemen über Berechtigungskonzepte bis hin zu Awareness-Bildung (siehe *1.7 Schutzmaßnahmen und Gegenstrategien*).

1.4.3.3 Buffer Overflow-Attacken

Pufferüberläufe (engl. *Buffer Overflows*) gehören zu den häufig über das Internet genutzten Sicherheitslücken. Bei einem Buffer Overflow werden durch Programmfehler oder Nichtbeachtung von Programmierstandards zu viele Daten in einen zu kleinen Speicherbereich geschrieben. Dies kann einen Programmabsturz, eine Verfälschung der Daten oder eine Beschädigung von Datenstrukturen zur Folge haben.

Während der Ausführung eines Programms werden vom Prozessor bestimmte Daten (gerade verarbeitete Daten, Rücksprungadresse) in einen sogenannten *Stack* als Zwischenspeicher geschrieben. Wird nun eine den Buffer übersteigende Zeichenkette übermittelt und ist keine entsprechende Sicherheitsstruktur vorhanden, wird zwar ab der vorgesehenen Stelle gespeichert, aber gleichzeitig überschreibt der überlange Teil der Zeichenkette den für andere Zwecke vorgesehenen Speicherplatz. Dadurch kann ein Angreifer einen geänderten Code mit den entsprechenden Privilegien einbringen. Dieser Code hat zum Ziel, dem Angreifer einen Zugang zum System zu verschaffen. Gefährdet sind dabei im Besonderen Anwendungen, die als Eingabe Zeichenketten entgegennehmen, wie zum Beispiel http-Anfragen bei Webservern. Buffer Overflows kann es auch in Server- und Clientsoftware geben, hier werden sie besonders von Würmern (siehe *1.3.4.4 Wurm*) ausgenützt.

Neben Fehlern in der Programmierung werden Pufferüberläufe vor allem durch das Vermischen von Daten und Programmen im gleichen Speicher[192] ermöglicht.

Hier ist bei der Vermeidung auch der Hebel anzusetzen, indem etwaige Fehler kurzfristig durch Patches (siehe *1.7.1.2.2 Patchmanagement*) behoben und langfristig Sicherheitsstandards bei der Programmierung eingehalten werden.

1.4.3.4 Passwort-Attacken

Hierbei geht es im Wesentlichen um das Herausfinden von Passwörtern, sei es durch Ausprobieren von Standardpasswörtern, durch *Login Scripting*[193] oder Entschlüsseln von Passwörtern.

In diesem Zusammenhang spielt die *Kryptoanalyse*[194] (siehe *1.7.2.1 Kryptologie*) eine zentrale Rolle. Bei den gängigen *Dictionary-Attacks* wird versucht, ein unbekanntes Passwort mit Hilfe von Software

[190] http://www.chkrootkit.org/ [27. Feber 2007]
[191] http://sourceforge.net/projects/tripwire/ [27. Feber 2007]
[192] Vgl. http://user.cs.tu-berlin.de/~icoup/archiv/3.ausgabe/artikel/neumann.html Dem Prinzip der von Neumann-Architektur folgend, wonach es nur einen Speicher für Programme und Daten gibt. [9. März 2007]
[193] Skripts zum An- und Abmelden von Geräten im Netzwerkbetrieb

und einer Passwortliste zu knacken. Alle Schlüssel aus einem „Wörterbuch“ werden durchprobiert. Diese Methode ist dann sinnvoll, wenn von einfachen Passwörtern ausgegangen werden kann.
Eine andere Technik sind *brute-force-Attacks*, worunter im Wesentlichen das Ausprobieren aller Möglichkeiten verstanden wird. Alle möglichen Schlüssel werden gereiht nach Wahrscheinlichkeit probiert. Die Methode ist bei relativ schwachen Passwörtern sehr effizient und erfolgreich. Ein Angreifer kann mit einem besseren Standardcomputer mehrere Millionen Schlüssel pro Sekunde testen.
Bei *Man In The Middle*-Attacken befindet sich der Angreifer entweder physikalisch oder virtuell zwischen den Kommunikationspartnern und hat dabei die Kontrolle über den Datenverkehr. Dabei können Informationen nach Belieben eingesehen, gesammelt und verändert werden. Zudem kann der Angreifer einem Partner das Gegenüber vortäuschen, ohne dass es bemerkt wird.
Die effektivste Gegenmaßnahme ist, *starke* Passwörter (Groß-, Kleinschreibung, Sonderzeichen etc.) zu verwenden und diese regelmäßig zu wechseln (siehe *1.7.1.3 Grundsätze im Umgang mit PCs zum Schutz vor Malicious Code* und *1.7.2.5 Graphisches Passwort*). Zudem sollten die Passwörter der Benutzer serverseitig nicht unverschlüsselt gespeichert werden. In der Regel wird lediglich der *Hash*[195] (siehe *1.7.2.1.4 Hash-Verfahren*) des Passworts gespeichert. Kommt der Angreifer in den Besitz dieser Hash-Datei, kann er beispielsweise mit einer Dictionary-Attack versuchen, an das Passwort zu kommen. Damit keine fertigen, indizierten Listen verwendet werden können, wird das Passwort vor dem Hashen um einen Zufallswert (*salt*[196]) erweitert.
Neben Verschlüsselung bietet die sogenannte *Integrity Protection* Manipulationsschutz vor Man In The Middle-Attacken. Jede übertragene Nachricht wird mit einem Identitätsstempel versehen, der mittels eines vorher ausverhandelten Codes erzeugt wird. Unter der Bedingung, dass der mit der Nachricht mitgeschickte Code dem vom Empfänger erwarteten entspricht, wird die Nachricht vom Empfängersystem verifiziert und weiter verarbeitet.

1.4.3.5 Webapplication-Attacken

Die Zahl der Applikationen im E-Commerce, E-Voting und E-Government steigt ständig. Für einen Angreifer bilden diese *Multi-Tier*-Architekturen (Webserver, Webanwendung, Datenbank) oft ein attraktives und lukratives Betätigungsfeld (siehe *3.4.4 Portale und Web Services*). Nachfolgend sollen die gängigsten Angriffsmethoden aufgezählt und näher erläutert werden: Buffer Overflow (siehe *1.4.3.3 Buffer Overflow-Attacken*), *Cross Site-Scripting*, *Cross Site Request-Forgery*, Denial of

[194] Die Kryptoanalyse bezeichnet die Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen.
[195] Ein Hash ist ein skalarer Wert („*Fingerprint*“), eine (nahezu) eindeutige Kennzeichnung einer übergeordneten Menge.
[196] Ein Salt besteht aus einer Reihe von zufälligen Bits. Durch die Verwendung eines salted values ist ein unverschlüsselter Wert nicht mehr eindeutig einem verschlüsselten Wert zuzuordnen.

Service (siehe *1.4.3.7 Denial of Service*), *Directory Traversal*, Man In The Middle-Attacken (siehe *1.4.3.4 Passwort-Attacken*), Phishing (siehe *1.4.1.2 Exkurs: Phishing*), *Session Hijacking* oder *SQL Injection*.

1.4.3.5.1 Cross Site-Scripting

Die Attacken werden webseitenübergreifend („*cross site*“) durchgeführt, so steht auf einer vom Angreifer kontrollierten Seite beispielsweise ein präparierter Hyperlink, der zur vermeintlich vertrauenswürdigen Webseite einer (meist) ahnungslosen dritten Partei führt.
Cross Site Scripting (kurz: *XSS*) [197] ist das Einschleusen von bösartigem Code in eine Webseite, wobei der eingeschleuste Code clientseitig ausgeführt wird. Ermöglicht wird XSS, wenn Usereingaben oder Variablenübergaben (Parameter) auf einer dynamischen Webseite nicht ordnungsgemäß überprüft werden.
Eine XSS-Attacke kann insbesondere in Kombination mit anderen Angriffsformen sehr effektiv sein, zum Beispiel Phishing (siehe *1.4.1.2 Exkurs: Phishing*) über XSS oder *Web Defacement*[198] via XSS.
Ein Artikel[199] von Computerworld zeigt Wege zur Bekämpfung von XSS: „*How to defeat the new No. 1 security threat: cross site-scripting. Cross site-scripting, often abbreviated XSS, is a class of Web security issues.*
In a typical XSS scenario, a Web page might use JavaScript to dynamically generate some document content based on a field in a Uniform Resource Identifier (URL). In the normal course of events, the site itself would generate legitimate information for that field. If, however, the script that generated the new content did not filter the URL, it would be possible for an attacker to feed the page a custom-designed URL that ran a script. The script could do almost anything, and the user would never know that he wasn't seeing legitimate content unless the hijacker was blatant. This is potentially very bad, since it is one way to enable phishing. For example, suppose a Web page with a cross site-scripting vulnerability belonged to a bank. An attacker aware of the vulnerability could forge E-Mails purporting to be from the bank, with URLs that indeed led to the bank's site, but contained some malicious script that wouldn't be obvious to a casual observer. Once a user clicked on the link in the E-Mail and logged into the bank site, their login credentials (in the form of cookies) for the current session would be transmitted to the attacker, who would be able to take over the user's account as long as the session was active. This is considerably worse than an attack that takes users to a forged Web page, because it can in principle bypass most forms of authentication protection. After all, it's

[197] Vgl. http://www.cgisecurity.com/articles/xss-faq.shtml [27. März 2007];
http://httpd.apache.org/info/css-security/ [27. März 2007]
[198] Defacement bezeichnet das unberechtigte Verändern/Verunstalten einer Website.
[199] Vgl. http://www.computerworld.com/ „How to defeat the new No. 1 security threat: cross-site scripting“ 29. September 2006 [27. März 2007]

using the bank's own authentication system, and then hijacking the results. David Flanagan, author of JavaScript: The Definitive Guide, says cross site-scripting enables a pernicious vulnerability whose roots go deep into the architecture of the Web."

Um eine Webanwendung vor einem XSS-Angriff zu schützen, sollten alle eingehenden Parameter vor der weiteren Verarbeitung durch die Applikation selbst in einem *Whitelist*-Verfahren geprüft werden.

Das Ausschalten von JavaScript[200] im Webbrowser (nur bedingt möglich, weil einige Seiten sonst nicht ausgeführt werden können) und der Einsatz von Applikation-Firewalls (siehe *1.7.2.4.1 Firewall*) können Schutz vor XSS-Angriffe bieten.

1.4.3.5.2 Session-Hijacking

Nachdem HTTP ein zustandsloses[201] Protokoll (siehe *1.3.4.2.3 HTTP-Sicherheit*) ist, muss die Webapplikation die Identifikation eines Benutzers selbst feststellen. Dazu wird zu Beginn jeder Sitzung eine eindeutige *SessionID* generiert, die der Browser des Benutzers bei allen folgenden Anfragen anfügt. Ist es dem Angreifer möglich, die SessionID mitzulesen, kann er durch das Hinzufügen der SessionID an seine eigenen Requests die Session übernehmen.

Während Session-Hijacking durch Verschlüsselung der Daten und starke Authentifizierung verhindert werden kann, ermöglichen es Intrusion Detection Systeme (siehe *1.7.2.4.4 Intrusion Detection Systeme und Intrusion Prevention Systeme*) zumindest, solche Angriffe zu erkennen.

1.4.3.5.3 SQL-Injection

Hierbei geht es um das Ausnützen von Sicherheitslücken bei SQL-Datenbanken zur Erlangung der Kontrolle auf die Datenbank. Eine Anfälligkeit für SQL-Injection weisen dynamische Skriptsprachen wie *ASP.NET*[202], *PHP*[203], *JSP*[204] und *CGI*[205] auf. Das Rüstzeug für eine SQL-Injection besteht aus einem Webbrowser und dem „Gespür“ für das Finden von wichtigen Daten. Findet der Angreifer eine Sicherheitslücke, kann er über Eingabefelder eines Formulars SQL-Abfragen oder -Befehle einschleusen. SQL-Anweisungen wie *SELECT, INSERT, DELETE* oder *DROP TABLE* können

[200] JavaScript ist eine objektbasierte Programmiersprache im Web. Sie wird für die Ausführung aktiver Inhalte innerhalb einer Webseite verwendet. Des Weiteren ermöglicht JavaScript das Schreiben und Lesen von Daten auf dem Besucher-PC, sogenannten Cookies.
[201] Zustandslos bedeutet, dass nach jeder Datenübertragung die Verbindung zwischen den beiden Kommunikationspartnern beendet und bei weiteren Daten eine neue Verbindung aufgebaut wird.
[202] Active Server Pages.NET (kurz: ASP.NET) ist eine Technologie von Microsoft zum Erstellen von Webapplikationen.
[203] Hypertext Preprocessor (kurz: PHP) ist eine Open-Source-Skriptsprache zur dynamischen Erstellung von Webseiten oder Webanwendungen.
[204] JavaServer Pages (kurz: JSP) ist eine Technologie zur dynamischen Erzeugung von HTML- und XML-Ausgaben eines Webservers.
[205] Das Common Gateway Interface (kurz CGI) ist ein Standard für den Datenaustausch zwischen einem Webserver mit einer Software und eine Variante um Webseiten dynamisch bzw. interaktiv zu machen.

problemlos zur Manipulation an die Datenbank geschickt werden. Der Einsatz von Metazeichen wie „, ` ´ \ Prozent oder /“ bringt Webapplikationen dazu, SQL-Code auszuführen.
Zudem ist es für den geübten Angreifer möglich, beliebige Daten (Tabellen, Passwörter etc.) aus der Datenbank zu lesen, Verbindungen zu anderen Systemen herstellen oder sogar Backdoors zu installieren.
Die Webapplikation ist grundsätzlich selbst für die Prüfung der Eingabedaten verantwortlich. Ergo dessen sollte bei der Programmierung auf die Einhaltung von Sicherheitsstandards und -empfehlungen geachtet werden, zumal der sorglose Umgang damit SQL-Injection-Attacken meist erst ermöglicht. Technisch kann der Einsatz von Applikations-Firewalls (siehe *1.7.2.4.1 Firewall*) dazu beitragen, Schwachstellen in Webanwendungen abzuschirmen. Bezüglich Rechteverwaltung sollten die Arbeiten – soweit wie möglich – beim SQL-Server mit eingeschränkten Zugriffsrechten erledigt werden.

1.4.3.6 Spoofing

Unter *Spoofing* werden Techniken zur Täuschung und Fälschung von Identitäten in Netzwerken verstanden. Die Motive für Spoofing reichen von Verschleierung einer Identität bis hin zum Ausspionieren von Daten. Spoofing kann dabei auf verschiedenen Netzwerk-Schichten angewendet werden:

- *DNS-Spoofing*: hierbei wird die Zuordnung eines Rechnernames zur zugehörigen IP-Adresse gefälscht, das heißt, ein Name zu einer falschen IP-Adresse und vice versa. Beispielsweise bekommt ein anfragender Client eine Antwort mit einer gespooften IP-Adresse zurück, so dass er auf eine falsche Webseite gelenkt wird (siehe *1.3.5.2 Datendiebstahl und Spionage*).
- *IP-Spoofing*: darunter wird das Versenden von Datenpaketen mit gefälschter Quell-IP-Adresse verstanden. Diese Technik findet bei Denial of Service-Angriffen (siehe *1.4.3.7 Denial of Service*) Verwendung oder um Zugang zu privaten Netzwerken zu bekommen.
- *MAC-Spoofing*: Die MAC-Adresse ist eine einzigartige, eindeutige Adresse einer Netzwerkkarte. Sicherungsmechanismen im Netzwerk stellen Verbindungen nur auf Basis bestimmter MAC-Adressen her. Ein Angreifer kann mittels spezieller Programme die MAC-Adresse ändern und kann – wenn er sich zumindest im selben Segment befindet – in ein Netzwerk eindringen. Durch das Spoofen von MAC-Adressen kann damit relativ einfach in ein WLAN (siehe *1.3.4.2.7 Wireless LAN-Sicherheit*) eingebrochen werden. Eine beliebte Absicherung von drahtlosen Netzen ist die MAC-Adress-Exklusivität.
- *Mail-Spoofing*: Die einfachste Art der Fälschung ist, dass sich der Angreifer einer nicht ihm gehörenden oder nicht existierenden E-Mail-Adresse bedient. Das Spoofen der E-Mail-Adresse ist

über offene Relays[206] möglich. Phishing-Attacken (siehe *1.4.1.2 Exkurs: Phishing*) bedienen sich der Technik des Mail-Spoofings.

- *URL-Spoofing*: dem Besucher wird nur die vermeintlich gewünschte Webseite angezeigt. Beispielsweise wird ihm vorgegaukelt, er ist auf http://tuwien.ac.at/ – stattdessen befindet er sich auf http://tuwien.ac.at@195.58.170.31. Möglich wird URL-Spoofing durch Sicherheitslücken in Webbrowsern.

Die geeignetste Gegenmaßnahme gegen Spoofing sind Firewalls mit Paketfilter (siehe *1.7.2.4.1 Firewall*). Im Speziellen sollte beim IP-Spoofing die Firewall Datenpakete wegwerfen, die von außen kommen, aber mit internen Quelladressen versehen sind. Auch nach außen gehende Pakete sollten gefiltert werden. Zudem bieten einige Protokolle (siehe *1.3.4.2 Protokoll- (Un) Sicherheiten*) eigene Maßnahmen gegen IP-Spoofing.

1.4.3.7 Denial of Service

Ein *Denial of Service-* (kurz: *DoS*) Angriff hat zum Ziel, Dienste zu kompromittieren und zu blockieren, damit sie nicht mehr zur Verfügung stehen. In der Regel geschieht das durch Überlastung oder Bindung der Systemressourcen.
Wird der Angriff von vielen Computern gleichzeitig durchgeführt, spricht man von einem *Distributed Denial of Service-Angriff* (kurz: *DDoS*). Die Basis dazu ist das zu Nutze machen fremder Rechner mit Hilfe von Trojanern, Backdoors etc. (siehe *1.3.4.1.1 Exkurs: Botnet*). Der Angreifer aktiviert zu einem bestimmten Zeitpunkt die Bots zu einem koordinierten, parallelen Angriff auf ein festgelegtes Ziel. Mit der entsprechenden Anzahl an Bots verfügt der Angreifer über die notwendige Bandbreite für einen Angriff. Zur Durchführung von DDoS-Attacken stehen im Internet Tools wie *Trin00*[207] oder *Stacheldraht*[208] zur Verfügung.
Unter DoS werden verschiedene Angriffsformen verstanden:

- Angriffe auf Applikationsebene: Hier wird ein Service mit Anfragen derart überhäuft, dass dieses nicht mehr oder nur mehr verzögert ausgeführt werden kann. Das kann durch eine große Anzahl von Anfragen an Webserver (HTTP-Dienst) geschehen oder durch viele voluminöse E-Mails (SMTP-Dienst).
- *Smurf-Angriffe*: der Angreifer schickt viele ICMP-Echo[209]-Anfragen, die sonst zur Prüfung der Verfügbarkeit eines Rechners verwendet werden, an Broadcast-Adressen fremder Rechnernetze. Jede dieser Anfragen wird somit an alle Clients innerhalb dieses Netzes weitergeleitet, die wieder

[206] Darunter werden SMTP-Server ohne Authentifizierungspflicht verstanden.
[207] http://www.brain-pro.de/Seiten/ddos/trinoo.tgz
[208] http://www.brain-pro.de/Seiten/ddos/stachel.tgz
[209] Internet Control Message Protocol (kurz: ICMP)-Echo wird auch als PING bezeichnet.

an die Absenderadresse antworten. Als Absenderadresse gibt der Angreifer jedoch nicht seine eigene an, sondern nimmt die Adresse des Angriffsziels (siehe *1.4.3.6 Spoofing*).

- *Ping of Death* ist ein ICMP-Paket, das Implementierungsfehler des TCP/IP-Protokolls in vielen Betriebssystemen ausnützt, um beim Empfänger einen Buffer Overflow (siehe *1.4.3.3 Buffer Overflow-Attacken*) zu erzeugen.
- *SYN-Flooding* ist die häufigste DoS-Angriffsform und nutzt die Art des Verbindungsaufbaus von TCP/IP aus. Der Verbindungsaufbau erfolgt durch Anfrage, Bestätigung und Rückbestätigung zwischen Client und Server. Gleichzeitig mit dem Bestätigen speichert der Server die Daten der Verbindung. Erhält er nun innerhalb eines bestimmten Zeitraums keine Rückbestätigung des Clients, werden die Verbindungsdaten gelöscht. Ein DoS-Angriff ist dann erfolgreich, wenn durch das laufende Versenden von Verbindungsanfragen von gespooften Clients, von denen keine Bestätigung erfolgen kann, die Kapazität der vom Server zu speichernden Verbindungsdaten überschritten wird.

Der Securityspezialist Symantec stellt in seinem Bericht für das erste Halbjahr 2006 [Symantec, 2006] fest, dass die Zahl der DoS-Attacken hoch bleibt. Symantec registrierte im Schnitt 6.110 DoS-Angriffe pro Tag, wobei Internet Service Provider am häufigsten im Visier der Angreifer standen. Während sich 2006 54 Prozent der DoS-Attacken gegen Ziele in den USA gerichtet haben, waren es im ersten Halbjahr 2007 bereits 61 Prozent [Symantec, 2007]. Die meisten Bot-Steuerungsserver stehen in den USA, die meisten Bot-Clients befinden sich in China (siehe *1.3.4.1.1 Exkurs: Botnet*).
Die US-Internetfirma *VeriSign*[210] hat bekannt gegeben, dass es Anfang des Jahres 2006 eine Welle von DoS-Attacken gegen viele Internet-Anbieter gegeben hat[211]. Eine Besonderheit der Attacken war die Art und Weise, wie Rechner zum Kollabieren gebracht wurden. Die registrierten Attacken zielten nämlich nicht direkt auf den eigentlichen Server, sondern nahmen einen Umweg über DNS (siehe *1.3.4.2.2 DNS-Sicherheit*). Bei jeder Anfrage zu einer Webseite wurde von einem DNS-Server die gesuchte URL einer IP-Adresse zugeordnet. Da die Absenderadressen gespooft (siehe *1.4.3.6 Spoofing*) waren, liefen die Antworten ins Leere und erzeugten dadurch bis zu 63 Mal mehr Daten als üblich. Bei einigen Attacken waren bis zu 32.000 DNS-Server involviert.
Mit dem Trojaner „Storm Worm“ wurde im Jahr 2007 ein Botnet von weltweit 1,8 Millionen infizierten Computern errichtet. Ziel war es, dieses an Spammer und Phishing-Betrüger zu vermieten oder selbst erpresserisch tätig zu werden. Vor allem Internet-Wettanbieter wurden und werden mit einer 50.000 Dollar-Forderung konfrontiert, um eine DDoS-Attacke abzuwenden[212].

[210] http://www.verisign.com/ [27. März 2007]
[211] Vgl. http://www.computerwoche.de/knowledge_center/it_security/573593/index.html [27. März 2007]
[212] Vgl. http://www.zdnet.de/security/news/0,39029460,39157537,00.htm [12. März 2008]

1.4.3.7.1 DDoS-Angriff auf Estland

Der Sicherheitsbeauftrage von Estland, *Ivar Tallo,* berichtet[213] von einem DDoS-Angriff auf das Land Estland im Mai 2007, er spricht in diesem Zusammenhang sogar von einem „*Cyberwar*" [Tallo, 2007, S 17f]. Seiner Darstellung nach wurden zunächst Regierungssysteme und Portale von Massenmedien und Internetserviceprovidern kompromittiert. Weiters versuchten die Attacken wichtige Telekombetriebe und Banken ebenso wie die elektronische Infrastruktur in Form von SMTP- und DNS-Servern lahm zu legen. Die Angriffe erfolgten unter Zuhilfenahme von Botnets anfänglich sporadisch, dann koordiniert. Erreicht wurde, dass der internationale Internettraffic Estlands nicht mehr funktionierte, dass innerhalb des Landes etliche Web Services nicht zur Verfügung standen und der elektronische Zahlungsverkehr zum Erliegen kam. Als Erkenntnisse des Angriffs wurde von der Regierung folgendes festgehalten:

- *We have become to rely on Internet much more than we realize.*
- *Crisis raises Internet use many times, not just percentages.*
- *We don't have international mechanism to deal with it.*

Ein vollständiger Schutz gegen DoS-Angriffe ist nicht möglich. Ein hohes Schutzniveau kann durch mehrere, auch kombinierte Maßnahmen in der organisatorischen und technischen Prävention und Systemüberwachung bzw. in der Reaktion erreicht werden.
Kritische Applikationen (z. B.: Onlinebanking) und Funktionalitäten (z. B.: Firewall) sollten redundant auf mehrere Systeme mit unterschiedlichen Zugängen, aber der gleichen IP-Adresse, aufgeteilt werden (siehe *1.3.2.2 Gegenmaßnahmen*). Der Angreifer müsste nun alle Zugangsmöglichkeiten ausschalten. Eine weitere Maßnahme ist die Aufteilung in Teil- oder Subnetze. Technisch bieten Filter (siehe *1.7.2.4 Perimetersicherheit*) einen probaten Schutz. So kann etwa ein Verbot von Ping-Anfragen Smurf-Attacken (siehe oben) verhindern. Router können – nach der Idee von *TCP-Interception* – so konfiguriert werden, dass sie Datenpakete erst nach einer Überprüfung der Existenz der Absenderadresse weiterleiten, somit können gespoofte IP-Pakete abgewiesen werden. TCP-Interception ist enorm ressourcenintensiv und kann somit auch den Router an die Kapazitätsgrenze bringen.
Systemüberwachung durch Intrusion Detection Systeme (siehe *1.7.2.4.4 Intrusion Detection Systeme und Intrusion Prevention Systeme*) ist ein wesentlicher Faktor zur Bekämpfung von DoS-Attacken. Im Zusammenspiel mit einer Firewall können Datenpakete erkannt und blockiert werden. Ist ein DoS-Angriff trotz aller Anstrengungen dennoch erfolgreich, sollte ein Notfallplan (siehe *1.7 Schutzmaßnahmen und Gegenstrategien*) existieren.

[213] Der Autor konnte im Mai 2007 im Rahmen einer Konferenz die Ausführungen und Diskussionen betreffend Cyberwar live mit verfolgen.

Beachtet werden sollte, dass ein DoS-Angriff oft nur als Ablenkungsmanöver eingesetzt wird. Durch die Konzentration der personellen und technischen Ressourcen auf die Abwehr werden andere Wege und Möglichkeiten eröffnet, einen andersartigen Angriff zu lancieren.
Das Paradoxe an (D)DoS-Angriffen ist, dass diese auch diejenigen treffen können, die sich sonst gut vor Eindringlingen aus dem Internet schützen. Das Problem sind jene Rechner, auf denen keine oder nur sehr wenige Grundschutzmaßnahmen (Antivirus etc.) umgesetzt sind. Diese Benutzer exponieren sich zum einen selbst den Gefahren aus dem Internet, zum anderen stellen sie auch für alle anderen Computer im Internet eine latente Gefahr dar. Daher sollte der PC zumindest durch Antivirusprogramm und Personal Firewall gesichert werden, um zu verhindern, dass er als Bot für (D)DoS-Angriffe auf andere Opfer missbraucht wird (siehe *1.7.1.3 Grundsätze im Umgang mit PCs zum Schutz vor Malicious Code*).

1.4.3.8 Hacking

Im Folgenden Beispiele für Hacking[214], die sich der in diesem Kapitel vorgestellten Techniken und Methoden bedienen.

Beispiel 1: Sniffing von SSL-Verbindungen
Beim Onlinebanking verlassen sich die Anwender in der Regel auf das Vorhandensein verschlüsselter Verbindungen. Dabei handelt es sich oft um eine trügerische Sicherheit, da die Verschlüsselung zwar sicherstellt, dass die versendeten Informationen von einem Angreifer nicht gelesen werden können, aber keinesfalls sichergestellt ist, dass der Benutzer mit dem gewünschten Partner kommuniziert. Durch DNS-Spoofing wird der Onlinebanking-User auf einen anderen Server umgeleitet. Zum Aufbau einer verschlüsselten SSL-Session werden zunächst die Public Keys (in der Grafik mit $PubKey_{nn}$ dargestellt) (siehe *1.7.2.1.5* Public Key Infrastructure) ausgetauscht. Der Hacker sorgt als Man In The Middle dafür, dass Client und Server jeweils die Public Keys des Hackers bekommen:

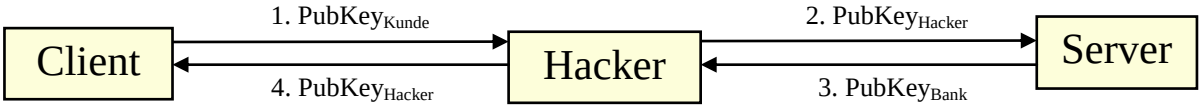


Abbildung 14: Public Key-Austausch

Der ahnungslose Benutzer gibt beim Onlinebanking seine Zugangsdaten (Verfügernummer, PIN) ein und schickt sie verschlüsselt mit dem Key des Hackers ab (in der nachfolgenden Grafik steht V für

[214] Zusammengestellt aus persönlichen Notizen und Konferenzunterlagen; http://www.idc-austria.at/index.php?showproduct=28053&content_lang=DE [12. März 2008]

Verschlüsselung). Der Hacker entschlüsselt die Verfügernummer und die PIN mit seinem Private Key (in der Grafik als E für Entschlüsselung mit $PrvKey_{nn}$ dargestellt) und verschlüsselt sie mit dem Public Key der Bank. Der Benutzer kann wie gewohnt mit seiner Bank kommunizieren, aber der Hacker liest mit:

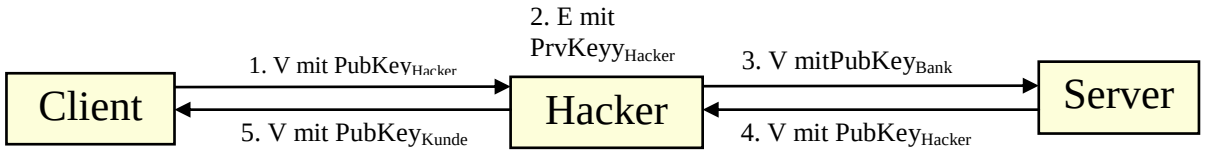


Abbildung 15: Übermittlung Zugangsdaten

Der Man In The Middle-Angriff kann nur gestoppt werden, wenn das X.509-Zertifikat (siehe *1.7.2.1.6 Digitale Zertifikate*) überprüft wird, welches die Identität des Webservers bestätigen soll. Das Zertifikat, muss sich unter den vertrauenswürdigen Stammzertifizierungsstellen des Webbrowsers befinden.

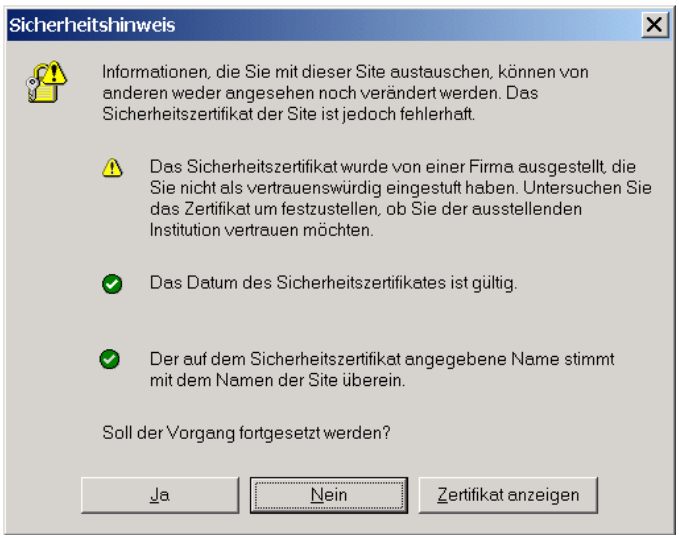


Abbildung 16: Überprüfung Zertifikat

Beispiel 2: Trojaner

Ein viel und gern verwendetes Werkzeug, um Zugriff auf fremde Systeme zu erhalten, ist der Trojaner (siehe *1.3.4.5 Trojanisches Pferd*). Ist ein Rechner mit einem Trojaner verseucht, wird über das Internet von einfachen Aktionen am PC bis hin zur Industriespionage vieles ermöglicht: Löschen von Dateien, Anzeigen des Bildschirminhalts, Ausspionieren von Tastatureingaben oder Kopieren von vertraulichen Dateien. Verfügt der überwachte Computer über ein Mikrophon, so lässt sich dieses als Wanze einsetzen, die über das Netzwerk abgehört werden kann.

Unter den Trojanern gibt es einige mit undokumentierten Merkmalen, wie beispielsweise *Cofeini*[215]. Das spezielle Feature ist, dass diese Trojaner die vom Angreifer gesammelten Informationen im Hintergrund selbstständig per E-Mail an Dritte weiterschicken. Damit wird der Angreifer selbst zum „Opfer".

Viele Benutzer wähnen sich vor Trojanern in trügerischer Sicherheit, weil sie Virenschutz und Personal Firewall im Einsatz haben. Zum einen erkennen Antivirenlösungen nur bekannte Trojaner, zum anderen lassen sich selbst restriktiv konfigurierte Firewalls umgehen. Beispielsweise kann mittels Firewall gesteuert werden, dass Microsofts E-Mail-Client *Outlook* nur auf den *SMTP*[216]- und *POP3*[217]-Port zugreifen darf. Um im konkreten Fall Zugriff zu erhalten und dabei die Personal Firewall zu täuschen, benennt der Trojaner einen seiner Prozesse einfach auf *Outlook.exe* um.

Beispiel 3: Attacken auf Webapplikationen

Da Webapplikationen meist Individuallösungen sind, gestalten sich die Angriffe auf diese anspruchsvoll. Automatisierte Scanner sind demnach nicht geeignet, solche Applikationen zu testen. Es zeigt sich, dass die Entwickler von Weblösungen oftmals zu wenig Fokus auf Sicherheit legen. Die auf dem Markt verfügbaren Webserver wie *Apache*[218] oder *Internet Informationsserver* (*IIS*)[219] haben oft selbst Programmschwachstellen oder sind unzureichend konfiguriert.

Der grundlegende Fehler besteht darin, den Eingabedaten des Anwenders ungeprüft zu vertrauen (siehe *1.4.3.5 Webapplication-Attacken*). Beim Onlinebanking kann ein Kunde seine Konten online verwalten. Jedes Konto wird durch eine eindeutige Kontonummer identifiziert. Meldet sich der Kunde bei seiner Bank an, so werden ihm die Namen und Nummern seiner Konten aufgelistet. Bei Auswahl eines der Konten wird per HTTP die jeweilige Kontonummer zur Bank geschickt. Standardmäßig ist es dem Kunden nicht möglich, Zugriff auf ein fremdes Konto zu erlangen. Modifiziert ein böswilliger Kunde aber die HTTP-Kommunikation (siehe *1.3.4.2.3 HTTP-Sicherheit*), ist er in der Lage, eine fremde Kontonummer zur Bank zu schicken – und erhält unter der Voraussetzung einer unzureichenden Sicherheitsabfrage der Webapplikation Zugriff auf ein fremdes Konto.

[215] Vgl. http://www.sophos.de/security/analyses/trojcafeini11.html [12. März 2008]
[216] Das Simple Mail Transfer Protocol (kurz: SMTP) dient zum Austausch von E-Mails.
[217] Post Office Protocol Version 3 (kurz: POP3) dient dazu, dass ein Client E-Mails von einem Server abholen kann.
[218] http://httpd.apache.org/download.cgi [12. März 2008]
[219] http://www.microsoft.com/WindowsServer2003/iis/default.mspx [27. März 2007]

Beispiel 4: Google-Hacking

Durch Konfigurationsfehler von Systemen kommt es immer wieder vor, dass vertrauliche Unternehmensdaten ungewollt und ungeschützt im Internet verfügbar sind. Unter Anwendung geschickter Google-Recherchen kann man gezielt nach solchen Dateien suchen. Mit den angeführten Grundbefehlen lässt sich mit der Google-Suchmaschine eine Reihe von interessanten Informationen gewinnen[220].

„*inurl*“: Suche nach Text innerhalb der URL.

„*intitle*“: Suche nach Text innerhalb des Seitentitels und der HTMLtags.

„filetype“: die Suche auf bestimmten Dateityp anhand der Dateinamenserweiterung einschränken.

„intext“: Suche auf den Text beschränken, z. B.: Text innerhalb von Links nicht beachten.

„*site*“: Suche auf einen Server oder eine Domain einschränken.

So kann etwa mit den Befehlen „*inurl:/_vti_pvt/users.pwd*“ oder „*filetype:log id password*“ nach Passwörtern gesucht werden. Mit „*allinurl: view indexframe shtml*“, „*intitle:"Live View / – AXIS"*“ oder „*inurl:LvAppl intitle:LiveApplet*“ lassen sich beispielsweise Webcams finden.

Selbst Preise bei der Bestellung in Webshops können etwa durch die Eingabe von „*allinurl: preis warenkorb*“ und ein paar Handgriffen verändert werden. Ob eine Preisänderung durchgeführt werden kann, sieht man, indem man auf einer so gefundenen Webseite zur Produktauswahl geht und beim Anklicken eines Produkts die Statusleiste am unteren Fensterrand beobachtet. Wird in dieser neben der Produktbezeichnung auch der Preis angeführt, ist eine Veränderung möglich:

Abbildung 17: Google-Hacking Anzeige des Preises

[220] Vgl. http://johnny.ihackstuff.com/ghdb.php [10. März 2007]

Der nächste Schritt ist dann beim Button „Hinzufügen des Produkts zum Warenkorb“ über die rechte Maustaste „Verknüpfung kopieren“ auszuführen und die Kopie dieser Daten in das Eingabefeld des Browsers einzufügen.

Abbildung 18: Google-Hacking Änderung des Preises

Danach ist lediglich der Preis beliebig zu ändern und die Bestellung könnte mit dem reduzierten Preis ganz normal durchgeführt werden.

1.4.4 ZUGRIFFSERHALTUNG

Hat der Angreifer Zugriff zu einem System erlangt, ist es meist von Interesse, diesen auch aufrecht zu erhalten [Weippl, 2004, Threats and Countermeasures, S 29]. Dazu dienen die vorgestellten Techniken und Tools wie Trojaner (siehe *1.3.4.5 Trojanisches* Pferd), Backdoors und Rootkits (siehe *1.4.3.2 Backdoor/Rootkit*).

1.5 EXKURS: MOBILES ARBEITEN

Mobile Arbeit – im Sinne der Ausübung seiner Tätigkeit außerhalb der Schul- und Büroräumlichkeiten – findet immer größere Bedeutung in der Ausbildungs- und Arbeitswelt[221]. *Mobile Enterprise*, *mobile Worker*, *mobile Distribution* oder *E-Learning* sind Begriffe für die Integration von mobilem Arbeiten in die Arbeitsprozesse. Durch den Einsatz von Mobilkommunikation (Notebook, PDA etc.) bestehen beachtliche Potenziale zur Effizienzsteigerung und zur Erhöhung der *Work-Life-Balance* von Mitarbeitern. Viele Arbeiten werden direkt beim Kunden oder unterwegs beziehungsweise von zuhause ausgeführt. Informationen gelangen schnell und unmittelbar zum Ort der Leistungserbringung. Das Management von Informationen und der dafür notwendigen Infrastruktur erfährt einen fundamentalen Wandel.

Ansatzpunkte für mobiles Arbeiten gibt es in den verschiedensten Bereichen der Wertschöpfungskette innerhalb eines Unternehmens. Auf der Versorgungsseite ermöglicht mobiles Versorgungsketten-Management (engl. *mobile Supply Chain Management*) [SAP, 2005] verkürzte Lieferzeiten durch eine optimierte Lagerhaltung. Typische Einsatzfelder sind etwa das Flottenmanagement oder die Warenverfolgung mit RFID[222] (siehe *2.3.3.3 RFID*). Betriebsintern kann durch mobile Unternehmensressourcenplanung (engl. *mobile Enterprise Ressource Planning*) [Teuteberg, Hilker, Kurbel, 2003] eine Prozessoptimierung erreicht werden. Beispielsweise erhöht der Einsatz von Wireless LAN (siehe *1.5.4 Local Area Network*) bei der Visite in Krankenhäusern die Effizienz der Behandlung. Auf der Absatzseite können ebenfalls Produktivitätssteigerungen erreicht werden.

[221] Vgl. http://www.onforma.de/ [12. März 2008]

Klassisches Beispiel ist der ortsunabhängige Zugriff des mobilen Außendienstes auf Kunden-, Vertrags- oder Lagerdaten.

Europäische Unternehmen erwarten für die kommenden Jahre eine zunehmende Verbreitung von mobilem Arbeiten[223]: Die Zugriffsmöglichkeit auf Unternehmensinformationen unabhängig vom Aufenthaltsort des Anwenders kann dessen Produktivität und Motivation signifikant erhöhen, in Summe steigert das die Effizienz eines Unternehmens. E-Mail und Kalender sind die am meisten per Fernzugriff genutzten Anwendungen, zugleich werden die Potenziale des Zugriffs auf Unternehmensdatenbanken und Recherche-Instrumente noch nicht ausgeschöpft. Laut dieser Studie (Herbst 2005) haben in Deutschland 56 Prozent der befragten Unternehmen Mitarbeiter, die von zuhause aus arbeiten.

Eine Befragung[224] des britischen Unternehmens *Sirenic*[225] im September 2006 hat ergeben, dass 70 Prozent der Befragten meinten, produktiver und effizienter bei flexibleren Arbeitsabläufen arbeiten zu können, aber nur knapp die Hälfte der britischen Unternehmen bietet mobiles Arbeiten an. Oft fehlt in den Führungsebenen der Unternehmen das Grundverständnis für die Voraussetzungen mobilen Arbeitens.

1.5.1 ARBEITSPLATZ DER ZUKUNFT

Forscher des deutschen *Fraunhofer Instituts für Arbeitswirtschaft und Organisation*[226] beschäftigen sich im Rahmen des Projektes „Office 21“ mit den Arbeitsabläufen und dem Arbeitsplatz des 21. Jahrhunderts. Bis 2020 werden etwa 80 Prozent der Arbeitnehmer mobile Arbeitnehmer (engl. *mobile Worker*) sein[227].

Im „Office 21 Showcase“ präsentieren die Wissenschaftler ihre Vorstellung von einem modernen Arbeitsplatz. Der Arbeitsplatz ist in ein Bürosystem eingebunden, in dem die Ressourcen je nach Bedarf verteilt werden. Der Mitarbeiter meldet sich mittels RFID-Karte oder PIN-Code am Platz an und kann ihn so für die gewünschte Zeit reservieren. Er findet seine bevorzugten Einstellungen sowohl am Computer wie auch am Telefon vor. Zum Einsatz soll der entwickelte Arbeitsplatz vor allem in Unternehmen kommen, deren Mitarbeiter sehr oft im Außendienst unterwegs sind. Wenn der Angestellte einen Büroplatz benötigt, findet er immer die besten Voraussetzungen und eine gute Infrastruktur vor. Zum anderen wird das Büro auch entsprechend den Erfordernissen ausgelastet. Im Optimalfall gäbe es weder Leerlaufzeiten, noch unbesetzte Arbeitsplätze oder ungenutzte Hardware.

[222] Vgl. http://www.eweek.com/article2/0,1759,1567819,00.asp [10. März 2007]
[223] Vgl. http://www.citrix.de/unternehmen/presse/pressemeldungen/2005/10/13_2/ “Mobile Working Within Major Blue Chip Companies “ Oktober 2005 [12. März 2008]
[224] Vgl. http://www.businessportal24.com/de-ch/Markt_Arbeiten_Potenzial_56019.html [27. März 2007]
[225] http://www.sirenic.com/ [10. März 2007]
[226] http://www.iao.fraunhofer.de/ [12. März 2008]
[227] Vgl. http://www.futurefoundation.net/ „The Future of Teleworking“ [12. März 2008]

Zentrales Element des „Office 21“-Arbeitsplatzes ist ein drehbarer Tisch und drei Monitore. Der Tisch dient entweder als Arbeitsfläche für eine Person oder er wird gedreht, um für ein Meeting Platz zu schaffen (In Studien wurde herausgefunden, dass die meisten Treffen mit zwei bis vier Teilnehmern ablaufen). Ein Monitor allein bietet sehr wenig Platz, daher wurden drei Displays nebeneinander in einen Arbeitsplatz integriert. Somit kann auf einem Schirm der E-Mail-Posteingang angezeigt werden, auf dem zweiten bleibt man mit Arbeitskollegen via Webkonferenz verbunden und auf dem dritten laufen die Programme, mit denen gerade gearbeitet wird. Im Teamwork-Modus können zusätzliche Notebooks einfach an das System angeschlossen werden. Ein Bildschirm wird dem tragbaren Computer zugeordnet, wodurch jeder Meetingteilnehmer einen direkten Blick auf den Bildschirm hat. Im Rahmen der Untersuchungen zum Projekt „Office 21“ ergründeten die Wissenschaftler auch Faktoren zur effizienten Gestaltung des Arbeitsprozesses von mobilen Mitarbeitern. Einen bestimmenden Faktor habe dabei die IT-Qualität, die direkt auf die Arbeitsleistung wirkt, jedoch nur wenn Mitarbeiter damit korrekt umgehen können, meinen die Studienautoren.

1.5.2 UBIQUITÄRES COMPUTING

In einer vom *Deutschen Bundesministerium für Bildung und Forschung* (kurz: *BMBF*) in Auftrag gegebenen Studie[228] wurde die Akzeptanz der Bevölkerung gegenüber der Technikentwicklung im Informationssektor untersucht. Vor dem Hintergrund immer kleinerer und leistungsstärkerer Computersysteme kommt die Studie zu dem Ergebnis, dass die Menschen in Deutschland grundsätzlich bereit sind, sich auf Technologien mit allgegenwärtiger Datenverarbeitung einzulassen. Die Studie mit Namen „Technikfolgenabschätzung – Ubiquitäres Computing und informelle Selbstbestimmung (TAUCIS)" wurde vom *Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein*[229] und dem *Institut für Wirtschaftsinformatik der Humboldt-Universität Berlin*[230] erarbeitet: Die Informationstechnik von morgen wird unsichtbar und allgegenwärtig. Ein Trend ist der steigende Einsatz immer kleinerer Rechner. Der Computer, in der heute eingesetzten Form, wird nach Einschätzung der Experten zum Auslaufmodell. Die Menschen sind bereit, allgegenwärtige Datenverarbeitung zu akzeptieren. Bedingungen sind jedoch, dass der Datenschutz gewährleistet ist, die Technik sicher und anwenderfreundlich sowie die Nutzung nicht verpflichtend ist. Ubiquitäres Computing umschreibt den Einsatz von kleinen Sensoren und Prozessoren in Produkten für den Alltag, die miteinander kommunizieren und bei Bedarf bestimmte Aktionen auslösen. Gegenstände werden dadurch „intelligent“ und können die Menschen in vielen Bereichen des alltäglichen Ablaufs unterstützen. Dazu zählt beispielsweise das Verfolgen von Waren in der Logistikbranche (siehe *2.3.3.3 RFID*). Beim Auto können Chips im Fahrzeugschlüssel nicht nur zum Bezahlen an der Tankstelle

[228] Vgl. http://www.bmbf.de/press/1890.php Oktober 2006 [26. März 2007]
[229] http://www.datenschutzzentrum.de/ [12. März 2008]
[230] http://www.wiwi.hu-berlin.de/Professuren/quantitativ/wi [12. März 2008]

dienen, sondern auch für die automatische Einstellung von Spiegel, Sitzhöhe und Klimaanlage nach den Vorlieben und Bedürfnissen des Fahrers sorgen. Intelligente Häuser erkennen ihre Bewohner, aktivieren pünktlich Wecker und Kaffeemaschine, drehen Lieblingsmusik auf und blenden individuelle Nachrichten ein.
Parallel zu diesen Entwicklungen müssen die Sicherheitsmaßnahmen weiter verbessert werden. Eine Strukturierung der Einsatzmöglichkeiten bzw. -geräte erfolgt anhand der Reichweite der Sendegeräte.

1.5.3 PERSONAL AREA NETWORK

Unter einem *Personal Area Network* (kurz: *PAN*) versteht man ein Netz, welches zwischen Geräten wie Mobiltelefonen, PDAs, Notebooks oder Drucker ad-hoc aufgebaut werden kann. PANs können daher mittels drahtgebundener (USB, FireWire[231]) oder mittels drahtloser Techniken (Infrarot, Bluetooth, RFID (siehe *2.3.3.3 RFID*)) etabliert werden. Die Reichweite ist auf wenige Meter begrenzt. Neben den kaum vorhandenen Sicherheitsvorkehrungen auf Clientseite – abgesehen von den am PC vorhandenen – gibt es vor allem bei den drahtlosen Kommunikationstechniken Angriffsmöglichkeiten.
Näher eingegangen werden soll auf Bluetooth. Es gibt laufend Berichte über Schwachstellen in der Bluetooth-Technik: die Möglichkeiten mittels Methoden wie *bluesnarfing* oder *bluejacking* reichen vom Auslesen privater Kontaktdaten bis hin zu Angriffen auf Freisprecheinrichtungen. Durch eine nicht-verpflichtende Verschlüsselung, unsichere Voreinstellungen von Herstellerseite, schwache PINs, unsichere Geräteschlüssel etc. ist es Unbefugten möglich, Bluetooth-Einheiten für den Zugriff auf private Daten zu missbrauchen.
Konkret bietet Bluetooth drei Sicherheitsfunktionen [Drecker, Pohlmann, 2006], die eine geschützte Kommunikation ermöglichen sollen. Beim erstmaligen Verbinden – *Pairing* – zweier Geräte wird ein sogenannter Verbindungsschlüssel erstellt. In diesem Schlüssel wird ein *Preshared Secret* eingebaut, das maßgeblich das Sicherheitsniveau beeinflusst. Authentifikation und Verschlüsselung sind weitere Sicherheitsfunktionen, wobei beide den Verbindungsschlüssel und eine Zufallszahl als Parameter nutzen. Da der Sicherheitslevel des Verbindungsschlüssels vom Preshared Secret bestimmt wird, sollte dieses mit der notwendigen Sensibilität behandelt werden.
Das deutsche BSI [BSI, 2003] empfiehlt die Einhaltung folgender Grundsätze: Es ist empfehlenswert, die vom Hersteller voreingestellte, oft unsichere Konfiguration zu überprüfen. Nicht benötigte Dienste sollten deaktiviert werden, um die Geräte so wenig wie möglich angreifbar zu machen. Die Sendeleistung sollte entsprechend des Funktionalitätsbedarfs eingestellt werden. Der PIN sollte ein möglichst langer und zufälliger sein. Im Falle einer Verschlüsselung ist darauf Bedacht zu nehmen, dass die Schlüssellänge mindestens 64 Bit beträgt und als Verschlüsselungsmodus nur Punkt-zu-Punkt

[231] FireWire (auch IEEE 1394) ist eine Schnittstelle zum Datenaustausch zwischen Computern und Zusatzgeräten.

akzeptiert wird. Weiters wird empfohlen, Maßnahmen im Bereich der Client Security (Virenschutz, Firewall, lokale Datenverschlüsselung etc.) zu setzen.

1.5.4 LOCAL AREA NETWORK

Lokale Netze (engl. *Local Area Network* (kurz: *LAN*)) sind ein Zusammenschluss von gleichberechtigten Rechnern und Peripheriegeräten für den Datentransfer auf einem räumlich begrenzten Gebiet. LANs können entweder drahtgebunden (Ethernet[232], Token Ring[233] und FDDI[234]) oder drahtlos (WLAN) arbeiten. Ein LAN kann sowohl im Heimbereich als auch innerhalb eines Betriebes eingerichtet werden, die Distanzen erstrecken sich demnach auf ein Gebäude oder einen Unternehmensstandort. Wireless LAN birgt die meisten sicherheitstechnischen Schwachstellen (siehe *1.3.4.2.7 Wireless LAN-Sicherheit*).

1.5.5 WIDE AREA NETWORKS

Weitverkehrsnetze (engl. *Wide Area Network* (kurz: *WAN*)) sind für die Sprach- oder Datenübertragung über weite Strecken konzipiert. Diese Netze sind in Industrieländern flächendeckend aufgebaut und werden für die geschäftliche wie private Kommunikation genutzt. Als Beispiele können das klassische analoge Telefonnetz ebenso erwähnt werden wie *ATM*[235] oder *Frame Relay*[236].

Neben diesen klassischen Leitungsformen sind kabellose Technologien wie *UMTS*[237] oder *WiMax*[238] als Beispiele anzuführen. Diese werden oft in der Definition von WAN nicht erwähnt, obwohl durch sie ebenso eine Datenübermittlung unternehmensübergreifend und über große Distanzen ermöglicht wird. Aus sicherheitstechnischer Sicht sind diese Technologien mit WLAN vergleichbar (siehe *1.3.4.2.7 Wireless LAN-Sicherheit*).

[232] Ethernet umfasst sowohl die physische Schicht (Kabeltypen, Stecker) als auch die Verbindungsschicht (Signalisierung, Protokolle) (siehe Abbildung 4: Protokolle des OSI-Schichtenmodells). Ethernet ist in der IEEE-Norm 802.3 standardisiert.

[233] Token Ring ist wie Ethernet eine Vernetzungstechnologie gemäß den OSI-Schichten 1 und 2, standardisiert in der Spezifikation IEEE 802.5.

[234] Fiber Distributed Data Interface (kurz: FDDI) ist eine ANSI-standardisierte Netzwerkarchitektur für lokale Netzwerke auf Basis Glasfaserkabel.

[235] Asynchronous Transfer Mode (kurz: ATM) ist eine vermittelnde, verbindungsorientierte WAN-Technologie. Mit ATM können Daten (Sprache, Audio, Video, interaktives Fernsehen etc.) in unterschiedlichen Übertragungsgeschwindigkeiten und Diensten realisiert werden.

[236] Frame Relay ist eine datenpaketorientierte Übertragungstechnik für Punkt-zu-Punkt-Verbindungen.

[237] Universal Mobile Telecommunications System (kurz: UMTS) ist ein standardisiertes System für die Mobilfunk-Kommunikation. Durch hohe Übertragungsraten und Dienste wie Multimedia soll der bisherige Standard Global System for Mobile Communications (kurz: GSM) abgelöst werden.

[238] Worldwide Interoperability for Microwave Access (kurz: WiMAX) ist ein Standard nach IEEE 802.16. Mit dieser Technik werden Internet-Breitbandzugänge via Funk angeboten.

1.6 EXKURS: E-MAIL/SPAM

Dem Medium E-Mail kommt sowohl im privaten wie unternehmerischen Umfeld eine immer wichtiger werdende Rolle zu. Betriebe nutzen E-Mail zunehmend für den Austausch unternehmensrelevanter Information, damit haben sie vitales Interesse, die Verfügbarkeit, Integrität und Vertraulichkeit der E-Mails sicherzustellen. Mit der steigenden Verwendung von E-Mail steigt auch der Missbrauch. Mittels E-Mails können Falschmeldungen (engl. *Hoaxes*) lanciert werden, oder kann Malware (siehe *1.3.4 Computer Anomalien/Malicious Code*) mitgeliefert werden. Des weiteren können E-Mails als Medium zur unberechtigten Informationsbeschaffung (siehe *1.4.1.2 Exkurs: Phishing*) missbraucht werden, zudem widerrechtlichen Inhaltes sein und unerwünscht zugestellt werden (*Spam*). Eine weitere Gefahrenquelle können E-Mail-Verteiler darstellen. Es kommt nicht selten vor, dass Verteiler noch Adressen von Personen enthalten, die nicht mehr zum Empfängerkreis gehören sollten. So haben beispielsweise Mitarbeiter eines deutschen IT-Unternehmens über Monate hinweg unbewusst Geschäftspläne an einen unautorisierten externen Partner gesendet, da dieser noch auf dem Verteiler stand.

Spam definiert sich demnach als unverlangt zugesandte Massen-E-Mail[239] (engl. *unsolicited bulk E-Mail*). Gesetzlich geregelt wird der Umgang mit den unerwünschten E-Mails im §*7 E-Commerce-Gesetz* (aus 2002) (kurz: *ECG*)[240] und in *§101 Telekommunikationsgesetz 1997* (kurz: *TKG*) (alte Rechtslage) bzw. *§107 TKG 2003*[241] (neue Rechtslage). Die österreichische Rechtslage zur E-Mail-Werbung ist unübersichtlich[242]: Von 1. August 1997 bis 19. August 2003 galt das TKG laut *BGBl. I Nr. 100/1997* (zuletzt geändert durch *BGBl. I Nr. 32/2002*), das in § 101 Anrufe – einschließlich dem Senden von Fernkopien – zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers generell untersagte; ab 19.8.1999 (*BGBl. I 188/1999*) galt das auch für E-Mails (*opt-in-Prinzip*). Dann trat am 1.1.2002 parallel dazu das ECG in Kraft, das in §7 ebenfalls eine Regelung gegen E-Mail-Werbung enthält. Diese Bestimmung untersagt E-Mail-Werbung nur dann, wenn sich der Empfänger in eine Liste bei der *RTR-GmbH*[243] eintragen läßt (*opt-out-Prinzip*). Mit dem TKG 2003 (in Kraft seit 20.8.2003) wurde das opt-in-Prinzip in §107 TKG gelockert; Werbung ohne vorherige Zustimmung an Unternehmer wurde zulässig. Mit dem Inkrafttreten der *TKG-Novelle 2005* am 1. März 2006 wurde die Ausnahme für Unternehmer wieder beseitigt [Kraft, 2006, S 252f]. Durch die TKG-Novelle 2005 wurde der Tatbestand des §7 ECG in §107 Abs. 3 übernommen, sodass dort nunmehr die Werbe-E-Mail umfassend geregelt ist. Damit sind Werbe-Mails nur mehr bei vorheriger Zustimmung und Vorliegen der Voraussetzungen nach §107 Abs. 3 zulässig.

[239] Vgl. http://www.spamhaus.org/definition.html [8. März 2008]
[240] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: ECG §7 [10. März 2007]
[241] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: TKG §107 [10. März 2008]
[242] Vgl. http://www.internet4jurists.at/e-mail/oe1.htm [8. März 2008]
[243] Vgl. http://www.rtr.at/ Rundfunk und Telekom Regulierungs-GmbH [8. März 2008]

Der russische IT-Sicherheit-Spezialist Kaspersky Lab konstatiert einen Trend weg von Viren hin zu Spam[244]. Unterstützt wird diese Aussage durch die *Threat-Statistik* von Messagelabs[245]. Von Dezember 2005 bis Dezember 2006 ist der Prozentsatz von Viren von 7 Prozent auf 0,3 Prozent gefallen, hingegen der Spamanteil bei den E-Mails gestiegen, er liegt bei 57 Prozent. Der Spamanteil hat sich laut Jahresbericht für 2007 von Messagelabs [Messagelabs, 2007] auf 84,6 Prozent erhöht. Zudem verweist der Bericht auf neue Spam-Techniken: „*Spam has become more inventive. In 2007 spammers waged stock pump-and-dump campaigns on the public using Adobe Acrobat PDF format files in order to evade traditional defenses. Later in the year this moved-up a gear by using other file attachment formats, including Microsoft Excel, Word, ZIP and more notably, MP3*." Für das Jahr 2008 wird folgende Entwicklung erwartet: „*The cyber-criminals toolboxes will continue to expand as more file attachments and approaches are adopted. Towards the end of 2007 we saw MP3 files used for the first time for stock spam purposes. MessageLabs experts predict that video file formats will be the next on the cyber-criminals list of scams, and spammers will follow the example of malware writers with PowerPoint attachments. With spam levels now averaging 75 percent of all email traffic, Instant Messaging (IM) was expected to be on the spammers list of targets for 2007. In reality this did not live up to expectations so the predicted increase in IM attention is now poised to be an actuality in 2008. As spammers learn from the virus writers targeted approach, MessageLabs predicts that spam will increase in intelligence during 2008. Spam-run sizes will remain vast but the content will be more targeted and stickier with the end goal of increasing the currently very low conversion rate*."

Laut einer vom Marktforscher *Marketagent*[246] durchgeführten Studie[247] im Jänner 2007 fühlen sich knapp 80 Prozent der im Internet aktiven Österreicher durch Spam zumindest gestört, 45 Prozent sogar stark belästigt. Insgesamt verbringen österreichische Internetbenutzer mehr als 350.000 Stunden pro Tag mit dem Löschen von Spam-E-Mails. In Summe kursieren in Österreich täglich rund 70 Millionen Spam-E-Mails, durchschnittlich erhalten die rund vier Millionen Internet-User 16,4 Spam-E-Mails pro Tag.

Ein interessanter Umstand ist, dass lediglich 200 Spammer 80 Prozent aller Spam-E-Mails in den USA und Europa verursachen[248]. Spamhaus zufolge lässt sich der Großteil des Spamaufkommens weiterhin auf die USA zurückführen, auch wenn die verantwortlichen Verursacher ihre Spuren über ständig wechselnde *Aliase*[249] und Domainadressen geschickt verwischen. Ein beliebter Trick, um Spuren zu verwischen, ist die Tarnung als Internet Service Provider.

[244] Vgl. http://www.viruslist.com/de/analysis?pubid=167696592 [27. Feber 2007]
[245] Vgl. http://www.messagelabs.com/Threat_Watch/Threat_Statistics [8. März 2008]
[246] http://www.marketagent.com/ [28. Feber 2007]
[247] Vgl. http://www.itirol.at/news/7746.html?style=textonly [28. Feber 2007]
[248] Vgl. http://www.spamhaus.org/rokso/ [27. März 2007]
[249] Kunstname; Nickname

Die Bedeutung von Spam lässt sich anhand einer Studie der *University of Oxford-Internet Institute*[250] ausmachen. Diese kommt zu dem Ergebnis, dass Spam-E-Mails, die Empfänger zum Kauf von Wertpapieren motivieren wollten, tatsächlich nachweisbare Wirkung auf die Aktienkurse gehabt haben. Im Großteil der Fälle wurden die Aktien nicht auf den großen Börsen gehandelt und waren meist illiquid. Die sogenannten „*Pink Sheets*" waren also nur im Freiverkehr erhältlich, das heißt, nicht offiziell zum Handel zugelassen, und nur durch Telefonverkehr mit Banken zu bekommen. Diese Wertpapiere werden üblicherweise nicht regelmäßig von Behörden überprüft, was es sehr leicht macht, sie zu manipulieren. Insgesamt wurden an die 300 Wertpapiere in E-Mails empfohlen. Bei der Auswertung konzentrierten sich die Wissenschaftler auf jenen Tag, an dem die meisten Nachrichten eines Typs empfangen wurden. Sie fanden heraus, dass an diesem Tag die Wahrscheinlichkeit 13 Mal höher war, dass diese Aktie das am aktivsten gehandelte Pink Sheet war, als an Tagen, an denen sie nicht durch Spam promotet wurde. Die dadurch erhöhte Liquidität und das größere Volumen waren entscheidend für den Erfolg der Spammer. Bei Volumenhöchststand verkauften die Spammer ihre vor der Werbeaktion erworbenen Anteile und konnten so satte Gewinne erzielen. Die Anleger jedoch mussten Verluste hinnehmen, denn obwohl am nächsten Tag der Kurs meist noch am selben Level blieb, war laut Studie am Tag darauf die Rendite um 5,9 Prozent niedriger als jene vergleichbarer Aktien.

Es gibt eine Reihe von Antispam-Maßnahmen [BSI, 2005-1, S 67ff]. Diese reichen von technischen Möglichkeiten wie dem Signieren von E-Mails (siehe *1.7.2.1.7 Elektronische Signatur*), „DomainKeys Identified Mail" (kurz: DKIM)[251], Filterung, *White- und Blacklist-Verfahren*[252] oder heuristischen Verfahren[253] bis hin zu organisatorischen Maßnahmen wie Erarbeiten einer Antispam-Policy (siehe *1.8.2.4.2 IT-Systemsicherheitspolitik*).

Microsofts hat mit „*Sender ID*" eine Antispam-Technologie entwickelt und stellt sie den Kunden seit Oktober 2006 kostenlos und ohne rechtliche Konsequenzen zur Verfügung. Die „Sender ID"-Technologie wird zur Verifizierung von E-Mail-Adressen eingesetzt. Über einen Serverabgleich kann festgestellt werden, ob die E-Mail von dem Mailserver stammt, den sie vorgibt zu benutzen (siehe *1.4.3.6 Spoofing*).

[250] Vgl. http://papers.ssrn.com/sol3/papers.cfm?abstract-id=920553 „Spam Works: Evidence from Stock Touts and Corresponding Market Activity" 14. März 2007 [27. März 2007]

[251] http://antispam.yahoo.com/domainkeys [26. Mai 2007]

[252] Auf einer Whitelist sind im Gegensatz zur Blacklist vertrauenswürdige Personen oder Firmen gelistet. Enthält ein Spamfilter eine Whitelist, bedeutet dies, dass E-Mails von den gelisteten Personen/Firmen immer akzeptiert werden.

[253] Als Heuristik bezeichnet man Strategien („Faustregeln"), die das Finden von entsprechenden Lösungen zu Problemen ermöglichen sollen, zu denen kein mit Sicherheit zum Erfolg führender Algorithmus bekannt ist. Heuristische Verfahren kommen zum Einsatz, um Spam-E-Mails zu identifizieren, die dem Filtersystem nicht bekannt sind.

1.7 SCHUTZMAßNAHMEN UND GEGENSTRATEGIEN

Die bisherigen Ausführungen haben gezeigt, dass der Wert Information auf viele Arten und auf unterschiedlichen Ebenen bedroht und angegriffen werden kann. Wurden bislang individuelle Schutzaktivitäten erläutert, sollen im Folgenden globale Maßnahmen aufgezeigt werden. Dabei bedarf es sowohl eines technischen wie eines organisatorischen Ansatzes. Diese gelten grundsätzlich für das unternehmerische Umfeld, einzelne Elemente sind auch für den Privathaushalt anwendbar.

1.7.1 ORGANISATORISCHE GEGENMAßNAHMEN

Hier geht es im Wesentlichen um eine nicht-taxative Aufzählung relevanter organisatorischer Maßnahmen zur Erreichung, Verbesserung und nachhaltiger Etablierung eines entsprechenden Informationssicherheitsniveaus. Dazu gehören Aktivitäten im Bereich der Ablauf- und Aufbauorganisation, der Betriebsführung oder zu beachtende Grundsätze im Umgang mit Informationssicherheit am Client (PC, Notebook etc.).

1.7.1.1 Organisation/Personal

1.7.1.1.1 Informationssicherheitsorganisation/Datenschutzorganisation

Der Aufbau einer Informationssicherheitsorganisation/Datenschutzorganisation beinhaltet die Festlegung von zuständigen Akteuren und Verfahren, damit die systematische und kontinuierliche Bearbeitung der sicherheitsrelevanten Aspekte sichergestellt ist. Dabei soll eine der Unternehmensgröße angepasste organisatorische Umgebung geschaffen werden, die die Erstellung und Pflege eines Informationssicherheitskonzepts (siehe *1.8.2 Umsetzung von Informationssicherheitsmanagement*) in effizienter Weise ermöglicht.

1.7.1.1.2 Awareness-Programme und Lobbying

Eine wesentliche Säule zur Erreichung und Hebung von Datenschutz- und IT-Sicherheitsstandards ist die Einbindung der Mitarbeiter (siehe *1.8.2.5.2 Sensibilisierung und Schulung* und *1.8.3 Der Faktor Mensch*). Die Erfahrung zeigt, dass durch die Einbeziehung der Mitarbeiter in Form von Sensibilisierungsmaßnahmen der größte Effekt in Bezug auf das Kosten/Nutzen-Verhältnis erzielt werden kann. Die Maßnahmen können dabei von Informationen im Intranet und Merkblättern über Bildschirmschoner und Videos bis zu Informationsveranstaltungen und Live-Hacking-Vorführungen reichen[254]. Wichtig dabei ist das systematische und wiederkehrende Vorgehen bzw. die Involvierung des Top-Managements und des Betriebsrates von Beginn an.

[254] Vgl. http://www.schuler-ds.de/awarenessprogramme.html [14. Marz 2008]

1.7.1.1.3 Audits und Revision

Die Durchführung eines Audits kann sich sowohl auf Anwendungen als auch auf Verfahren beziehen. Die Ziele werden dabei durch bestehende Regelungen und Gesetze zum Datenschutz und der Informationssicherheit vorgegeben: Securitypolicies (siehe *1.8.2.4.2 IT-Systemsicherheitspolitik*), Datenschutzgesetz, IT-Grundschutzhandbuch oder ISO 27001 (siehe *1.8.4 Informationssicherheitsstandards und -Vorschriften*).
Als Ergebnis jeden Audits gibt es einen Bericht, der die vorgefundene Ist-Situation in Bezug auf das definierte Soll analysiert und bewertet. Dabei werden mögliche Defizite festgehalten und erläutert, wie diese beseitigt werden können.

1.7.1.2 Betriebsführung

1.7.1.2.1 Information Technology Infrastructure Library (ITIL)

ITIL ist ein de-facto-Standard für Gestaltung, Implementierung und Management elementarer Steuerungsprozesse in der IT. Der Standard beinhaltet eine umfassende und öffentlich verfügbare fachliche Dokumentation zur Planung, Erbringung und Unterstützung von IT-Serviceleistungen[255], die auf praktischen Erfahrungen beruhen. ITIL beschreibt, *was* zu tun ist. *Wie* diese Aufgaben in den einzelnen Unternehmen umzusetzen sind, hängt von den Rahmenbedingungen in den Betrieben ab. Das gewährleistet, dass ITIL unabhängig von Branche und Unternehmensgröße realisierbar ist.
Das Ziel von ITIL besteht im Wesentlichen darin, technologiezentrierte IT-Organisationen prozess-, service- und kundenorientiert auszurichten, wobei die Vorgehensweise unabhängig von Technik, Technologie oder Anbietern ist. [BSI, 2005-2]
Strukturiert wird ITIL durch taktisch-strategische (*Service Delivery*) und operationale Elemente (*Service Support*). Die Gestaltung, Planung, Vereinbarung, Überwachung, das Berichtswesen und die Optimierung der IT-Services erfolgt im Rahmen des Service Delivery durch fünf Prozesse: Service Level-Management, Finanzmanagement für IT-Services (engl. *Financial-Management for IT-Services*), Verfügbarkeitsmanagement (engl. *Availability-Management*), Kapazitätsmanagement (engl. *Capacity-Management*) und Kontinuitätsmanagement (engl. *IT-Service Continuity-Management*).
Fünf operative Prozesse steuern im Service Support die Servicequalität in den Leistungserstellungsprozessen: Störungsmanagement (engl. *Incident-Management* mit der Funktion *Service Desk*), Problemmanagement (engl. *Problem-Management*), Änderungsmanagement (engl. *Change-Management*), Versionsmanagement (engl. *Release-Management*) und Konfigurationsmanagement (engl. *Configuration-Management*).

[255] Vgl. http://www.itil.org/de/ [11. März 2008]

Unter dem Projektnamen „ITIL Refresh“ wird die aktuell publizierte best practices-Sammlung in Version 3[256] übergeführt, wobei zeitgemäße Themen *Sourcing, Shared Service-Models, Service Management, Wissensdatenbank* oder *Request-Management* eingearbeitet werden. Der Umstieg erfolgt in sogenannten Tranchen und soll mit Sommer 2007[257] abgeschlossen sein. Die Ausrichtung von ITIL erfolgt noch stärker nach den Geschäftsanforderungen, der Fokus liegt auf dem *Service Life Cycle*. ITIL ist damit Grundlage zur Erfüllung der Compliance-Anforderungen (SOX, Basel II etc.) und stellt die lernende Organisation nach dem *Deming Quality Cycle*[258] in den Mittelpunkt. ITIL-V3 ist mit dem Standard ISO/IEC 20000[259] abgestimmt.

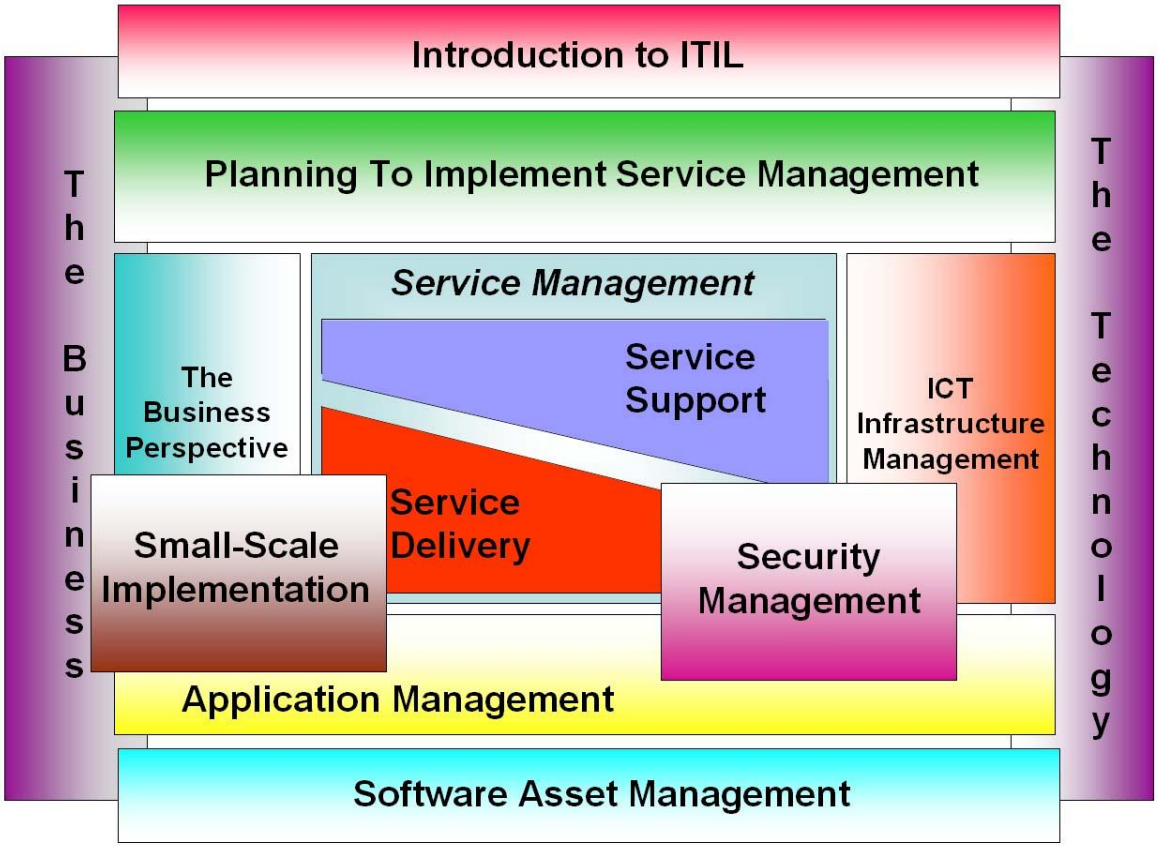


Abbildung 19: CA „*Leveraging ITIL*“

Um ein holistisches Vorgehen zu erreichen, gibt es neben dem Servicemanagement unter anderem das *ICT Infrastructure-Management* und das *Security-Management*. Damit kann die

[256] Vgl. http://www.itil.org/de/itilv3-servicelifecycle/index.php [16. März 2008]
[257] Vgl. http://www.itsmf.de/news/news.asp?NewsID=56 [16. März 2008]
[258] Vgl. http://www.balancedscorecard.org/bkgd/pdca.html [16. März 2008]
[259] Vgl. http://www.itil.org/de/isoiec20000/index.php [16. März 2008]

Informationssicherheit stärker in die IT-Prozesse eingebunden werden. Informationssicherheit wird in ITIL im Kontinuitätsmanagement auf Basis der britischen Norm *BS 7799*[260] abgehandelt.
ITIL wird hier beispielhaft als Orientierungshilfe zur Steuerung einer IT dargestellt. Es gibt auch andere Ansätze[261], die sich größtenteils komplementär zueinander verhalten: *HP-ITSM*[262], CObiT (siehe *1.8.4.2.1 CobiT*) oder *Microsoft Operations Framework* (MOF)[263].

1.7.1.2.2 Patchmanagement

Der Trend hin von Individualsoftware zum Massenprodukt bringt mit sich, dass deutlich mehr Schwachstellen eines Codes entdeckt und geschlossen werden können. Ist eine Schwachstelle ausfindig gemacht worden, kann sie sehr schnell missbräuchlich ausgenutzt werden (siehe *1.3.4.1.2 Verbreitungsmöglichkeiten Zero-Day-Exploits*).
Patchmanagement ist demnach eine der wichtigsten Aufgaben von Systemadministratoren. Updates bedeuten oftmals, dass das System neu gestartet werden muss. Aus diesem Grund ist Patchmanagement in erster Linie eine organisatorische Herausforderung. In Abstimmung mit den Kunden muss ein sogenanntes „Wartungsfenster" definiert werden, damit die Systemunterbrechung nicht zu sehr den Geschäftsfortgang stört. Die große Herausforderung besteht vor allem darin, dass die geplanten Patches vorher im Kontext der bestehenden Systeme getestet werden. Dafür muss für kritische Systeme eine Testumgebung geschaffen werden, wo minutiös die Konstellation auf den Echtsystemen nachgebildet wird.
Der immer kleiner werdenden Wartungszeit kann mit Patchmanagement-Werkzeugen entgegnet werden. Damit können unternehmensweit konzertiert Software-Updates eingespielt werden, um Sicherheitslücken zu schließen und Software auf Letztstand zu halten. Die Tools bieten den Vorteil, Patches schnell auf eine Vielzahl von Systemkomponenten aufzubringen. Das *CERT*[264] stellt in einer Untersuchung fest, dass sich durch konsequentes Patchmanagement 95 Prozent aller potentiellen Angriffsflächen eines Systems beseitigen lassen. Für den Einsatz von Patchmanagement-Werkzeugen sprechen zudem Zeit- und Kostenersparnisse.

1.7.1.2.3 IT-Versicherungen

Die Informationstechnik stellt eine Vielzahl an technischen Schutzmaßnahmen für Probleme der Informationssicherheit bereit. Diese können ihre Wirkung allerdings nur dann entfalten, wenn sie effektiv eingesetzt werden. Deshalb liegt es nahe, Informationssicherheit nicht nur mit technischen und organisatorischen Hilfsmitteln anzustreben, sondern auch die ökonomischen Aspekte zu

[260] http://www.bsi-global.com/ [16. März 2008]
[261] Vgl. http://www.itsmi.de/content/itil_portal/0index/view [16. März 2008]
[262] Vgl. http://h20219.www2.hp.com/services/cache/10309-0-0-225-121.html [11. März 2007]
[263] Vgl. http://www.itsmi.de/content/itil_portal/0index/4mof/0index/view [16. März 2008]
[264] http://www.cert.org/ Computer Emergency Response Team [16. März 2008]

berücksichtigen [Böhme, 2005] (siehe *1.8.5 Kommerzieller Aspekt*). Versicherungen können ein geeignetes Mittel zum Umgang mit IT-Risiken sein.

Es wird zwischen zwei Risikotypen unterschieden: Zum einen gibt es *Eigenschäden* beim Versicherungsnehmer selbst. Diese umfassen beispielsweise Gewinnausfall durch Datendiebstahl, Zerstörung von Daten sowie Betriebsunterbrechungen durch Hacker-Angriffe, Computerviren, Software- und Programmierfehler. *Drittschäden* sind hingegen Kosten, die Dritten durch Fehler des Versicherungsnehmers entstehen. Hier können zum Beispiel Schäden durch weitergeleitete Viren oder Datenschutzverletzungen nach Spionagefällen angeführt werden.

Versichert [Piller, 2005-1, Teil 1, S 161] werden können Schäden und Ausfälle in Einzel- oder pauschalierter Vertragsform in den Bereichen Elektronik, Mehrkosten (zusätzliche Betriebsweiterführungskosten aufgrund eines Schadensfalls), Betriebsunterbrechung, Computer-Missbrauch oder Informationsverlustes.

Der Internetserviceprovider *AOL*[265] beschreitet neue Wege und bietet seinen Kunden seit Winter 2006 eine kostenlose Diebstahlversicherung an[266]. Bei Datendiebstählen von Versicherungsnummern, Bankdaten und ähnlichen Informationen werden insgesamt bis zu 10.000 Dollar Schadenersatz ausbezahlt. Die Reparatur beschädigter Computer wird zusätzlich mit Zahlungen bis zu 1.000 Dollar gedeckt, der Betrag wird jedoch am aktuellen Wert des jeweiligen Computers gemessen und kann sich demnach deutlich verringern. Durch Datendiebstahl entstandene Kosten und Behördenwege werden ebenfalls mit bis zu 1.000 Dollar von der Versicherung gedeckt.

1.7.1.3 Grundsätze im Umgang mit PCs zum Schutz vor Malicious Code

Viele Benutzer – das trifft vor allem auf die privaten zu – sind der Meinung, ihr PC sei zu wenig „interessant“, um Sicherheitsangriffen ausgesetzt zu werden. Angreifer missbrauchen PCs aus dem einfachen Grund, weil sie sich eben missbrauchen lassen. Ein PC ist also schon alleine deshalb interessant genug, weil er Sicherheitsprobleme aufweist. Werden die wesentlichen, meist einfach durchzuführenden Grundsätze[267] im Umgang mit Sicherheit beachtet, ist es für den Angreifer viel schwieriger bzw. unmöglich, des PCs habhaft zu werden (siehe *1.3.4.1.1 Exkurs: Botnet*, *1.7.2.7 Sicherheitsmaßnahmen von Microsoft*).

- Ausschalten des Rechners bzw. Trennen der Internetverbindung bei Nichtbenutzung,
- Verwendung von geeigneten, zyklisch wechselnden Passwörtern; Sensibilität im Umgang mit Zugangscodes,
- Einsatz von aktuell gehaltenen Schutzprogrammen (Antivirus, Firewall etc.) mit automatisierten Systemscans,

[265] http://www.aol.com/ [16. März 2008]
[266] Vgl. http://preventingidentitythefttips.com/trans/ge-preventing-identity-theft.php [27. März 2007]
[267] Vgl. http://www2.uibk.ac.at/zid/security/pc-basics.html [16. März 2008]

- Reduzierung der administrativen Benutzerrechte,
- Durchführung von (Betriebs-)Systemupdates,
- Datensicherung,
- nach Möglichkeit Verwendung verschiedener Browser mit aktivierten Sicherheitsfeatures,
- Vorsicht beim Öffnen unbekannter Dateien, sorgsamer Umgang bei Filesharing,
- Deaktivierung von nicht benötigten Services und Ports (USB etc.).

1.7.2 TECHNISCHE GEGENMAßNAHMEN

Technisch gibt es eine Vielzahl an Möglichkeiten, Information und Infrastruktur zu schützen. Im Folgenden soll auf einige davon näher eingegangen werden, vor allem auf jene, die für die digitale Identität Relevanz haben.

1.7.2.1 Kryptologie

Die Kryptologie beschäftigt sich mit Verschlüsselungsverfahren und ist der Überbegriff für Kryptographie und Kryptoanalyse. Während es bei der Kryptographie um die Wissenschaft der Verschlüsselung von Informationen geht, steht die Kryptoanalyse für Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen.
Mit steganographischen Methoden hingegen wird nicht die Information verschleiert, sondern die Existenz der Nachricht verborgen. Ein Forscherteam der *University of Princeton*[268] hat im Herbst 2006 eine neue Methode vorgestellt[269], mit der Daten über öffentliche Glasfaserleitungen übertragen und dabei versteckt werden können, sodass es nahezu unmöglich ist, diese abzufangen und zu entschlüsseln. Das entwickelte Verfahren basiert nicht auf Software-Verschlüsselung, die Chiffrierung wird bei der Einspeisung in das Netz mit einer Hardware erreicht. Die Daten werden unter den viel stärkeren Signalen des normalen Datenverkehrs sicher verborgen und sind somit schwer zu entdecken.

1.7.2.1.1 Verschlüsselungsverfahren

Verschlüsselungsverfahren lassen sich in die *symmetrische*, *asymmetrische* und *hybride* Methode unterteilen[270].
Bei *symmetrischen Verschlüsselungsverfahren* wird nur ein Schlüssel zur Ver- und Entschlüsselung verwendet. Der Schlüssel muss daher sowohl der ver- als auch der entschlüsselnden Seite bekannt

[268] http://www.osa.org/ [15. Jänner 2007]
[269] Vgl. http://www.innovations-report.de/html/berichte/informationstechnologie/bericht-71913.html [27. März 2007]
[270] Vgl. http://www.tcp-ip-info.de/security/verschluesselung.htm [16. März 2008];
http://www.datenschutzzentrum.de/selbstdatenschutz/internet/verschluesseln.htm [16. März 2008];
http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm [17. März 2008];
http://www.elektronik-kompendium.de/sites/net/0908071.htm [16. März 2008]

sein. Die Übergabe des Schlüssels an den Empfänger sollte sicher erfolgen, beispielsweise durch persönliche Weitergabe. Im Umgang mit dem Schlüssel ist höchste Sorgfalt angebracht.

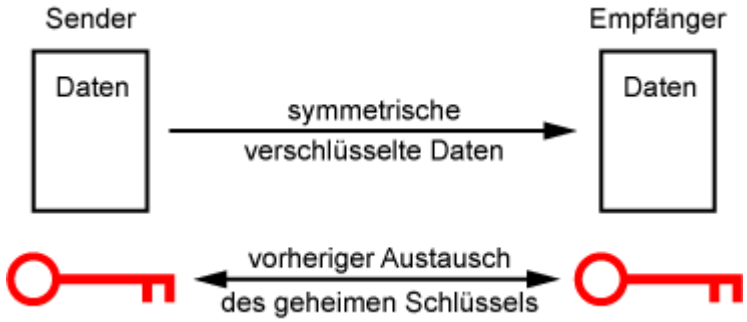


Abbildung 20: Schematische Darstellung symmetrisches Verfahren

Symmetrische Verschlüsselungsverfahren bieten bei entsprechender Schlüssellänge ein hohes Maß an Sicherheit, dennoch ist die Durchsatzgeschwindigkeit hoch. Ein Anwendungsgebiet dieses Verfahrens ist das *Pay-TV*. Das Fernsehsignal wird vom Anbieter verschlüsselt gesendet, die TV-Konsumenten können mit dem passenden Schlüssel dieses Fernsehsignals entschlüsseln. Die Problematik des „Schwarzsehens" beim Pay-TV zeigt gleichzeitig den Schwachpunkt von symmetrischen Verfahren. Jeder, der in den Besitz des Schlüssels kommt, kann die damit verschlüsselten Daten entschlüsseln.
Die bekanntesten symmetrischen Verschlüsselungsalgorithmen sind: *DES*[271], *3DES*[272], *RC*[273] in verschiedenen Versionen, *Blowfish*[274], *AES*[275].
Nachteile dieses Verfahrens sind die Geheimhaltung des Schlüssels, die sichere Übermittlung an den Kommunikationspartner und die Anzahl der Schlüssel, da für jeden Partner ein eigener Schlüssel existiert.
Bei *asymmetrischen Verschlüsselungsverfahren* hingegen wird mit zwei Schlüsseln gearbeitet. Der öffentliche Schlüssel (engl. *Public Key*) und der private Schlüssel (engl. *Private Key*) sind so miteinander verknüpft, dass mit einem Public Key verschlüsselte Daten nur mit dem dazu gehörigen Private Key entschlüsselt werden können.

[271] http://www.itwissen.info/definition/lexikon//_desdes_desdata%20encryption%20standard%20des_desdes-verschl%fcsselung.html [16. März 2008]; Digital Encryption Standard (kurz: DES)
[272] http://www.itwissen.info/definition/lexikon//_3des3des_3destriple%20des%203des_3desdreifach-des.html [16. März 2008]; Triple Digital Encryption Standard (kurz: 3DES)
[273] http://www.itwissen.info/definition/lexikon//_rc4rc4_rc4rivest%20cipherrc4_rc4rc4-algorithmus.html [16. März 2008]; Rivest Cipher (kurz: RC)
[274] http://www.itwissen.info/definition/lexikon//blowfish_blowfish.html [16. März 2008]
[275] http://www.itwissen.info/definition/lexikon//_aesaes_aesadvanced%20encryption%20standard%20aes_aesaes-verschl%fcsselung.html [16. März 2008]; Advanced Encryption Standard (kurz: AES)

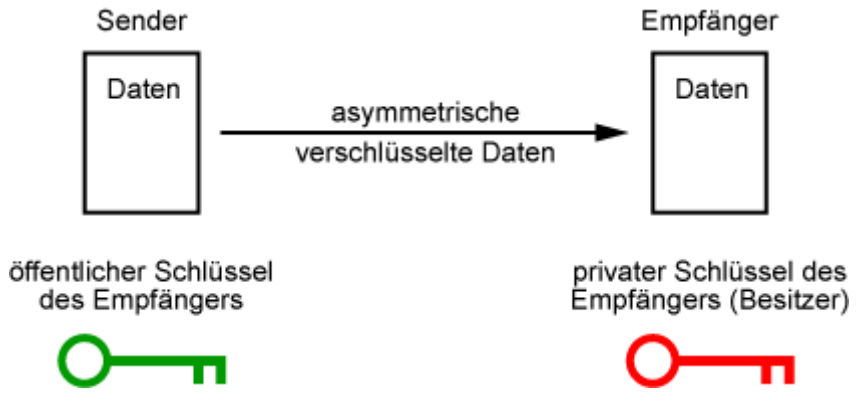


Abbildung 21: Schematische Darstellung asymmetrisches Verfahren

Um Daten sicher zu transportieren, benötigt der Absender den Public Key des Empfängers, damit er die Nachricht verschlüsseln kann. Der Empfänger entschlüsselt mit dem nur in seinem Besitz befindlichen Private Key. Das Schlüsselpaar hat eine gemeinsame mathematische Basis (beispielsweise eine Primzahl mit hunderten Dezimalstellen), das Herleiten eines Schlüssels aus dem anderen ist bei geeigneter Schlüssellänge praktisch nicht möglich.

Bekannte asymmetrische Verschlüsselungsalgorithmen sind: *Diffie-Hellman*[276] und *RSA*[277]. Anwendung finden asymmetrische Kryptosysteme zur Sicherstellung der Vertraulichkeit und Authentizität im E-Mail-Verkehr (*S/MIME*[278]) ebenso wie in kryptografischen Protokollen wie *SSH*[279], SSL/TLS (siehe *1.3.4.2.5 SSL/TLS-Sicherheit*) oder HTTPS (siehe *1.3.4.2.3 HTTP-Sicherheit*).

Gegenüber symmetrischen Verfahren haben asymmetrische den Nachteil, dass sie langsamer sind (RSA ist rund 1000 Mal langsamer als DES)[280] und aufgrund der mathematischen Abhängigkeiten der beiden Schlüssel auch höhere Schlüssellängen benötigt werden.

Die Vorteile der symmetrischen und asymmetrischen Methode werden in *hybriden Verschlüsselungsverfahren* vereint. Zunächst wird ein sogenannter *Session-Key* nach dem Zufallsprinzip generiert, dieser dann mit dem Public Key des Empfängers verschlüsselt. Die eigentlichen Daten werden aus Performancegründen nach einem symmetrischen Verfahren verschlüsselt. Die verschlüsselten Daten werden zusammen mit dem verschlüsselten Session-Key an den Empfänger geschickt. Dieser kann mit seinem Private Key den Session-Key extrahieren und damit die Nachricht entschlüsseln.

---

[276] http://www.itwissen.info/definition/lexikon//_dhadha_dhadiffie%20hellman%20algorithm%20dha_dhadiffie-hellman-algorithmus.html [16. März 2008]

[277] http://www.itwissen.info/definition/lexikon//_rsarsa_rsarivest-shamir-adleman%20rsa_rsarsa-verfahren.html [16. März 2008]; Rivest-Shamir-Adleman (kurz: RSA)

[278]http://www.itwissen.info/definition/lexikon//_s--slash--mimes--slash--mime_s--slash--mimesecure%20mimes--slash--mime_s--slash--mimes--slash--mime-algorithmus.html [16. Dezember 2008]; Secure/Multipurpose Internet Mail Extensions (kurz: S/MIME)

[279] http://www.itwissen.info/definition/lexikon//_sshssh_sshsecure%20shellssh_sshssh-protokoll.html [16. März 2008]; Secure Shell (kurz: SSH)

[280] Vgl. http://www.tcp-ip-info.de/security/verschluesselung.htm [16. März 2008]

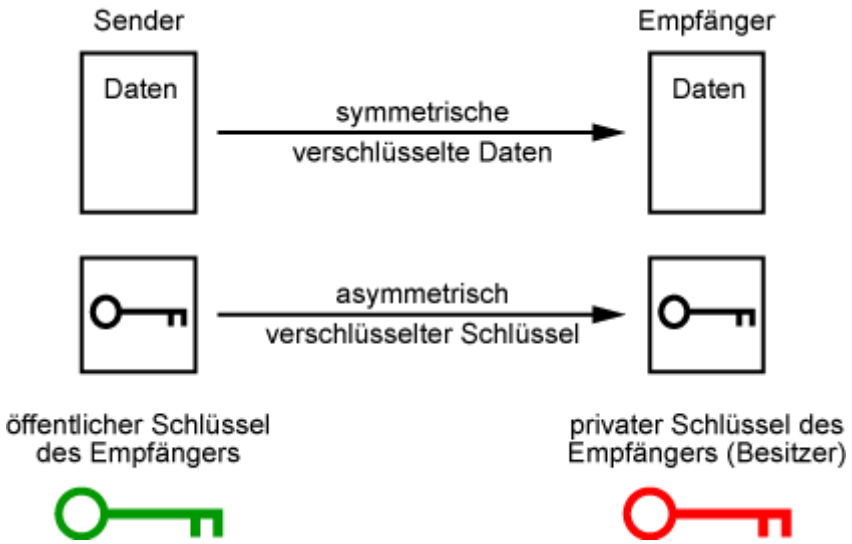


Abbildung 22: Schematische Darstellung eines hybriden Verfahrens

Grundsätzlich gilt bei allen Verschlüsselungsformen immer die Grundregel: Je länger der Schlüssel, desto höher die Sicherheit. Ein langer Schlüssel verhindert das Entschlüsseln durch Ausprobieren (Brute-Force-Attacken, siehe *1.4.3.4 Passwort-Attacken*). Der bei jedem Vorgang neu erzeugte Zufallsschlüssel muss so generiert werden, dass keine Systematik erkennbar ist. Hybride Verschlüsselung kommt sehr häufig zur Anwendung, eines der bekanntesten Verfahren ist PGP (Pretty Good Privacy).

1.7.2.1.2 Quantenkryptographie

Unter Quantenkryptographie[281] werden Verfahren verstanden, die es ermöglichen, an zwei voneinander getrennten Orten eine identische Bitfolge zu erzeugen, welche in der Folge zur Verschlüsselung von Nachrichten herangezogen werden kann. Aufgrund von quantenphysikalischen Naturgesetzen (miteinander verschränkte Photonen verhalten sich auch über große Entfernungen hinweg gleich) ist das unbemerkte Abhören des Schlüssels nicht möglich. In der Forschung – dabei ist ein österreichisches Team der *Universität Wien*[282] federführend – werden Einsatzmöglichkeiten von Quantenkryptographie erarbeitet. Für den praktischen Einsatz der Quantenkryptographie muss allerdings noch in vielen Bereichen (Elektronik, Kryptographie, Software) Entwicklungsarbeit geleistet werden. Eine weitere Herausforderung besteht darin, diese Verschlüsselungstechnik in bestehende IT-Infrastruktur-Lösungen zu integrieren.

Damit die Theorie in der Praxis überprüft werden kann, wurde im Rahmen des europäischen Forschungsprojekts „*SECOQC*"[283] im Frühjahr 2007 ein Demonstrationsnetz für Quantenkryptografie

[281] Vgl. http://www.quantenkryptographie.at/ [15. Jänner 2008]
[282] http://www.quantum.at/ [15. Jänner 2007]
[283] Vgl. http://www.secoqc.net/ [27. März 2007]

mit fünf Knotenpunkten zwischen Wien und St. Pölten errichtet. Die Knoten sind über ein herkömmliches Glasfaserkabel miteinander verbunden, in jedem Knotenpunkt befinden sich Module zur Schlüsselerzeugung sowie weitere Module zur Verschlüsselung, Entschlüsselung und Weiterreichung von Schlüsseln.

1.7.2.1.3 Verschlüsselungschip am Client

IBM[284] hat einen Chip namens „*Secure Blue*" entwickelt, der für die Verschlüsselung der Daten auf (mobilen) Clients (PC, PDA, Handy) sorgt. Die Intention ist, das Sicherheitsniveau von Serversystemen auf die Geräte der Endbenutzer zu bringen. Der Verschlüsselungsmechanismus wird auf Halbleitern des Prozessors aufgebracht und soll dadurch für einen lückenlosen (bei gängigen Systemen ist der Weg vom Chip zum Prozessor in der Regel nicht verschlüsselt) Schutz der Daten sorgen. Die integrierte Verschlüsselung ist auch zum Schutz von urheberrechtlichem schützenswerten Material einsetzbar (siehe *2.3.3.5 Digital Rights Management*).
Intel[285] verfolgt mit „*Trusted Platform Module*" [Intel, 2002] einen ähnlichen Ansatz (siehe *1.7.2.8 Trusted Computing*).

1.7.2.1.4 Hash-Verfahren

Die *Hash*-Funktion[286] ermöglicht es, aus einer beliebig langen Quellinformation einen kurzen, eindeutigen Hash-Wert („*Fingerprint*") zu erzeugen. Der Absender erzeugt aus einer zu verschlüsselnden Information den Hash-Wert und sendet sowohl die Information als auch den generierten Hash-Wert an den Empfänger. Dieser berechnet aus der gelieferten Information nach dem gleichen Verfahren den Hash-Wert und vergleicht beide Werte miteinander. Die Übereinstimmung der Werte impliziert, dass die Information unverändert geblieben ist.
Hash-Verfahren sollen zum einen schnell, zum anderen sicher (Anm.: Integrität) sein. Der Hash-Wert sollte so eindeutig sein, dass es praktisch nicht möglich ist, eine Information derart zu ändern, sodass der Hash-Wert der manipulierten Information genau dem der Originalinformation entspricht („Kollisionsfreiheit"[287]).
Neben der Kryptologie finden Hash-Verfahren bei der Speicherung von Passwörtern Anwendung. Es wird nicht das Passwort selbst, sondern lediglich der Hash-Wert dessen auf dem System gespeichert. Da aus dem Hash-Wert die Originalinformation („Unumkehrbarkeit"[288]) nicht eruiert werden kann, ist

[284] Vgl. http://www.ibm.com/news/ch/de/2006/04/11.html [15. Jänner 2007]
[285] http://www.intel.com/ [15. Jänner 2007]
[286] Vgl. http://hash_funktion.know-library.net/ [3. Jänner 2007];
http://www.tfh-berlin.de/~oo-plug/A&D/Hash.html [3. Jänner 2008];
http://www.staff.uni-mainz.de/pommeren/DSVorlesung/KryptoBasis/Hash.html [3. Jänner 2007]
[287] Vgl. http://www.s-trust.de/lexikon/k/kollisionsfreiheit.htm [3. Jänner 2007];
http://ig.cs.tu-berlin.de/oldstatic/ap/rg/002/glossar/glossar/k-terms/kollisionsfreiheit.html [3. Jänner 2007]
[288] Vgl. http://hash_funktion.know-library.net/ [3. Jänner 2007]

die Speicherung des Hash-Wertes sicher. Bei der Authentifizierung (siehe *2.2.6 Autorisierung, Authentifizierung*) wird das Passwort vom Benutzer eingegeben, daraus wird ein Hash-Wert erzeugt und mit dem hinterlegten Hash-Wert verglichen.
Weiters kann der Hash-Wert zum Auffinden von Daten in Datenbanken und zum digitalen Signieren eines Dokumentes (siehe *1.7.2.1.6 Digitale Zertifikate*) verwendet werden.
Bekannte Hash-Verfahren sind: *MD2, MD4, MD5*[289], *SHA*[290] oder *RIPEMD*[291].

1.7.2.1.5 Public Key Infrastructure

Unter *Public Key Infrastructure*[292] (kurz: *PKI*) werden die Rahmenbedingungen und die Infrastruktur verstanden, mit der es möglich ist, eine gegenseitige Authentisierung, eine vertrauliche Kommunikation und rechtsverbindliche digitale Unterzeichnung von Dokumenten für offene, unsichere Netze (Internet) sicherzustellen. Damit werden durch PKI mit Authentizität, Vertraulichkeit, Integrität und Verbindlichkeit (siehe *1.2.2 Anforderungen an die Informationssicherheit*) vier wesentliche Anforderungen an die Sicherheit erfüllt.
Mittels asymmetrischer Verschlüsselung werden die Daten digital signiert und verschlüsselt. Die Sicherstellung, dass der dazu nötige Public Key auch tatsächlich dem Absender gehört, wird durch digitale Zertifikate (siehe *1.7.2.1.6 Digitale Zertifikate*) erreicht. Das digitale Zertifikat wird durch eine digitale Signatur (siehe *1.7.2.1.7 Elektronische Signatur*) geschützt, deren Echtheit wieder mit dem öffentlichen Schlüssel des Zertifikatausstellers geprüft werden kann.

Wesentliche Bestandteile einer PKI sind:

- Hard- und Software.
- Digitale Zertifikate: Digital signierte Daten, die dem Nachweis der Echtheit von Objekten dienen.
- Registrierungsstelle (engl. *Registration Authority*, kurz: *RA*): Diese Organisation prüft die Richtigkeit der Daten für das gewünschte Zertifikat und genehmigt den Antrag der durch die Zertifizierungsstelle signiert wird.
- Zertifizierungsstelle (engl. *Certificate Authority*, kurz: *CA*): Organisation zur Bereitstellung des Zertifikats.

---

[289] http://www.tech-faq.com/message-digest.shtml [3. Jänner 2007];
http://www.irnis.net/gloss/message-digest.shtml [3. Jänner 2007]; Message Digest (kurz: MD)
[290] http://www.itl.nist.gov/fipspubs/fip180-1.htm [3. Jänner 2007]; Secure Hash Algorithm (kurz SHA); Laut c't 7/2007 Seite 204 ist SHA-1 geknackt worden;
[291]
http://www.itwissen.info/definition/lexikon//_ripemdripemd_ripemdrace%20integrity%20primitives%20evaluation%20message%20digestripemd_ripemd.html [3. Jänner 2008]; RACE Integrity Primitives Evaluation Message Digest (kurz: RIPEMD)
[292] Vgl. http://www.cio.gv.at/it-infrastructure/pki/ [3. Jänner 2007];
http://www.pki-page.org/ [3. Jänner 2007];
http://www.tecchannel.de/sicherheit/grundlagen/402051/ [9. Jänner 2007]

- Zertifikatsperrliste (engl. *Certificate Revocation List*, kurz: *CRL*): Liste von Zertifikaten, die vor Ablauf der Gültigkeit zurückgezogen wurden.
- Verzeichnisdienste (siehe *3.4.1 Verzeichnistechnologien*): Verzeichnis, das die ausgestellten Zertifikate enthält (*LDAP*[293]- bzw. *X.500*[294]-Server).
- Dokumentation: Beschreibung der Arbeitsprinzipien, des Registrierungsprozesses, des Management der Keys und des technischen Schutzes der PKI-Infrastruktur.

Während sich der Aufbau einer eigenen PKI-Umgebung (RA, CA) für größere Unternehmen lohnen kann, können kleinere Organisationen ihre Zertifikate von PKI-Dienstleistern beziehen. Zentrales Element dabei ist eine Software zum Betrieb der Zertifizierungsstelle. Am Markt gibt es einige Produkte: etwa Microsoft mit in *Windows Server 2003* integriertem CA für *Active Directory*[295], *Novell* mit dem *Certificate Server* mit Integration in das *eDirectory*[296], *Entrust Authority*[297] oder *OpenCA*[298] für Open Source *Linux*.

1.7.2.1.6 Digitale Zertifikate

Ein Zertifikat[299] ist ein „elektronischer Ausweis“[300], der die Zugehörigkeit eines öffentlichen Schlüssels zu einer Identität (Person, private oder öffentliche Organisation) bestätigt. Die Definition nach *Public Key Cryptography*-Standards (kurz: *PKCS*)[301] legt das Inhaltsformat fest, der Standard *X.509v3*[302] beschreibt das Datenformat. *PKCS#7*[303] wird für den Austausch der öffentlichen Schlüssel genutzt, *PKCS#12*[304] enthält zusätzlich den kennwortgeschützten privaten Schlüssel.
Digitale Zertifikate werden durch verschiedene Zertifizierungsinstanzen (sie sollten im Idealfall so vertrauenswürdig wie z. B. eine Behörde sein) in verschiedenen Qualitätsstufen ausgestellt, die sich in der Zuverlässigkeit der im Zertifikat enthaltenen Informationen ausdrückt. Die Zuverlässigkeit hängt von der Art der Identifizierung der Schlüsseleigentümer und dem Verfahren zur Sperrung der

[293] Vgl. http://www.ietf.org/rfc/rfc2251.txt [3. Jänner 2008]; Lightweight Directory Access Protocol (kurz: LDAP) ist ein Protokoll für die Kommunikation zwischen dem sogenannten LDAP-Client und dem Verzeichnis (Directory Server). Ein solcher Verzeichnisdienst enthält objektbezogene Daten (z.B. Personendaten, Systemkonfigurationen etc.).
[294] X.500 beschreibt den Aufbau eines Verzeichnisdienstes, LDAP basiert auf X.500, entspricht aber nicht allen Anforderungen.
[295] http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx [4. Jänner 2007]
[296] http://www.novell.com/products/certserver/ [4. Jänner 2007]
[297] http://www.entrust.com/pki/ [4. Jänner 2007]
[298] http://pki.openca.org/ [4. Jänner 2007]
[299] Vgl. http://www.tecchannel.de/sicherheit/grundlagen/402051/index3.html [9. Jänner 2007]
[300] Vgl. http://www.cryptoshop.com/index.php [9. Jänner 2007]
[301] Vgl. http://www.ietf.org/rfc/rfc3447.txt [4. Jänner 2007]; http://www.rsasecurity.com/rsalabs/node.asp?id=2124 [4. Jänner 2007]
[302] Vgl. http://tools.ietf.org/html/rfc3280 [17. Jänner 2008]
[303] Vgl. http://www.ietf.org/rfc/rfc2315.txt [7. Jänner 2007]; http://www.rsasecurity.com/rsalabs/node.asp?id=2129 [7. Jänner 2007]
[304] Vgl. http://www.rsasecurity.com/rsalabs/node.asp?id=2138 [7. Jänner 2007]

Zertifikate ab. Während einige Zertifizierungsstellen die Antragsteller nur persönlich gegen Vorlage eines amtlichen Ausweises identifizieren, gibt es bei anderen keine Prüfung der Angaben des Antragstellers.

Jedes digitale Zertifikat wird von der ausgebenden Stelle beglaubigt, die ihrerseits wieder von einer höheren Stelle beglaubigt sein kann. Das so entstehende hierarchische Vertrauenssystem bildet eine PKI (siehe *1.7.2.1.5 Public Key Infrastructure*), die gemeinsame Wurzel ist ein sogenanntes *Root Certificate*[305].

Ein zur Zertifizierungshierarchie konträres Vertrauensmodell wird durch das *Web of Trust*[306] repräsentiert. Jedes Mitglied im Web of Trust kann ein Zertifikat erzeugen.

Zertifikate enthalten in der Regel [BSI, 2006-1]

- den Namen (auch eindeutiges Pseudonym) des Zertifikatausstellers und des Schlüssel-Eigentümers,
- den öffentlichen Schlüssel,
- die Informationen zu den Algorithmen,
- die laufende Nummer und die Gültigkeitsdauer des Zertifikats,
- die Angabe des zulässiges Anwendungs- und Geltungsbereich des öffentlichen Schlüssels,
- die digitale Signatur des Ausstellers über alle anderen Informationen.

Unterschieden wird zwischen Server-Zertifikaten und Client-Zertifikaten.

Es obliegt dem Benutzer, ob er dem Zertifikat des Herausgebers traut. Beim Besuch einer Website bzw. Datenaustausch über das Internet überträgt der Server seinen öffentlichen Schlüssel an den Client. Auf der Clientseite prüft der Webbrowser anhand seiner Zertifikatsliste (standardmäßig bzw. manuell installiert), ob der empfangene öffentliche Schlüssel vertrauenswürdig ist. Ist das Zertifikat am Client vorhanden, wird eine verschlüsselte Verbindung aufgebaut bzw. der Benutzer in einer Interaktion gefragt, ob er das Zertifikat überprüfen und akzeptieren will. Die Verschlüsselung arbeitet nach dem SSL-Protokoll (siehe *1.3.4.2.5 SSL/TLS-Sicherheit*), welches im Browser durch eine https-Verbindung angezeigt wird. Die vom Client gesendeten Daten kann nur jener Server entschlüsseln, der den öffentlichen Schlüssel ausgegeben hat.

Namhafte Zertifikate-Anbieter sind *VeriSign*[307] oder *Thawte*[308]. In Österreich bietet etwa die Firma *A-Trust* [309] Zertifikate an.

[305] Beispielhaft: http://www.cacert.org/index.php?id=3 [9. Jänner 2008]
[306] Vgl. http://www.w3.org/Consortium/Points/ [12. März 2007]
[307] http://www.verisign.com/ [9. Jänner 2007]
[308] http://www.thawte.com/ [9. Jänner 2007]
[309] http://www.a-trust.at/ [9. Jänner 2007]

Verwendung finden digitale Zertifikate bei der digitalen Signatur, als Sicherheitsfeatures in Netzwerkprotokollen (z. B.: SSL, IPSec) oder zum Schutz von E-Mails mit S/MIME oder PGP (siehe *1.7.2.1.8 Exkurs: E-Mail-Sicherheit*).

1.7.2.1.7 Elektronische Signatur

Die elektronische Signatur[310] bietet die Möglichkeit, elektronische Daten mit einer elektronischen Unterschrift zu versehen. Im *§2 Signaturgesetz*[311] (kurz: *SigG*) *Ziffer 1* werden unter elektronischer Signatur *elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen,* verstanden. Damit kann sichergestellt werden, dass die Informationen tatsächlich vom Signator stammen und dass sie während der Übermittlung nicht verändert wurden. Weiters können Signaturen zur Identifikation – zum Beispiel beim Online-Banking (siehe *1.4.1.2 Exkurs: Phishing*) – verwendet werden. Der Empfänger hat die Möglichkeit, die elektronisch signierten Daten zu überprüfen, womit das Vertrauen in die elektronische Kommunikation wesentlich gesteigert wird.
Zur Umsetzung der elektronischen Unterschrift bedarf es geeigneter, kryptographischer Verfahren und Maßnahmen (siehe *1.7.2.1.1 Verschlüsselungsverfahren, 1.7.2.1.4 Hash-Verfahren, 1.7.2.1.5 Public Key Infrastructur*). Bei der elektronischen Signatur handelt es sich um ein asymmetrisches Verfahren, bei dem aus dem zu unterschreibenden Text ein Hash berechnet wird. Dieser Fingerprint wird mit dem Private Key verschlüsselt und an die eigentliche, weiterhin unverschlüsselte Nachricht angehängt. Der Empfänger entschlüsselt den Hash mit dem öffentlichen Schlüssel des Absenders und kann so die Authentizität des Absenders und die Integrität der Nachricht feststellen.

Digitale Signatur versus Elektronische Signatur[312]
Oftmals werden die Begriffe „Digitale Signatur“ und „Elektronische Signatur“ fälschlicherweise synonym verwendet. Während es bei der Digitalen Signatur – wie schon ausgeführt – um ein kryptographisches Verfahren handelt, geht es bei der Elektronischen Signatur um eine rein rechtliche Angelegenheit.
Um eine rechtlich gültige Kommunikation über E-Mail zu ermöglichen, Verträge über das Internet abschließen oder Amtswege online abwickeln zu können, bedarf es juristischer Voraussetzungen und Rahmenbedingungen. Diese sind die Grundlage dafür, dass eine elektronische Willenserklärung rechtliche Wirkung entfaltet und bei Gericht anerkannt wird. Zudem muss danach getrachtet werden, dass der länderübergreifende Datenverkehr nicht behindert wird.

[310] Vgl. http://www.a-sit.at/de/signatur/index.php [10.März 2008]
[311] http://www.signatur.rtr.at/de/legal/sigg.html [10. März 2008]
[312] Vgl. http://www.internet4jurists.at/intern25a.htm [10. März 2008]

In der Europäischen Union (kurz: EU) wurde bereits am 13.12.1999 die *Richtlinie 99/93/EG*[313] *über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen* verabschiedet. Nach *Artikel 5* der Richtlinie dürfen elektronische Signaturen im geschäftlichen Verkehr nicht diskriminiert und müssen von Gerichten und Behörden anerkannt werden. Der eigenhändigen Unterschrift gleichgestellt werden elektronische Signaturen nur dann, wenn sie den im Anhang der Richtlinie erläuterten Sicherheitsstandards entsprechen.

In Österreich ist das SigG (*BGBl I Nr. 190/1999*) seit 1.1.2000 in Kraft. Am 2.2.2000 wurde die *Signaturverordnung* mit *BGBl II Nr. 30/2000*[314] – zuletzt geändert durch *BGBl II Nr. 527/2004*[315] – kundgemacht. Die Novelle zum SigG *(BGBl I 2008/8*[316]) und die *Signaturverordnung 2008*[317] (kurz: SigV 2008; *BGBl II 2008/3*[318]) gelten seit 7.1.2008. Die Neuregelungen sollen eine Klarstellung und Vereinfachung der bestehenden signaturrechtlichen Bestimmungen herbeiführen und damit zur Verbreitung digitaler Signaturen beitragen. Der bislang weiter gefasste Anwendungsbereich des Gesetzes wird damit auf jenen der europäischen Signatur-Richtlinie 1999/93/EG eingeschränkt. Es erfolgt eine Anpassung von Begriffen an die in der Richtlinie. Dabei wird insbesondere der Begriff fortgeschrittenen elektronischen Signatur (§2 SigG Ziffer 3) sowie der qualifizierten elektronischen Signatur (§2 SigG Ziffer 3a) anstelle der sicheren elektronischen Signatur in das Gesetz aufgenommen. Die einfache Signatur bleibt bestehen. Neben natürlichen Personen können nun auch juristische Personen als Signator fungieren. Qualifizierte Zertifikate können allerdings – wie schon bisher – nur auf eine natürliche Person ausgestellt werden. Zu Erleichterungen kommt es bei der Identifikation von Personen, denen ein qualifiziertes Zertifikat ausgestellt wird: Während bisher ein amtlicher Lichtbildausweis zwingende Voraussetzung war, sind nun auch andere gleichwertige Methoden der Identitätsfeststellung zulässig (z. B.: Feststellung der Identität des Zertifikatwerbers mittels RSa-Brief).

Die verschiedenen Arten elektronischer Signaturen können grundsätzlich in ein abgestuftes System eingereiht werden. Je nach Sicherheitsniveau und Zertifikat, das bei der Signaturerstellung eingesetzt wird, erlangen die signierten Dokumente unterschiedliche Rechtswirkungen[319]: *einfache, fortgeschrittene* und *qualifizierte Signatur*, spezielle elektronische Signaturen (z.B.: *Amtssignatur, Rechnungssignatur*).

Das Signaturgesetz unterscheidet zwischen der einfachen, der fortgeschrittenen und der qualifizierten elektronischen Signatur. Für die einfache elektronische und fortgeschrittene Signatur ist ein von einer Zertifizierungsstelle ausgestelltes Zertifikat erforderlich, andere hardware- oder softwaretechnische

[313] http://eur-lex.europa.eu/de/index.htm [10. März 2008]
[314] http://www.a-sit.at/pdfs/SigV2000.pdf [10. März 2008]
[315] http://www.a-sit.at/de/dokumente_publikationen/gesetze/ [10. März 2008]
[316] http://www.a-sit.at/pdfs/SigG%20Novelle%202007%20BGBl%208_2008.pdf [10. März 2008]
[317] http://www.signatur.rtr.at/de/legal/sigv.html [10. März 2008]
[318] http://www.a-sit.at/pdfs/SigV_2008.pdf [10. März 2008]

Ausrüstungen sind nicht vorgesehen. Vielfach wird die einfache elektronische Signatur für das Signieren von E-Mails verwendet, die fortgeschrittene Signatur für die Erstellung sogenannter „Serversignaturen“ (z. B.: Amtssignatur, Rechnungssignatur). Als Beweismittel vor Gericht ist zwar die einfache elektronische Signatur verwendbar, der eigenhändigen Unterschrift entspricht rechtlich ausschließlich die qualifizierte elektronische Signatur. Für die Erstellung einer qualifizierten elektronischen Signatur sind eine Chipkarte (z. B. Bankomatkarte, e-Card), ein Lesegerät und eine Software (*Secure Viewer*[320]) erforderlich. Zudem ist ein qualifiziertes Zertifikat[321] notwendig, mit dem die Identität des Chipkarten-Inhabers bestätigt wird. In Österreich bietet die Firma A-Trust solche Zertifikate (siehe *1.7.2.1.6 Digitale Zertifikate*) für qualifizierte elektronische Signaturen an. Die qualifizierte elektronische Signatur ist nicht für jede Anforderung geeignet. Qualifizierte elektronische Signaturen können nicht automatisiert erstellt werden, weil die Signaturfunktion eine PIN-Eingabe erforderlich macht.

Bis Dezember 2007 gab es, aufgrund der einfacheren Handhabung in Verwaltungsverfahren, Verwaltungssignaturen. Die bis zu diesem Zeitpunkt ausgestellten Signaturen bleiben bis zum Ablauf des Zertifikates, längstens jedoch bis 31.12.2012, gültig. Die für eine Verwaltungssignatur erforderliche „Bürgerkarte"[322] musste keine Chipkarte sein, sondern konnte auch als Funktion virtuell existieren, etwa in Form der von der Firma *Mobilkom*[323] angebotenen *A1-Signatur*[324] (Anm.: Dienst von Mobilkom mit 2. Jänner 2008 beendet).

Zudem existieren verschiedene Spezialformen elektronischer Signaturen, die bekannteste ist die Amtssignatur. Mit der Amtssignatur[325] können behördliche Dokumente (z. B.: Bescheide) signiert werden, die Besonderheit liegt in der bildlichen Darstellung („Bildmarke“) und in einem besonderen Attribut im Signaturzertifikat („Behördenkennzeichen“). Andere Beispiele sind die *elektronische Signatur der Justiz*, die *elektronische Notarsignatur*, die *Archivsignatur* und die Rechnungssignatur.

---

[319] Vgl. http://www.digitales.oesterreich.gv.at/site/5567/default.aspx [10. März 2008]
[320] Vgl. http://www.signatur.rtr.at/de/security/faq160.html [10. März 2008]
[321] Vgl. http://www.signatur.rtr.at/de/security/faq210.html [10. März 2008] Bei einem qualifizierten Zertifikat handelt es sich um ein Zertifikat, das den Anforderungen von §5 und §7 SigG entsprechen muss. Ein qualifiziertes Zertifikat hat zumindest folgende Angaben zu enthalten: Den Hinweis darauf, dass es sich um ein qualifiziertes Zertifikat handelt. Den unverwechselbaren Namen des Zertifizierungsdiensteanbieters und den Staat seiner Niederlassung. Den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muss. Gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft des Signators. Die dem Signator zugeordneten Signaturprüfdaten (Public Key). Beginn und Ende der Gültigkeit des Zertifikats. Die eindeutige Kennung des Zertifikats. Gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats. Gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist. Auf Verlangen des Zertifikatswerbers weitere rechtlich erhebliche Angaben.
[322] http://www.buergerkarte.at/ [10. März 2008]
[323] http://www.mobilkom.at/ [10. März 2008]
[324] Vgl. http://www.a1.net/business/a1signatur [10. März 2008]

Exkurs: Signieren und Verschlüsseln

Während beim Signieren die Nachricht im Klartext verschickt wird, wird beim Verschlüsseln der Text mit den vorgestellten Methoden chiffriert. Schützenswerte Informationen sollten demnach verschlüsselt und signiert übertragen werden.

Signieren

- Sicherstellung der Authentizität und Integrität.
- Signieren mit privatem Schlüssel des Signators.
- Prüfung der Signatur mit öffentlichem Schlüssel des Signators.

Verschlüsseln

- Sicherstellung der Vertraulichkeit.
- Verschlüsseln mit öffentlichem Schlüssel des Empfängers.
- Entschlüsseln mit privatem Schlüssel des Empfängers.

1.7.2.1.8 Exkurs: E-Mail-Sicherheit

E-Mails werden grundsätzlich in Klartext übertragen, folglich können sie mit einfachen Mitteln (mit)gelesen werden. Ein weiteres Problem ist die simple Möglichkeit, die Absenderadresse zu fälschen (siehe *1.4.3.6 Spoofing*). Dies zeigt sich vor allem bei Spams (siehe *1.6 Exkurs: E-Mail/Spam*) und bei Phishing-Angriffen (siehe *1.4.1.2 Exkurs: Phishing*). Per se ist zudem nicht feststellbar, ob die E-Mail beim Datentransfer in irgendeiner Form verändert wurde.

Die Sicherheitsanforderungen an eine E-Mail sind die eindeutige Identifizierung des Absenders (Authentizität), die Nicht-Bestreitbarkeit (Verbindlichkeit), die Unverfälschtheit der Nachricht (Integrität) und die Gewissheit der Exklusivität für den Kommunikationspartner (Vertraulichkeit). Die geeigneten Maßnahmen dazu sind die elektronische Signatur und die Verschlüsselung. Zwei Technologien zur Umsetzung dieser Maßnahmen sind die an anderer Stelle bereits erwähnten PGP und S/MIME. Zweiteres wird von vielen E-Mail-Clients wie Microsoft Outlook oder *Lotus Notes*[326] standardmäßig unterstützt, PGP wird durch Zusatzsoftware (engl. *Plug-Ins*) in die Clients integriert. Die Technologien arbeiten in ähnlicher Weise und nutzen PKI bzw. digitale Zertifikate.

S/MIME arbeitet auf Basis X.509 (siehe *1.7.2.1.6 Digitale Zertifikate*), für PGP hingegen gibt es (noch) keine X.509-Zertifizierung. Der Absender signiert die E-Mail mit seinem Private Key. Der Empfänger hat die Möglichkeit, mit dem im Zertifikat mitgeschickten Public Key des Absenders die E-Mail hinsichtlich Integrität und Authentizität zu überprüfen. Wenn die E-Mail auch vertraulich übertragen werden soll, verschlüsselt der Absender die E-Mail mit dem Public Key des Empfängers. Dieser kann mit seinem Private Key die E-Mail wieder entschlüsseln.

[325] Vgl. http://www.cio.gv.at/faq/Amtssignatur/ [15. Jänner 2007]
[326] http://www-306.ibm.com/software/lotus/ [11. Jänner 2007]

Grundsätzlich gibt es bei der E-Mail-Verschlüsselung und -Signierung den Client- und den Perimeter-Ansatz. Beim ersten wird die E-Mail im E-Mail-Client signiert beziehungsweise verschlüsselt, quasi eine *End-to-End*-Lösung. Der erhebliche Nachteil dabei ist, dass es Perimeter-Schutzprogrammen nicht möglich ist, die E-Mails auf Malicious Code hin zu überprüfen. Beim Einsatz einer Perimeter-Lösung wird durch zentrale Schutzprogramme Malware bereits vor dem Eindringen in das Unternehmensnetzwerk erkannt und eliminiert.

1.7.2.2 System-Hardening

Die Umsetzung von Maßnahmen auf Systemseite (Firewall, Betriebssystem, Datenbank, Applikation) zur Erhöhung des Sicherheitsniveaus wird als Hardening bezeichnet:

- Systemupdates: Programminstallationen, Service Packs, Security Updates etc.,
- Konfigurationsänderungen: Firewall-Regel, Windows Registry-Einträge etc.,
- *Service Stripping*[327],
- Kernelmodifikationen.

Am Beispiel eines Webservers (Microsofts Internet Information Server) sollen einige Hardening-Maßnahmen veranschaulicht werden. Der erste Schritt ist die Überprüfung, ob die Betriebssystem-Einstellungen den Einstellungen des IIS entsprechen bzw. nicht widersprechen. Der IIS wird in der Grundinstallation nur mit den minimalen Diensten versehen. Bei der Konfiguration muss vor allem auf die Parameter „Rechteverwaltung“ und „Zugriff“ besonderes Augenmerk gelegt werden, dazu müssen die Berechtigungen für Verzeichnisse im Betriebssystem angepasst werden. Hinsichtlich Web Service-Konfiguration sind die Services, die Interaktionen mit dem Internet erlauben, mit besonderer Sorgfalt einzustellen (zum Beispiel: *WebDAV*[328]). Neben Backup- und Wiederherstellung ist ein kontinuierlicher Updateprozess wesentlich.

1.7.2.3 Biometrie

Es gibt in vielen Bereichen großen Bedarf, Personen einwandfrei und unwiderlegbar zu identifizieren[329]. Die Berechtigung, ein Gebäude zu betreten, Geld von einer Bank abzuheben, einen Zugang zu elektronischen Daten zu erlangen etc. ist immer an die Identität einer Person geknüpft. Das einzige Mittel, die Identität einer Person unwiderlegbar festzustellen, ist die Erkennung eindeutiger persönlicher Eigenschaften. Die Technik zur Erkennung wird als Biometrie bezeichnet**.** Von den drei Möglichkeiten der Authentisierung von Personen anhand von Wissen, Besitz oder Eigenschaft bieten

[327] Entfernen/Deaktivieren von nicht benötigten Diensten und Services
[328] Web-based Distributed Authoring and Versioning (kurz: WebDAV) ist eine Erweiterung des HTTP-Protokolls zur Bereitstellung von Dateien im Internet.
[329] Vgl. http://www.identix.ch/Einfuehrung/Biometrie%20deutsch.htm [24. Jänner 2007]

sich biometrische Verfahren zur Festlegung der Authentizität am besten an[330]. Während Wissen (z. B.: PIN, Passwort) und Besitz (z. B.: Chipkarte) nur mittelbar und temporär einer Person zuordenbar sind, sind biologische Merkmale unmittelbar und dauerhaft an eine Person gebunden.

Körperliche Merkmale können nicht wie einer Person zugeordnete Besitzelemente verloren oder vergessen werden, sie sind auch nicht geheim. Biometrische Kennzeichen können nicht übertragen bzw. weitergegeben werden. Dadurch ergeben sich erhebliche Vorteile gegenüber einer Authentisierung mittels Besitz oder Wissen.

Biometrische Merkmale entstehen entweder genetisch, zufällig oder konditioniert[331].

Eine Liste im Zuge biometrischer Verfahren verwendeter Merkmale: Fingerabdruck, Gesichtsform, Handgeometrie, Handschriftdynamik, DNA, Retina, Rhythmus der Tastaturanschläge, Sprachbild, Unterschrift [A-Sit, 2004, S 4].

Biometrische Merkmale können durch Verfahren mit den Zielsetzungen „Identifikation“ und „Verifikation“ unterschieden werden [A-Sit, 2004, S5]:

- Identifikation (1:n-Vergleich, „Wer bin ich?“): Das Merkmal einer vorerst noch unbestimmten Person wird gegen eine Menge von Referenzdaten bekannter Personen verglichen, um die Person zu identifizieren. Das System liefert aufgrund des biometrischen Merkmals den Namen bzw. die UserID. Ein Beispiel dafür ist die Gebäude-Zugangskontrolle, bei der die Zugangsberechtigten den bekannten Personenkreis bilden.
- Verifikation (1:1-Vergleich, „Ich bin NN“): Diese wird im Zuge der Authentifizierung, also des Nachweises einer behaupteten Identität, durchgeführt. Der Anwender hinterlegt Referenzdaten entweder in einer von ihm kontrollierten Komponente (z. B.: Chipkarte) oder unter einem Identifikator, sodass die Verifikation des Merkmals gegen die dem Identifikator zugeordneten Referenzdaten erfolgt. Ein Beispiel für die Verifikation ist das Ersetzen einer PIN durch ein biometrisches Merkmal.

Das Grundprinzip der biometrischen Erkennung ist bei allen Systemen gleich. Alle biometrischen Systeme enthalten – unabhängig von ihrem oft individuellen technologischen Aufbau – die Komponenten der Personalisierung des Benutzers im System (engl. *Enrolment*), die Erfassung der biometrisch relevanten Eigenschaften einer Person und die Erstellung von Datensätzen (engl. *Templates*) sowie den Vergleich der aktuellen mit den gespeicherten Daten (engl. *Matching*). Die Erfassung biometrischer Merkmale erfolgt sowohl bei der erstmaligen Erfassung zur Erstellung des

[330] Vgl. http://www.bsi.bund.de/fachthem/biometrie/einfuehrung.htm – Einleitung [29.Jänner 2007]
[331] Vgl. http://www.bsi.bund.de/fachthem/biometrie/einfuehrung.htm – Biometrische Merkmale und Verfahren – Grundsätzliche Verfahrensweise [29. Jänner 2007]

sogenannten Referenzdatensatzes als auch bei der späteren Erfassung zur Wiedererkennung durch Sensoren wie Kamera, Mikrofon, Tastatur, Geruchssensoren oder Fingerabdrucksensoren[332].
Biometrische Verfahren sind nie ganz exakt, Personen sind nur mit einer gewissen Wahrscheinlichkeit bestimmbar. Die Zuverlässigkeit der Identifikation bzw. Verifikation wird hauptsächlich nach zwei Kriterien beurteilt: nach der Zulassungsrate Unberechtigter (*Falschakzeptanzrate* (kurz: *FAR*)) und nach der Abweisungsrate Berechtigter (*Falschrückweisungsrate* (kurz: *FRR*)).

1.7.2.3.1 Einsatzbeispiele

Biometrische Verfahren finden – neben den herkömmlichen – in vielen Bereichen des Internets Anwendung[333], um die Identifikation von Personen zu ermöglichen bzw. zu erleichtern:

- Digitalisierung der Kommunikation,
- E-Government-, E- und M-Commerce-Lösungen,
- Elektronische Signatur und Smartcard,
- Virtualisierung von Unternehmen.

Ein kurzer Auszug aus umgesetzten Projekten im Bereich Biometrie:
Seit dem 16. Juni 2006 werden in Österreich in Umsetzung von EU-Vorgaben nur noch Reisepässe (*Sicherheitspass*[334] [BMI, 2005-1]) mit einem Chip und einem gedruckten Foto ausgegeben.
Während im österreichischen Parlament Notebooks mit Fingerprint-Zugang im Einsatz sind[335], authentifiziert der Flughafen in Frankfurt registrierte Vielflieger mittels Irisscan[336].

1.7.2.3.2 Sicherheitsaspekte und Datenschutz

Bei biometrischen Daten handelt es sich um personenbezogene Daten[337] [Dohr, Weiss, Pollirer, 2006, S 39] (siehe *1.7.3.1 Datenschutz*), und damit laut *§4 Abs. 1 DSG*[338] um „Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist“. Eine Verarbeitung von biometrischen Daten ist daher nur zulässig, wenn entweder eine gesetzliche Grundlage oder eine freiwillige Einwilligung des Betroffenen vorliegt (vgl. *§§§6, 7, 8 DSG*).

---

[332] Vgl. http://www.bsi.bund.de/fachthem/biometrie/einfuehrung.htm – Ablauf einer biometrischen Erkennung [1. Feber 2007]
[333] Vgl. http://www.innovation-aktuell.de/kl0319.htm [1. Feber 2007]
[334] Vgl. http://www.help.gv.at/Content.Node/2/Seite.020950.html [2. Feber 2007];
http://www.bmi.gv.at/oeffentlsicherheit/2005/09_10/BIOMETRIE.pdf [2. Feber 2007]
[335] Vgl. http://www.parlament.gv.at/portal/page?_pageid=908,212516&_dad=portal&_schema=PORTAL [2. Feber 2007]
[336] Vgl. http://www.tecchannel.de/news/themen/business/420011/ [2. Feber 2007]
[337] http://ris.bka.gv.at/taweb-cgi/taweb?x=d&o=l&v=jus&db=JUST&t=doc4.tmpl&s=(9ObA109/06d) [12. März 2007];
http://www.lfd.niedersachsen.de/master/C27956_N13146_L20_D0_I560.html [12. März 2007]
[338] http://www.dsk.gv.at/dsg2000d.htm#4 [1. Feber 2007]

Bei einem datenschutzfreundlichen Verfahren werden bereits beim Enrolment nur die für einen späteren Vergleich notwendigen Daten erfasst und gespeichert. Damit wird ausgeschlossen, dass aus den Rohdaten Rückschlüsse auf persönliche Merkmale gezogen werden, die über den eigentlichen Verwendungszweck hinausgehen. Eine Speicherung der vollständig erhobenen biometrischen Daten ist in der Regel nicht notwendig[339].

Bei der Verspeicherung der Referenzdaten gibt es zwei unterschiedliche Ansätze: In Identifikationssystemen ist eine zentrale Verwahrung von Referenzdaten (z. B.: Datenbank) erforderlich. In Verifikationssystemen können die Referenzdaten unter Kontrolle des Benutzers stehen (z. B.: Chipkarte).

Seit 2004 werden bei allen einreisenden Nicht-US-Bürgern im Rahmen des *US-Visit*-Programms[340] Fingerabdrücke sowie Lichtbild erfasst und in Datenbanken verspeichert. Dieses Beispiel zeigt die Unerlässlichkeit, datenschutzrechtliche Grundprinzipien einzuhalten.

1.7.2.4 Perimetersicherheit

Wie schon bei den Anforderungen an die Informationssicherheit (siehe *1.2.2 Anforderungen an die Informationssicherheit*) erläutert, werden unter Perimetersicherheit die Schutzmaßnahmen (Firewall, Webfilter, Virenscanner etc.) am Übergang zwischen dem Internet und dem Unternehmensnetz verstanden. Ein Beispiel für Perimeterschutz ist die sogenannte *Demilitarized Zone* (kurz: *DMZ*), die durch Firewallsysteme getrennt von außen und innen erreichbar ist, wobei eine Direktverbindung durch die DMZ jedoch nicht möglich ist.

1.7.2.4.1 Firewall

Unter einer Firewall[341] werden Systeme verstanden, die den Zugriff und Datenverkehr zwischen verschiedenen Netzwerken regeln. Der klassische Anwendungsfall ist der Schutz des Firmennetzwerkes vor dem Internet.

Firewallsysteme können sowohl aus Hardware- als auch Softwarekomponenten bestehen.

Die Arbeitsweise von Firewalls ist sehr unterschiedlich ausgerichtet:

- *Paket-Filter* benutzen die Headerinformationen (z. B.: IP-Adresse) der Datenpakete und Ports (Dienste), um zu entscheiden, wie ein entsprechendes Paket behandelt werden soll: Weiterleiten, Verwerfen, Protokollieren etc.

[339] Vgl. http://www.bfdi.bund.de/nn_533592/DE/Schwerpunkte/Biometrie/Artikel/BiometrieUndDatenschutz.html [17. März 2008]

[340] Vgl. http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm [1. Feber 2007]

[341] Vgl. http://www.tecchannel.de/sicherheit/grundlagen/401639/ [15. Jänner 2007]; http://www.bsi-fuer-buerger.de/infiziert/06_05.htm [15. Jänner 2007]; http://www.sicher-im-internet.at/allgemein/firewall.html [15. Jänner 2007]; http://www.howstuffworks.com/firewall.htm [15. Jänner 2007]

- Bei der *Stateful Inspection*-Methode merkt sich die Firewall im Gegensatz zum Paketfilter den Status einer Verbindung und kann dadurch ein neues Datenpaket einem zusammenhängenden logischen Datenstrom zuordnen.
- *Application Level*-Firewalls bedienen sich der Informationen der Anwendungsschicht (siehe L7 *Abbildung 4: Protokolle des OSI-Schichtenmodells*). Damit können die Nutzdaten ausgewertet oder nicht erwünschte Anwendungsprotokolle blockiert werden.

In den letzten Jahren ist neben den in Unternehmen unerlässlichen *Netzwerk Firewalls* durch die steigende Mobilität auch die Bedeutung der *Personal Firewall* gestiegen. Die Personal-Firewall ist auf Clientseite installiert und dafür bestimmt, den Datenverkehr des Endbenutzers ortsunabhängig zu schützen.

1.7.2.4.2 Content-Filter

Content-Filter[342] überprüfen die Daten auf Applikationsebene (siehe auch Application-Level-Firewalls). Typische Aufgabe eines Content-Filters sind das Filtern von ActiveX-, JavaScript-Elementen und Spams, das Löschen von E-Mails mit verseuchtem Code, Sperren von Inhalten etc.
In der Praxis ist ein solches System nicht ohne ständige Kontrolle und manuelle Eingriffe einsetzbar. Der Prozess der Filterung ist ein schwieriger Vorgang, es kann vor allem im Bereich der E-Mails vorkommen, dass nicht gewünschte Mails zugestellt („*false negative*“) und gewünschte Mails gefiltert („*false positive*“) werden. Zudem kommt die Problematik der Verschlüsselung an zentraler Stelle (siehe *1.7.2.1.8 Exkurs: E-Mail-Sicherheit*).

1.7.2.4.3 Proxy

Ein Proxy[343] baut stellvertretend für Rechner die Verbindung zu Servern im Internet auf. Damit wird der Datentransfer effizienter bzw. schneller, womit auch die Sicherheit erhöht wird.
Gemeinhin wird unter dem Begriff „Proxy“ ein HTTP-Proxy verstanden, der die Daten zwischen Client und Webserver transferiert. Ein Proxy kann mehrere Funktionen erfüllen.

- Cache: ein Proxy speichert Daten besuchter Webseiten. Wenn erneut eine Anfrage nach einer Webseite erfolgt, prüft der Proxy, ob die Webseite bereits indiziert ist. Ist dies der Fall, bekommt der Besucher der Webseite die Daten prompt aus dem Cache geliefert. Dabei hat der Proxy sicher zu stellen, dass der gelieferte Inhalt nicht veraltet ist. Ist diese Webseite noch nicht gespeichert, wird der Besucher vom Proxy zu der gewünschten Seite verbunden. Das Zwischenspeichern der

[342] Vgl. http://www.virenschutz.info/Content-Filter-Techniklexikon-bei-Virenschutz-info_201.html [17. Jänner 2007];
http://www.tecchannel.de/client/sicherheit/402413/index4.html [17. Jänner 2007]
[343] Vgl. http://www.itwissen.info/definition/lexikon//_proxy%20server_proxy-server.html [17. Jänner 2007];
http://www.lexikon-suchmaschinenoptimierung.de/proxy-server.htm [17. Jänner 2007]

Webseiten erhöht die Antwortzeiten und reduziert die Netzlast. Zudem kann ein Proxy verschiedenen Benutzern je nach Auslastung unterschiedliche Bandbreite zur Verfügung stellen.

- Filter (siehe *1.7.2.4.2 Content-Filter*): mit Proxys können bestimmte Webseiten gesperrt bzw. Zugriffe darauf (Surfverhalten der User) protokolliert werden.
- Client-Anonymisierung: Beim Weiterleiten der Daten des Clients an den Webserver durch den Proxy bzw. die Firewall wird die IP-Adresse des Servers/der Firewall mitgeschickt und die IP-Adresse des Clients bleibt verborgen.

Proxys gibt es nicht nur für das HTTP-Protokoll, sondern auch für das SMTP-Protokoll. SMTP-Proxys überwachen und filtern den Mailverkehr zwischen Internet und Mailserver.
Ein *Reverse-Proxy*[344] hingegen ist ein Proxyserver, der logisch vor dem Unternehmens-Webserver platziert wird. Alle HTTP-Requests aus dem Internet werden durch den Proxyserver bedient, der die Anfragen entweder selbst beantwortet (Cache) oder sie an den Webserver weitergibt. Reverse Proxys sind ein wirksames Mittel gegen Webserver-Attacken aus dem Internet.
Als *Offene Proxys* werden jene Proxys bezeichnet, die ohne Anmeldung benutzt werden können. Diese werden zur Anonymisierung von Clients benutzt. Vor allem bei Kaskadierung mehrerer offener Proxys ist eine Rückverfolgung schwer möglich.
Der Einsatz eines Proxy-Servers sollte genau überlegt sein. Mit einem mangelhaft konfigurierten Proxy kann es Dritten ermöglicht werden, die eigene Adresse zu verbergen. Bei Misskonfiguration eines Reverse Proxys kann die Sicherheit des internen Netzwerks bedroht sein.

1.7.2.4.4 Intrusion Detection Systeme und Intrusion Prevention Systeme

Intrusion Detection Systeme (kurz: *IDS*)[345] [Bacher, 2004] erkennen unerwünschte Zu- und Angriffe auf Computersysteme. Zudem kann mit einem IDS der unternehmensinterne Datenverkehr überwacht werden. Neben der Überwachung des Netzwerktraffics bietet ein IDS Informationen einerseits zur Auslastung des Netzwerks andererseits über ungewöhnliche Aktivitäten. Intrusion Detection Systeme vergleichen den Datenstrom mit bekannten Angriffssignaturen aus der Musterdatenbank. Sobald ein Regelverstoß erkannt wird, erfolgt neben der Protokollierung die Meldung an die Systemadministration, welche sofort manuelle Gegenmaßnahmen setzen muss.
Mit *Intrusion Prevention Systemen* (kurz: *IPS*) hingegen können automatisiert Gegenmaßnahmen getroffen werden, wie zum Beispiel das temporäre Sperren einer IP-Adresse oder das Verwerfen von Datenpaketen.

[344] Vgl. http://www.united-security-providers.ch/web/tt/produkte/secure-entry-server/technologie/reverse-proxy/ [17. Jänner 2007]
[345] Vgl. http://www.synspector.de/ids_systeme/was_sind_ids.asp [22. Jänner 2007]

1.7.2.4.5 Network Access Control

Network Access Control (kurz: *NAC*)[346] ist eine Netzwerksicherheitstechnologie, die Unternehmen vor Malware, unkontrolliertem Zugriff durch LAN/WLAN bzw. fehlendes Patchmanagement schützt. Im Wesentlichen geht es darum, einen Client beim Verbindungsaufbau mit dem Netzwerk zu identifizieren, seine Konformität mit vorhandenen Sicherheitsrichtlinien zu überprüfen und entsprechend den Zugriff auf die Netzwerkressourcen zu gewähren bzw. zu verbieten. Technisch vergleicht diese Integritätsfunktion den Client-Status mit vordefinierten Vorlagen (Patch-Version, Service Packs, Virenschutz, Firewall) und führt auf die Unternehmensumgebung abgestimmte Prüfungen durch. Um nichtaktuelle Clients und Gastgeräte auf den letzten Stand bzw. Mindeststandard zu bringen, bietet NAC eine sogenannte Quarantäne-Funktion.

NAC gibt es in den Ausführungen mit bzw. ohne Agent. Agent-basiertes NAC ist dezentral ausgelegt und dadurch schneller. Dafür muss auf jeden Client ein Agent ausgebracht werden. Die Installation der Clients und die Verwaltung können aufgrund der Gerätevielfalt und Betriebssystemunterschiede (Notebook, PC, Drucker, VoIP-Telefon, PDA, Gast-Notebook etc.) in einem Netzwerk relativ umfangreich und komplex werden. *Agentless*-NAC arbeiten zentral ohne Installation auf den Clients. Die Komplexität reduziert sich gegenüber Agent-basierenden NACs dadurch, dass keine Software installiert werden muss. Die verschiedenen Geräte und Betriebssysteme können daher im Netzwerk leichter gehandhabt werden, zudem werden die Interaktionen mit den Benutzern minimiert.

Eine nicht ausgereifte NAC-Implementierung kann die Funktion des gesamten Netzwerks beeinträchtigen. Je nach Implementierung kann die Bereitstellung und Verwaltung ein zeitaufwändiger Prozess sowohl für Benutzer als auch für die IT-Administration sein.

1.7.2.5 Graphisches Passwort

Neben den herkömmlichen Empfehlungen und Lösungen für die Handhabung von Passwörtern gibt es mit dem grafischen Passwort einen neuen Ansatz. Das Unternehmen *MERLINnovations*[347] hat mit *SecLookOn* [MERLINnovations, 2007] ein graphisches Authentifizierungsverfahren entwickelt. Mit Hilfe der sogenannten *Challenge-Response*-Methode wird dem Anwender eine Frage (Challenge) gestellt, welche der User beantwortet (Response). Die Frage ist durch die steganographische Aufbereitung (siehe *1.7.2.1 Kryptologie*) nur für den Anwender erkennbar. Die Eingabe ist durch die besondere Struktur auch bei der gleichen Frage immer eine andere und daher ein Einmalcode (engl. *One-Time-Code*). Auf eine genauere Erklärung des Autorisierungs- und Authentifizierungsprozesses wird an dieser Stelle verzichtet, nähere Informationen sind dem angeführten Weblink zu entnehmen.

[346] Vgl. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html [5. Feber 2007]; http://www.symantec.com/Products/enterprise?c=prodinfo&refId=1304&ln=de_DE [5. Feber 2007]
[347] http://www.merlinnovations.com/ [9. März 2007]

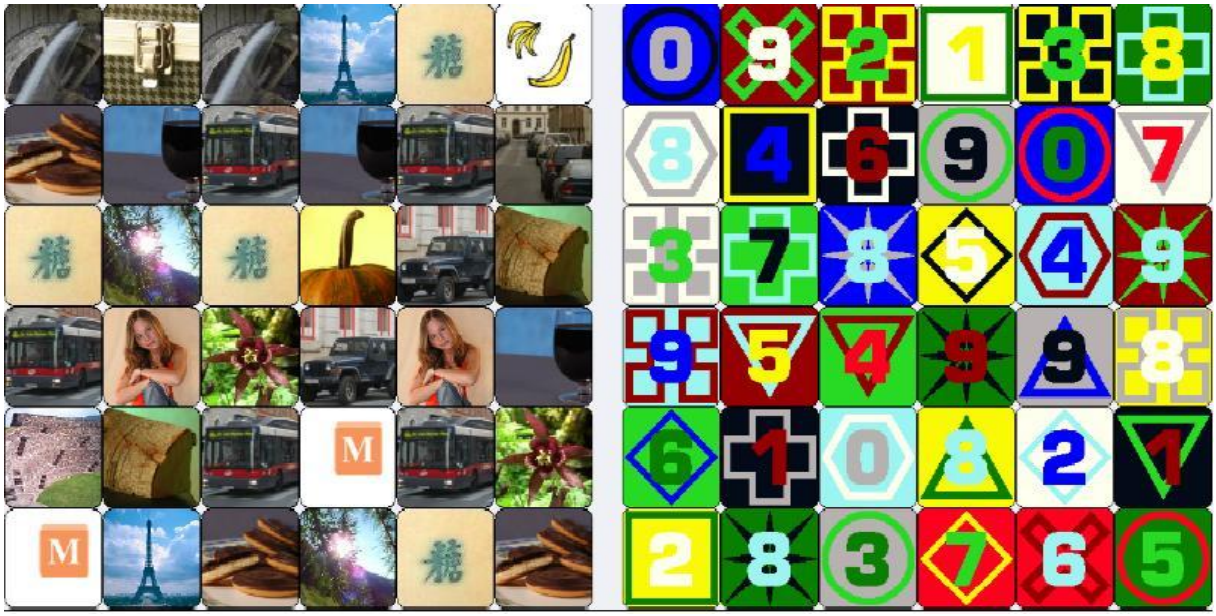


Abbildung 23: Beispiel für Authentifizierung nach SecLookOn

Auf Anwenderseite ist lediglich ein Webbrowser notwendig, damit ist diese Lösung flexibel einsetzbar. SecLookOn bietet Schutz etwa gegen Phishing (siehe *1.4.1.2 Exkurs: Phishing*), Crackerangriffe (siehe *1.4.3.1 Exkurs: Script Kiddie/Hacker/Cracker*) oder Man in the Middle-Attacken (siehe *1.4.3.4 Passwort-Attacken*).

1.7.2.6 Neue und alternative Ansätze des Schutzes vor Malicious Code

Die Innovationszyklen und die fortschreitende Entwicklung von Malware verlangen nach immer neuen Abwehrmethoden. Die Firma *HP* hat mit der *Virus Throttle*-Software[348] ein Produkt am Markt, das unkonventionelle Ansätze zur Bekämpfung von Viren bietet. Virus Throttle sucht nach virus-ähnlichen Verhaltensmustern, reduziert oder stoppt Netzwerkverbindungen eines potenziell infizierten Geräts solange, bis auszuschließen ist, dass es sich um keinen Virenangriff handelt. Je schneller Malicious Code sich verbreitet, desto schneller reagiert das Schutzprogramm, und zwar ohne menschliches Zutun, zudem wird ein Alarm für die IT-Administration ausgelöst.
IBM präsentiert eine Möglichkeit, Computer ohne Schutzsoftware vor Malware zu schützen[349]. Die Methode arbeitet – im Gegensatz zu den herkömmlichen – mit Whitelists anstelle von Blacklists. Das Grundprinzip dabei ist, im Kernel nur zuvor autorisierten Code auszuführen. Eine im Betriebssystem-Kernel des Rechners laufende Runtime-Software hat zur Aufgabe, nur erlaubte Programme zu exekutieren. Die Kehrseite ist der hohe administrative Aufwand: beispielsweise muss nach jedem Update die auszuführende Software wieder erlaubt werden.

[348] Vgl. http://www.hp.com/rnd/news/virus_throttle_software.htm [1. Feber 2007]
[349] Vgl. http://www.almaden.ibm.com/ [1. Feber 2007]

Eine Lösung namens *InterCloud Security Service*[350] des Herstellers Trend Micro soll ferngesteuerte Computernetzwerke (siehe *1.3.4.1.1 Exkurs: Botnet*) in Echtzeit erkennen und isolieren. Mit diesem Produkt können Netzwerke mit vielen Hosts (z. B.: Internet Service Provider) geschützt werden, indem beispielsweise der Zugang zum Netz verweigert oder die Quarantäne-Funktion aktiviert wird.
Die Firma Symantec bietet mit *Norton Confidential*[351] ein Sicherheitsprogramm, das die Anwender vor Gefahren aus dem Internet (gefälschte Webseiten, Schadprogramme) schützen soll, welche auf das Ausspionieren von (sensiblen) Daten abzielen. Zur Identifizierung von Phishing-Seiten kombiniert die Lösung herkömmliche Sperrlisten mit heuristischer Technologie. Das Ziel ist, bei der Dateneingabe Aktionen von Keylogger- oder *Screencapture*-Programmen zu verhindern.

1.7.2.7 Sicherheitsmaßnahmen von Microsoft

Die Verbreitung der Betriebssysteme von Microsoft ist direkt proportional zu dessen Bedeutung für das Sicherheitsniveau. Vor allem im Hinblick auf Botnets (siehe *1.3.4.1.1 Exkurs: Botnet*) ist im privaten Umfeld ein sicherer PC ohne viel Zutun des Benutzers oberstes Ziel (siehe *1.7.1.3 Grundsätze im Umgang mit PCs zum Schutz vor Malicious Code*). Das am 30. Jänner 2007 am Markt erschienene Client-Betriebssystem *Windows Vista*[352] umfasst eine Menge von Sicherheitsfeatures[353]:

- Der Benutzerkontenschutz ermöglicht es Benutzern ohne administrative Rechte produktiv zu arbeiten und allgemeine Systemeinstellungen zu ändern. So wird verhindert, dass die Benutzer potenziell gefährliche Änderungen vornehmen. Administratoren-Rechte werden passwortgeschützt nur für bestimmte Installationsprozesse und den damit zusammenhängenden Zeitraum gewährt. Damit will Microsoft verhindern, dass schadhafte Programme ohne Wissen der User und unter Ausnützung von Administratoren-Rechten ins System eindringen können.
- Microsoft Internet Explorer, der standardmäßige Webbrowser von Windows Vista, hat viele Erweiterungen im Bereich Sicherheit erfahren. Er schützt den Benutzer vor Phishing- (siehe *1.4.1.2 Exkurs: Phishing*) und Spoofing- (siehe *1.4.3.6 Spoofing*) Angriffen. Ein Feature ist beispielsweise der geschützte Modus. Dabei werden Applikationen als Dienste mit niederer Berechtigung eingestuft, die nicht direkt auf das Betriebssystem zugreifen dürfen. Dadurch wird verhindert, dass mit Malware versetzte Websites die Daten des Benutzers missbrauchen oder Konfigurationsänderungen vornehmen.
- Windows Vista erkennt durch die Zwei-Wege-Firewall und das *Windows Defender*-System viele Arten potenziell gefährlicher Codes.

[350] Vgl. http://www.trendmicro.com/en/products/nss/icss/evaluate/overview.htm [1. Feber 2007]
[351] Vgl. http://www.symantec.com/home_homeoffice/transactsafely/overview.jsp [1. Feber 2007]
[352] http://www.microsoft.at/windowsvista/default.html [2. Feber 2007]
[353] Vgl. http://www.microsoft.com/germany/technet/prodtechnol/windowsvista/evaluate/feat/secfeat.mspx [2. Feber 2007]

- Filterprogramme für ausgehenden Netzwerkverkehr ermöglichen die administrative Kontrolle über Peer-to-Peer-Filesharing-Anwendungen.
- Die Absicherung der Dienste (siehe *1.7.2.2 System-Hardening*) kann den Schaden, den Angreifer im Fall einer Kompromittierung eines Dienstes anrichten können, einschränken.
- Administratoren können den Netzwerkzugriffsschutz (siehe *1.7.2.4.5 Network Access Control*) nutzen, um den Zugriff für nicht den Vorgaben entsprechenden Clients auf das interne Netzwerk zu verhindern. So wird die potenzielle Ausbreitung von Malware auf andere Rechner verhindert.
- *BitLocker* ist eine Möglichkeit zur Datenverschlüsselung für mobile und stationäre Geräte. Mit BitLocker sind die vollständige Verschlüsselung von Laufwerken (inklusive Systemdateien, Auslagerungsdatei und Ruhezustands- (engl. *Hibernation*) Datei) und die Integritätsüberprüfung von Komponenten beim Systemstart möglich. Die Integritätsprüfung beim Systemstart stellt sicher, dass eine Datenentschlüsselung und damit ein Betriebssystemstart nur dann erlaubt wird, wenn die entsprechenden Komponenten unverändert sind und sich das verschlüsselte Laufwerk im entsprechenden Computer befindet. Mit BitLocker wird verhindert, dass ein Nicht-Berechtigter ein anderes Betriebssystem startet oder ein Tool verwendet und so die Systemverschlüsselung von Vista umgeht. Im Idealfall wird auch Hardware in Form des *Trusted Platform Module* (kurz: *TPM 1.2*)[354] (siehe *1.7.2.8 Trusted Computing*) verwendet, um die Daten bzw. Schlüssel zu hinterlegen. Standardmäßig ist für BitLocker keine Aktion des Endbenutzers notwendig, sogar die Aktivierung kann remote und automatisch durchgeführt werden.
- Die *Parental-Control*-Funktion gibt Eltern/Erziehungsberechtigten eine weitreichende Kontrolle über die Webaktivitäten ihrer Kinder. So können Eltern festlegen, welche Webseiten besucht werden dürfen und von welchen Adressen Downloads gestattet sind.
- Der Verlust oder Diebstahl des intellektuellen Eigentums eines Unternehmens (siehe *2.3.3.5 Digital Rights Management*) ist eine immer stärker werdende Bedrohung. Der integrierte *Rights Management-Client* ermöglicht es Organisationen, Richtlinien bezüglich der Nutzung von Dokumenten durchzusetzen.
- Mit *Forefront*[355] gibt es eine vollständige Sicherheits-Suite (Schutz vor Malicious Code, gesicherter Zugang zum Unternehmen, Updatemanager etc.) mit Integrationsmöglichkeit in Verzeichnisstrukturen und in Kommunikationsplattformen.

[354] TPM ist ein Hardware-Chip, der zur Erhöhung der Datensicherheit auf Computern beitragen soll. Der Chip ist nicht User-, sondern Systemgebunden, zudem enthält er eine eindeutige Kennung zur Identifizierung des Rechners. Eine Ausführung von bestimmten Anwendungen kann nur bei aktiviertem TPM erlaubt werden.
[355] http://www.microsoft.com/forefront/default.mspx [28. Feber 2007]

1.7.2.8 Trusted Computing

Hierbei handelt es sich um ein Konzept, das manipulationssichere Hardware zum Ziel hat. Neben dem Schutz von privaten Daten soll insbesondere die Integrität eines Betriebssystems sichergestellt werden. Umsetzung findet das Konzept in Form eines Hardwarebausteines. Dieser Baustein wird von einer Gruppe von Unternehmen[356], die sich als *Trusted Computing Group (*kurz: *TCG)*[357] zusammengeschlossen haben, unter dem Namen *Trusted Platform Module* (kurz: *TPM*)[358] (siehe *1.7.2.7 Sicherheitsmaßnahmen von Microsoft*) spezifiziert. Die zum großen Teil frei zugänglichen Spezifikationen werden von der TCG laufend überarbeitet, die ersten Versionen der Spezifikation dienen als Grundlage für die TPM-Chips[359].

Um die Manipulation von Soft- und Hardware zu entdecken, muss ein System geschaffen werden, welches selbst weder physisch noch softwaretechnisch manipulierbar ist und so auf eine sichere Weise Referenzwerte speichern kann. Diese Funktionalitäten werden im TPM realisiert [Gerstbach, Tomek, 2003, S 6]:

- Generierung und sichere, persistente Speicherung von geheimen Schlüsseln,
- Sichere Ablage von als vertrauenswürdig eingestuften Systemkonfigurationen,
- Bereitstellung von speziellen Schlüsseln und anonymen Identitäten, mit denen die Plattformen Dritter als vertrauenswürdig erkannt werden können bzw. um Daten mit anderen Plattformen auszutauschen,
- Verwaltungsfunktionen, mit denen unter anderem das TPM von einem Benutzer ein- und ausgeschaltet werden kann.

Viele renommierte Hersteller bieten Lösungen an: *Infineon*[360], IBM (*Lenovo* Notebooks)[361] oder HP (Notebook, Server)[362]. Es werden immer mehr TPM-Chips in neue Systeme verbaut, eine vollständige Akzeptanz und Durchdringung kann aber nur erreicht werden, wenn die Funktionalitäten von TPM vollkommen in die Hardware und die Betriebssysteme integriert werden. Beispielsweise gibt es seit Jahren in diesem Bereich Bestrebungen von Intel und Microsoft. Intel bezeichnet sein umfassendes Hardwaresicherheitskonzept als *„LaGrande Technology"* (kurz: *LT*)[363]. Bei LT werden durch die geschützte Ausführung und den geschützten Input/Output der Schutz und die Integrität von Daten verbessert, die auf einem Client-PC gespeichert oder erstellt werden. Mithilfe von LT will Intel Software-Angriffe auf einen in der Hardware verankerten Systemschutz unmöglich machen. Durch LT

[356] https://www.trustedcomputinggroup.org/about/members/ Aktuelle Mitglieder [4. Feber 2007]
[357] https://www.trustedcomputinggroup.org/home [4. Feber 2007]
[358] https://www.trustedcomputinggroup.org/groups/tpm/ [4. Feber 2007]
[359] Vgl. http://www.bsi.de/sichere_plattformen/trustcomp/ [4. Feber 2007]
[360] http://www.infineon.com/tpm [4. Feber 2007]
[361] http://www.pc.ibm.com/europe/security/de/index.html [4. Feber 2007]
[362] http:://www.hp.com/ [4. Feber 2007]

sollen Manipulationen an Eingabegeräten wie Tastatur oder Maus und Veränderungen der Ausgabe über Grafikkarten verhindert werden. Am TPM-Chip werden innerhalb von LT die Schlüsselverwaltung und die Speicherung der Konfigurationen vorgenommen.

Microsoft erarbeitet unter dem Titel „*Next Generation Secure Computing Base"*[364] (kurz: *NGSCB*) Sicherheitslösungen. Auf der Hardwareseite benötigen die Betriebssysteme von Microsoft einen TPM-Chip, mit dessen Hilfe die Kernfunktionalitäten[365] von NGSCB realisiert werden:

- über die Hardware abgesicherte vertrauenswürdige Anwendungsprogramme gegen Manipulations- und Ausspähungsversuche,
- die geschützte Ablage von Daten durch TPM,
- Sicherstellung einer unbeobachteten Eingabe und unveränderten Ausgabe sensibler Daten,
- Bereitstellung einer Art „Beglaubigung" der Vertrauenswürdigkeit des Gesamtsystems.

Neben TPM werden von TCG mit Software, Mobiles etc. noch einige andere Bereiche mehr untersucht und Lösungen angeboten.

Neben den positiven Aspekten für eine Erhöhung der Sicherheit bergen die Initiativen der TCG Missbrauchspotential und sorgen für Diskussionen:[366] „*Sowohl die TCG als auch die Hersteller schildern ihre Ziele nur unklar. Eine genaue Strategie, die konkrete Anwendungsszenarien beschreibt, sind sie bisher schuldig geblieben. Bisher kann der Benutzer eines PC, entsprechende Kenntnisse vorausgesetzt, seinen Rechner vollständig kontrollieren. Er hat alle Freiheiten, welche Software und Hardware er auf welche Weise einsetzen möchte. Zukünftig könnten diese Möglichkeiten bei einer restriktiveren Plattform mit einem sicheren Betriebssystem wegfallen. Mit dem Argument „Sicherheit" können Anwendungen gesperrt oder die Verwendung von Einsteckkarten abgelehnt werden. Die Konfiguration eines Rechners, die Lizenzierung der verwendeten Produkte und die Urheberrechte von gespeicherten Inhalten können jederzeit überprüft und an Dritte übermittelt werden. Der Benutzer muss sein Vertrauen in die Sicherheitskomponenten auf Schlüssel begründen, die er nicht selbst erzeugt hat. Ob die gespeicherten Schlüssel wirklich geheim und einmalig sind, ist nicht überprüfbar. Schließlich besteht die Gefahr, dass Hersteller von Hardware und Betriebssystemen die neuen Sicherheitsinitiativen nutzen, um bestehende Monopole zu festigen oder neue aufzubauen. Wesentliche Innovationen im Bereich der Informationstechnik beruhen aber gerade auf der Vielfältigkeit verfügbarer Lösungen. Hinzu kommt ein großer Anteil „offener Software" (Open Source Software), die für einen stetigen Transfer von Wissen in der Informationstechnik sorgt. Restriktive Systeme*

[363] Vgl. http://www.intel.com/technology/security/ [4. Feber 2007]
[364] Vgl. http://www.microsoft.com/resources/ngscb/default.mspx [4. Feber 2007]
[365] Vgl. http://www.bsi.de/sichere_plattformen/trustcomp/infos/tcgi.htm [4. Feber 2007]
[366] Vgl. http://www.bsi.de/sichere_plattformen/trustcomp/infos/tcgi.htm – Risiken und Missbrauch [4. Feber 2007]

könnten die Verwendung dieser freien Alternativen zu den rein kommerziellen Lösungen stark einschränken oder gar zum Erliegen bringen."

Eine von *Phoenix Technologies*[367] im Oktober 2006 präsentierte Studie[368] liefert Anbietern von Trusted Computing ein gutes Argument in der Kontroverse über diese Computersicherheitstechnologie. Die Studie kommt zum Schluss, dass jene Attacken am schädlichsten waren, bei denen die Login-Daten gestohlen wurden. Die Untersuchung ergab, dass 84 Prozent der Angriffe hätten verhindert werden können, wenn die Identität des ins Firmennetzwerk eindringenden Geräts überprüft worden wäre. Trotz allem wird von einigen[369] die Meinung vertreten, dass Trusted Computing „zuviel des Guten sein könnte" und es billigere und einfachere Möglichkeiten gibt: die Unterscheidung zwischen zugelassenen und nicht zugelassenen Computern könnte in einigen Bereich anhand von IP-Adressen erfolgen.

1.7.3 GESETZESLAGE

Das Internet ist kein rechtsfreier Raum[370], daher sind Eingriffe in Rechte Dritter (z. B.: Urheberrecht) sowie Bestimmungen des Zivil-, Straf- (siehe *1.3.5.1 Rechtlicher Rahmen*) und Wettbewerbsrechts als auch des Marken- und Persönlichkeitsschutzes zu beachten. Im Internet und bei den verschiedenen Kommunikationstechniken gibt es viele rechtlich ungeklärte Situationen und Probleme. Herkömmliche Gesetze sind zwar auf das Internet anwendbar (sogenannte *Medienneutralität des Rechts*), in der Regel aber für die besonderen Anforderungen nicht ausgelegt. So muss beispielsweise der Abschluss von Online-Verträgen (z.B. bei Webshops, Software-Download etc.) in Österreich nach dem *Allgemeinen Bürgerlichen Gesetzbuch* (*ABGB*)[371] aus dem Jahr 1811 beurteilt werden. Da das naturgemäß nicht immer friktionsfrei läuft, waren und sind rechtliche Anpassungen und Ergänzungen notwendig. Die Europäische Union hat den Regelungsbedarf erkannt und entsprechende Richtlinien erlassen. Vor allem die *E-Commerce-Richtlinie* (*E-Commerce-RL 2000/31/EG*[372]) und die *Fernabsatz-Richtlinie* (*Fernabsatz-RL 97/7/EG*[373]) haben spezielle Rücktrittsrechte (3 Monate) und Informationspflichten mit sich gebracht[374].

Das *Zivilrechts-Institut* der *Universität Innsbruck*[375] führt zum Thema „Internet und Recht" Folgendes aus[376]: „*Die grundsätzliche Anwendbarkeit des überkommenen Normensystems auch auf das Internet*

[367] http://www.phoenix.com/ [4. Feber 2007]
[368] Vgl. http://www.zdnet.de/security/news/0,39029460,39146842,00.htm [27. März 2007]
[369] Vgl. http://www.eff.org/ [4. Feber 2007] Aussagen vom Electronic Frontier Foundation-Institut, das sich mit den gesellschaftlichen Folgen von Trusted Computing auseinander setzt
[370] Vgl. http://www.bsi-fuer-buerger.de/recht/index.htm [6. Feber 2007]
[371] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: ABGB [7. Feber 2007]
[372] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 32000L0031 [7. Feber 2007]
[373] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 397L0007 [7. Feber 2007]
[374] Vgl. http://archiv.output.at/content/06-05/artikel/itlaw_29.htm [6. Feber 2007]
[375] http://www.uibk.ac.at/zivilrecht/ [7. Feber 2007]
[376] Vgl. http://www.uibk.ac.at/zivilrecht/buch/kap2_0.xml?section-view=true;section=4 [7. Feber 2007]

ist seit Langem gelebte Praxis. Jedoch wurde auf Grund der spezifischen Charakteristika des weltweiten Netzes (vor allem Ubiquität, Dezentralisation, Informationsflut) wiederholt sondergesetzlichen Regelungen das Wort geredet, was sich bereits in mehreren leges speciales niedergeschlagen hat. Grundsätzlich sollten aber trotz der rasenden Entwicklung der neuen Medien nicht die tragenden Grundorientierungen und -wertungen unserer Rechtsordnung, besonders des allgemeinen Zivilrechts, aus dem Blick verloren werden. Nicht eine weitere Zersplitterung der Rechtsordnung kann nämlich das Ziel sein; vielmehr ist danach zu streben, die Probleme des E-Commerce durch eine Fruchtbarmachung der Normen und Prinzipien des geltenden Rechts in den Griff zu bekommen. Nur dort, wo dies tatsächlich auf Grund einer signifikant unterschiedlichen Interessenskonstellation unumgänglich ist, soll das Normensystem bedacht weiterentwickelt, beziehungsweise ergänzt werden."

Die EU erlässt Richtlinien, welche in Österreich innerhalb einer bestimmten Frist in Gesetzen verankert werden müssen. Einige der wichtigsten werden in den Erläuterungen der Universität Innsbruck erwähnt: „*Diese Charakteristika stellen Rechtsanwender und Gesetzgeber vor schwierige Aufgaben: unter anderem im Internationalen Privatrecht*[377] *(IPR), im Haftungsrecht (E-Commerce-Gesetz*[378] *§§13, 14, 15, 16, 17, 18) beispielsweise bei den Providern (Dezentralisierung) oder auch im Konsumentenschutz (siehe Konsumentschutzgesetz*[379]*) im sogenannten B2C-Bereich (Menge, Geschwindigkeit, Flüchtigkeit und „Unkörperlichkeit" der digitalen Information), deren gegenwärtige Lösungsansätze Gegenstand dieser Ausführungen sind. Das Internet stellt eine Schnittmenge unterschiedlichster Rechtsgebiete dar; einen zentralen Schwerpunkt bildet aber das Zivilrecht. Hierbei zeichnen sich wiederum zwei Teilbereiche ab: Zum einen die Bestimmungen des ABGB im Hinblick auf das Vertrags- und Schadenersatzrecht, die grundsätzlich auch dann gelten, wenn Geschäftsbeziehungen via das Internet oder über das Handy (M-Commerce) abgewickelt werden. Zum andern die zahlreichen – oft auf EU-Richtlinien beruhenden – leges speciales im zivilrechtlichen Bereich, vor allem das E-Commerce-Gesetz (ECG), das Fernabsatz-Gesetz*[380]*, das Signaturgesetz*[381]*."*

[377] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: IPRG [7. Feber 2007]
[378] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: ECG [7. Feber 2007]
[379] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Konsumentenschutzgesetz [7. Feber 2007]
[380] http://www.ris.bka.gv.at/taweb-cgi/taweb?x=d&o=d&v=bgbl&d=BGBL&i=13345&p=3 [7. Feber 2007]
[381] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Signaturgesetz [7. Feber 2007]

Im Wesentlichen sind für Österreich folgende Rechtsbereiche – Online-Recht als Querschnittsmaterie – betroffen:

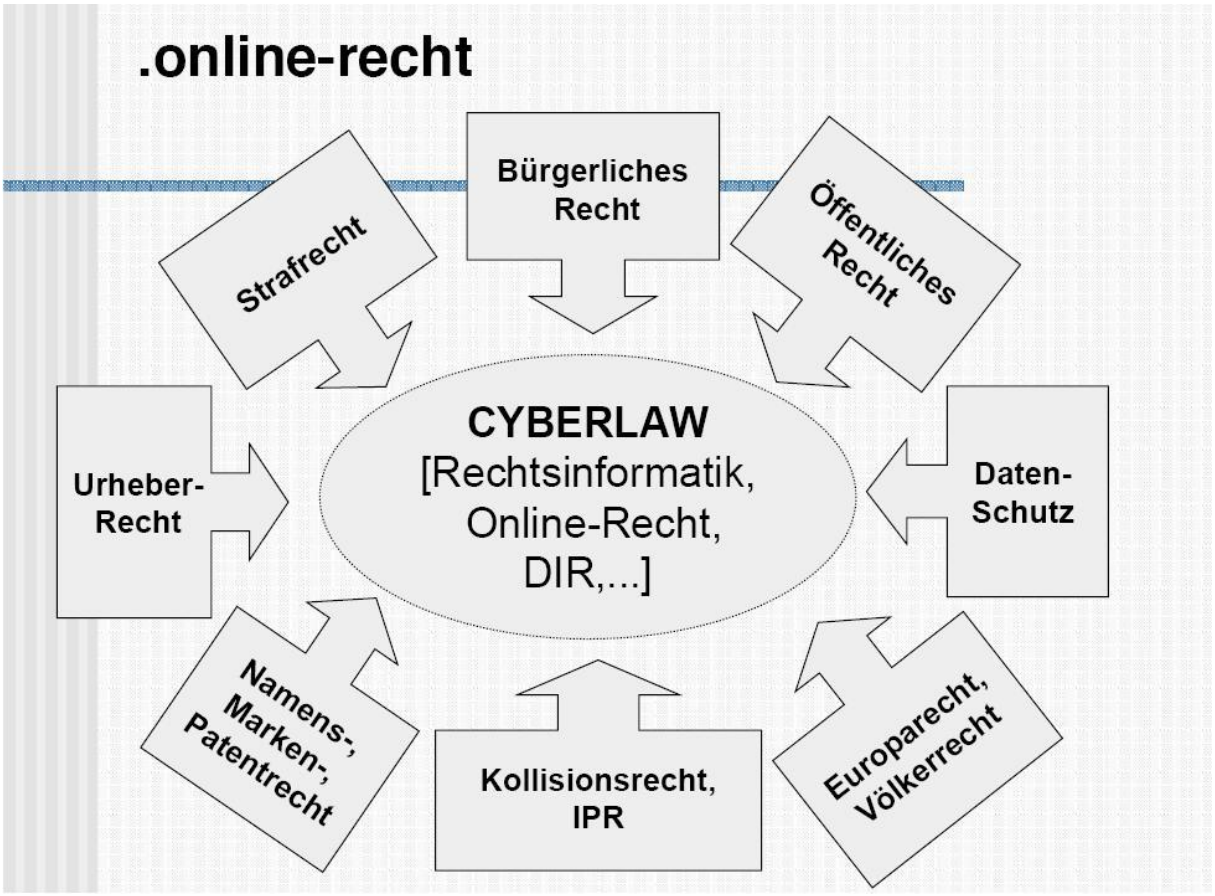


Abbildung 24: Online-Recht

1.7.3.1 Datenschutz

Das Recht auf Privatsphäre ist im *Artikel 8* des *Vertrages über die Europäische Union (*kurz: *EUV)* und im *Artikel 8 der Europäischen Menschenrechtskonvention (*kurz: *EMRK)*[382] verankert. In Österreich kommt zudem das *Staatsgrundgesetz* (kurz: *StGG*) zur Geltung.

Der rechtliche Rahmen für die Europäische Union wird durch die *Datenschutz-Richtlinie 95/46/EG*[383] vom 24. Oktober 1995 (Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr), die *Telekommunikations-Datenschutz-Richtlinie 97/66/EG*[384] vom 15. Dezember 1997 (Verarbeitung personenbezogener Daten und Schutz der Privatsphäre im Bereich der Telekommunikation) und der *E-Commerce-Datenschutz-RL 02/58/EG*[385] vom 12. Juli 2002 (Verarbeitung personenbezogener Daten und Schutz der Privatsphäre in der elektronischen Kommunikation) abgesteckt. Hinsichtlich Kommunikation mit Nicht-EU-Mitgliedstaaten muss

[382] http://ec.europa.eu/justice_home/fsj/privacy/law/treaty_en.htm [10. Feber 2007]
[383] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 31995L0046 [10. Feber 2007]
[384] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 31997L0066 [11. Feber 2007]
[385] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 32002L0058 [11. Feber 2007]

gewährleistet sein, dass personenbezogene Daten aus der europäischen „Datenschutzzone“ nur in jene Länder außerhalb der EU exportiert werden dürfen, welche einen ebensolchen Datenschutzstandard gewährleisten und wo das Grundrecht „angemessen“ geschützt ist[386]. Mit den USA ist dafür das *Safe-Harbor-Abkommen*[387] abgeschlossen worden.

In Österreich ist der Datenschutz Bundeskompetenz. Die Datenschutzrichtlinie der EU wurde im *Datenschutzgesetz 2000* (kurz: *DSG 2000*) umgesetzt. Das DSG 2000 enthält strengere Anforderungen als die vorgegebene EU-Richtlinie. Sonderbestimmungen zum Datenschutz sind beispielsweise im Telekommunikationsgesetz und Signaturgesetz enthalten.

Das DSG 2000 regelt nicht nur die Verwendung personenbezogener (gilt für natürliche und juristische Personen) Daten, die Auskunftsrechte Betroffener, die Zulässigkeit der Weitergabe von Daten und den Umgang mit Daten in Netzwerken, sondern enthält auch Bestimmungen zur Datensicherheit und zu Kontroll- und Rechtsschutzmaßnahmen und sieht Strafen bei der missbräuchlichen Verwendung von Daten vor. Unter personenbezogenen Daten werden Angaben über Betroffene verstanden, deren Identität bestimmt oder bestimmbar (Stichwort: Pseudonyme) ist. „Nur indirekt personenbezogen“' sind Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann[388].

Das Grundrecht auf Datenschutz ist im *§1 DSG 2000* festgehalten. Geschützt werden sollen – schutzwürdiges Interesse vorausgesetzt – personenbezogene Daten. Ein Schutzinteresse ist nicht vorhanden, wenn die Daten allgemein (öffentlich) verfügbar oder auf den Betroffenen nicht rückführbar sind. Ein staatlicher Eingriff ist lediglich im Rahmen der Grundrechtsschranken möglich. Er darf nur zur Wahrung wichtiger öffentlicher Interessen gemäß Art 8 (2) EMRK eingreifen.

Personenbezogene Daten dürfen grundsätzlich nicht verarbeitet (lt. *§4 DSG* 2000 im Sinne von jeder denkbaren Form der Erhebung, Nutzung, Verarbeitung, Aufbewahrung und Übermittlung von personenbezogenen Daten) werden, es sei denn, die Zulässigkeitsanforderungen werden erfüllt bzw. Erlaubnistatbestände treten ein [Proksch, 2006, S 18ff]:

- Der Zweck muss eindeutig festgelegt und rechtmäßig sein; eine spätere Zweckänderung ist unzulässig, die Daten müssen aktuell sein bzw. laufend aktualisiert werden. Nach Zweckerreichung ist die weitere Aufbewahrung der Daten grundsätzlich unzulässig (lt. *§6 DSG 2000*).

[386] Vgl. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm [11. Feber 2007]
[387] http://www.export.gov/safeharbor/ [11. Feber 2007]
[388] Vgl. http://www.internet4jurists.at/intern27a.htm [11. Feber 2007]

- Eine Datenverwendung ist überhaupt nur zulässig, wenn dadurch keine schutzwürdigen Interessen verletzt werden. Hierbei wird zwischen sensiblen und nicht-sensiblen Daten (lt. *§§8, 9 DSG 2000*) unterschieden. Nichtsensible Daten dürfen verwendet werden, wenn:
  - der Betroffene eingewilligt hat (der Widerruf einer solchen Einwilligung ist jedoch jederzeit möglich),
  - ein Gesetz dies ausdrücklich vorsieht,
  - Daten anonym sind,
  - lebenswichtige Interesse des Betroffenen dies erfordern,
  - überwiegendes Interesse eines Dritten (Privaten) vorliegt (Interessensabwägung zwischen schutzwürdigen Interessen des Betroffenen einerseits und jenen des Auftraggebers andererseits).

  Sensible, personenbezogene Daten sind Daten (ethnische Herkunft, politische Meinung, religiöse Zugehörigkeit, Gesundheit, Sexualleben, Gewerkschaftsstatus) natürlicher Personen mit besonders schutzwürdigem Interesse. Diese Daten dürfen nur verwendet werden, wenn:
  - sie der Betroffene selbst veröffentlicht oder seine ausdrückliche (jederzeit widerrufbare) Zustimmung erteilt hat,
  - eine gesetzliche Ermächtigung vorliegt oder
  - die Verwendung zur Wahrung überwiegend wichtiger, öffentlicher Interessen nötig ist.

Sowohl für den Auftraggeber (natürliche oder juristische Person, welche die Verwendung von Daten veranlasst bzw. zu verantworten hat) wie auch für den Betroffenen (natürliche oder juristische Person, deren Daten verwendet werden) gibt es Rechte und Pflichten.
Im Wesentlichen hat der Auftraggeber eine Informations-, Melde-, Auskunfts- und Richtigstellungspflicht, der Betroffene hingegen das Recht auf Beauskunftung, auf Richtigstellung und Löschung seiner Daten. Des Weiteren besitzt der Betroffene ein Beschwerde- bzw. Klagsrecht, ein Widerspruchsrecht wegen seines Geheimhaltungsinteresses und Anspruch auf Schadenersatz.
Der Unterschied zwischen Daten im privaten und öffentlichen Bereich liegt in der Geltendmachung: während bei einer Datenschutzverletzung durch Private Klage bei einem ordentlichen Gericht eingereicht werden kann, ist eine Verletzung durch eine öffentliche Institution bei der *Datenschutzkommission*[389] anhängig. Diese ist für die Kontrolle des Datenschutzes, unabhängig ob privat oder öffentlich, zuständig.
Der Datenschutz genießt in Österreich – wie auch in den meisten anderen Ländern – noch nicht jenen Stellenwert, den er innehaben sollte. Obwohl Österreich den Anspruch erhebt, eine strenge Datenschutz-Auslegung zu haben, ist der nicht-autorisierte Gebrauch von persönlichen Daten an der

[389] http://www.dsk.gv.at/ [11. Feber 2007]

Tagesordnung. Mit der durch das Internet ermöglichten und vereinfachten Datensammlung und -verknüpfung steigt die Notwendigkeit des Datenschutzes enorm.

1.7.3.2 Arbeitsrechtliche Grundlagen der Informationssicherheit in Unternehmen

Die folgenden Ausführungen gehören inhaltlich zum Kapitel Unternehmenssicherheit (siehe *1.8 Unternehmenssicherheit*), werden aber aufgrund des kontextuellen rechtlichen Zusammenhanges an dieser Stelle dargestellt.

Die Einführung und die steigende Nutzung der „neuen Medien" im Arbeitsprozess bringt eine zusätzliche brisante Komponente in die Datenschutzdiskussion. Mit der fortschreitenden Digitalisierung entsteht eine zunehmend bessere Kontrollmöglichkeit der Arbeitnehmer (siehe *2.3.4 Exkurs: Privacyaspekte für den betrieblichen User*).

Arbeitgeber und Arbeitnehmer sollten eine Regelung für die Nutzung der (digitalen) Betriebsmittel finden. Dabei sollte festgelegt werden, ob eine private Nutzung erlaubt ist, und wenn dies der Fall ist, in welchem Umfang. Die Intention hinter einer solchen Regelung [Tonninger, 2005, S 1] ist zum einen die Aufrechterhaltung der Systemfunktionalität und zum anderen die Verhinderung einer verminderten Arbeitsleistung des Arbeitnehmers durch Privatnutzung.

„*Grundsätzlich schuldet der Arbeitnehmer während der Arbeitszeit – außerhalb der Arbeitspausen – dem Arbeitgeber das uneingeschränkte Bemühen um den vereinbarten bzw. angemessenen Arbeitserfolg. Damit ist die Vornahme irgendeiner privat bedingten Nutzung grundsätzlich nicht zu vereinbaren. Dies muss klar auch für die private Nutzung des Internets gelten. Dies bedeutet, dass ein Verbot oder konkrete Vorgaben des Arbeitgebers bezüglich der privaten Verwendung grundsätzlich gilt. Der Arbeitnehmer hat sich dementsprechend zu verhalten bzw. diesbezügliche Weisungen zu befolgen."* [Posch, 2002, S 1]. Bei einem Verbot der privaten Nutzung ist es dem Arbeitsgeber erlaubt, (dienstliche) E-Mails seiner Mitarbeiter zu lesen sowie im Verdachtsfall eine personenbezogene Auswertung der E-Mails durchzuführen [Tonninger, 2005, S 5].

Üblicher als ein generelles Verbot ist, dass Arbeitnehmern erlaubt wird, „*das Internet als Informationsmedium insoweit zu nutzen, als es zumindest entfernt mit der beruflichen Tätigkeit zu tun hat, wobei auch der Konsum von üblichen Nachrichten in gewissem Umfang geduldet wird.*"[390]

Geregelt hingegen werden sollte, was explizit verboten ist (z. B.: Besuch von Webseiten zweifelhaften Inhalts, Download von Musik, Verschicken von privaten E-Mails an mehr als drei Empfänger etc.).

Gibt es jedoch keine Regelung in Form einer Betriebsvereinbarung ist der Umgang mit dem zulässigen Nutzungsumfang schwieriger zu handhaben. Hier kann lediglich auf den „Hausbrauch", auf den Umständen angemessenen Umfang verwiesen werden. Wenn es nur einen E-Mail-Account gibt, dürfen E-Mails vom Arbeitgeber nicht gelesen werden. Personenbezogene Auswertungen sind nur

[390] Vgl. http://www.internet4jurists.at/intern32a.htm [11. Feber 2007]

dann zulässig, wenn der Verdacht einer strafrechtlichen relevanten Handlung besteht [Tonninger, 2005, S 7].

1.7.3.2.1 Mitwirkung des Betriebsrates

Gemäss *§96 Abs 1 Z 3 Arbeitsverfassungsgesetz*[391] bedürfen Kontrollmaßnahmen und technische Systeme zur Kontrolle der Arbeitnehmer, sofern diese Systeme die Menschenwürde berühren, zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates. (Anm.: Die Rechte der Personalvertretung im öffentlichen Bereich sind zudem noch im jeweiligen *Personalvertretungsgesetz*[392] geregelt [Sommer, Vlastos, 2004].)

Derartige Maßnahmen haben in Form einer Betriebsvereinbarung zu erfolgen. „*Der Begriff Kontrollmaßnahme umfasst nicht nur die Zu- und Abgangskontrolle sowie die Kontrolle der Arbeitnehmer während des Aufenthalts im Betrieb, sondern schließt auch Kontrollen des dienstlichen Verhaltens außerhalb des Betriebs und Überwachung der Privatsphäre, aber auch Kontrollen zur Feststellung bestimmter Einstellungen und persönlicher Eigenschaften mit ein. Unter Kontrollmaßnahmen sind daher alle zur Überwachung von Arbeitnehmern geeigneten menschlichen Verhaltensweisen und technischen Vorrichtungen zu verstehen, wobei diese nur abstrakt dazu geeignet sein müssen, die Arbeitnehmer zu kontrollieren. Auf die tatsächliche Überwachung kommt es nicht an. Die bloß objektive Möglichkeit zur Kontrolle der Arbeitnehmer wirft mitunter große Probleme auf, ist doch beinahe jedes technische System dazu geeignet, Kontrolle auszuüben.“* [Posch, 2002, S 4]

Im Dezember 2006 entschied der *Oberste Gerichtshof* (kurz: *OGH*)[393] per Beschluss *9 ObA 109/06d*[394], dass ein Zeiterfassungssystem auf Basis eines biometrischen Fingerscans als Eingriff in die Menschenwürde zu bewerten ist. Die Menschenwürde ist somit im Sinne des §96 Abs 1 Z 3 ArbVG berührt und die Einführung eines Zeiterfassungssystems daher jedenfalls mitbestimmungspflichtig[395]. In einem Krankenhaus sollte das bisherige Zeiterfassungssystem durch ein biometrisches System ersetzt werden. Der Betriebsrat verlangte eine Betriebsvereinbarung, die jedoch von der Geschäftsführung abgelehnt wurde. Als Folge verlangte der Betriebsrat eine einstweilige Verfügung und hat vom OGH in allen Instanzen Recht bekommen.
Der OGH wertete den biometrischen Vorgang als einen zu starken Grundrechtseingriff für ein mit herkömmlichen Möglichkeiten (z. B.: Stechuhr) erreichbares Ziel.

Jede automationsunterstütze Verarbeitung personenbezogener Daten des Arbeitnehmers bedarf gemäß §96 Abs 1 Z 3 Arbeitsverfassungsgesetz grundsätzlich der Zustimmung des Betriebsrates.

---

[391] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Arbeitsverfassungsgesetz §19 [11. Feber 2007]
[392] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Personalvertretungsgesetz §19 [16. März 2007]
[393] http://www.ogh.gv.at/ [11. Feber 2007]
[394] http://www.ris.bka.gv.at/jus/ Suche nach: 109/06d [11. Feber 2007]
[395] Vgl. http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=09391war [11. Feber 2007]

1.7.3.2.2 Personalinformationssysteme

„*Grundsätzlich können Personalinformationssysteme als technische Systeme zur Kontrolle der Arbeitnehmer angesehen werden, da bereits die „Eignung" des Systems einen Arbeitnehmer zu kontrollieren für diese Qualifizierung ausreicht. Zur Abgrenzung muss daher das Kriterium des „Berührens der Menschenwürde" herangezogen werden, um zu beurteilen, ob ein elektronisches Personalinformationssystem unter §96 Abs 1 Z 3 ArbVG oder §96 Abs 1 Z 1 ArbVG subsumiert werden kann. Der Gesetzgeber hat damit eine Art „Sicherheitsnetz" für Arbeitnehmer schaffen wollen, indem er im §96 a Abs 3 ArbVG ausdrücklich normiert, dass durch die Abs 1 und 2 die sich aus §96 ergebenden Zustimmungsrechte nicht berührt werden. Fällt also eine Maßnahme nicht unter §96 ArbVG, kommt §96 a ArbVG zur Anwendung. Kann nicht festgestellt werden, unter welchen Paragraph die Maßnahme fällt, so hat der Betriebsinhaber, wenn der Betriebsrat die Zustimmung verweigert, eine Klärung im Rechtsweg herbeizuführen."* [Posch, 2002, S 6]

Führt ein Unternehmen Aufzeichnungen über nicht-personenbezogene Daten (z. B.: Durchschnittskrankenstände oder -urlaube), sind diese nicht zustimmungspflichtig. Wird allerdings eine Verknüpfung zu einem Arbeitnehmer hergestellt, kann diese Maßnahme zustimmungspflichtig werden, es sei denn, sie dient zur Erfüllung von gesetzlichen Anforderungen an den Arbeitgeber (z. B.: Zahlung von Krankenentgelt, Meldung an die Sozialversicherung etc.). Fachliche Voraussetzungen gehören nicht zu den personenbezogenen Daten im Sinne des §96 Abs. 1 Z 1 ArbVG und können demnach ohne Zustimmung des Betriebsrates erfasst werden. Der Arbeitgeber darf daher alle bisherigen beruflichen Tätigkeiten, Qualifikationen und Kenntnisse des Arbeitsnehmers registrieren, soweit eine Zweckmäßigkeit vorliegt.

Die Menschenwürde kann im Zusammenhang mit Daten der Internetnutzung dann berührt werden, wenn Logfiles nicht nur protokolliert, sondern auch aktiv gespeichert werden. Möchte daher ein Arbeitgeber das „Surf-Verhalten" seiner Mitarbeiter aufgrund gespeicherter Logfiles überprüfen, hat er wegen der damit verbundenen Berührung der Menschenwürde entweder eine Betriebs- oder eine Individualvereinbarung abzuschließen. Dasselbe hat für jene Fälle zu gelten, in denen eine entsprechende Filtersoftware nicht nur Zugriffe verhindert, sondern fehlgeschlagene Zugriffsversuche auch speichert [Brodil, 2004, S 166].

Der Betriebsrat hat nach dem Arbeitsverfassungsgesetz Informationsrechte im Zusammenhang mit Personalinformationssystemen. Hierbei geht es vor allem um das Einsichtsrecht: mit Zustimmung des Arbeitnehmers kann der Betriebsrat vom Unternehmenseigentümer die Information verlangen, welche personenbezogenen Daten des Betroffenen verspeichert und verarbeitet werden.

1.7.3.2.3 Haftung und Schadenersatz

Ob Naturkatastrophen, unzureichende Wartung, Viren oder Datenklau durch unredliche Mitarbeiter: Die Schäden und die damit verbundenen Haftungsrisiken, die in Unternehmen durch IT-Probleme

entstehen können, sind enorm. Die Haftung für solche Schäden trifft nicht nur die Unternehmen selbst, sondern kann auf die verantwortlichen Manager delegiert werden. Das Unternehmen haftet für Schaden gegenüber geschädigten Dritten (Kunden, Partner etc.), die verantwortlichen Manager, die entsprechende Sicherheitsmaßnahmen unterlassen haben, gegenüber dem Unternehmen[396]. In eine Verantwortung kommen die Mitarbeiter nur dann, wenn ihnen ein Verschulden an dem Schaden nachgewiesen werden kann. Dafür können schon Nachlässigkeiten oder Fehlentscheidungen ausreichen [Tonninger, 2005, S 17].

Exkurs: Schadenersatzrecht in Österreich[397]

Grundsätzlich trifft der Schaden nach *§1311 ABGB*[398] denjenigen, in dessen Vermögen oder Person er sich ereignet hat. Im Schadenersatzrecht gibt es zwei große Systeme: Verschuldenshaftung (Haftung für rechtswidrig und schuldhaft verursachte Schäden) und Gefährdungshaftung (Haftung aufgrund der spezifischen Gefährlichkeit einer Sache). Die Verschuldenshaftung kommt zur Anwendung, wenn ein Täter einen Schaden bei einem Dritten rechtswidrig und schuldhaft verursacht hat. Voraussetzung sind somit Schaden, Verursachung, Rechtswidrigkeit und Verschulden. Fehlt auch nur eine dieser Voraussetzungen, ist Schadenersatz ausgeschlossen. Hinsichtlich des Schadens wird zwischen dem Vermögensschaden (positiver Schaden und entgangener Gewinn) und dem ideellen oder immateriellen Schaden (z. B.: Schmerzensgeld etc.) unterschieden. Diese Unterscheidung ist bedeutsam, da ideelle Schäden nur in Ausnahmefällen ersetzt werden.

Weitere Voraussetzung des Schadenersatzes in der Verschuldenshaftung ist die Rechtswidrigkeit des Handelns. Hier gilt der Grundsatz, dass jemand, der sich im Rahmen des Erlaubten verhält, grundsätzlich keinen Schadenersatz leisten muss. Die Rechtswidrigkeit eines Verhaltens kann sich aus einem aktiven Tun oder einem Unterlassen ergeben.

Ein Schaden muss schließlich nur von dem Verursacher (*Kausalitätsprinzip*) ersetzt werden. Dies wird durch die *conditio sine qua non* (*Äquivalenztheorie*) geprüft, indem man fragt, ob der Schaden auch eingetreten wäre, wenn man das pflichtwidrige Verhalten wegdenkt. Die entscheidende Frage lautet also: Wäre der Schaden also auch eingetreten, wenn der Schädiger die konkrete Handlung nicht gesetzt hätte? Probleme können hier etwa im Falle des Vorhandenseins mehrerer Schädiger (kumulative Kausalität, alternative Kausalität, überholende Kausalität) bestehen. Der Schädiger soll nur für jene Schäden haften, die er adäquat verursacht hat.

Eine weitere Voraussetzung der Verschuldenshaftung ist die Voraussetzung der subjektiven Vorwerfbarkeit des rechtswidrigen Verhaltens. Schuldhaft handelt, wer ein Verhalten setzt, das er hätte vermeiden sollen und auch vermeiden hätte können. Hier wird zwischen mehreren

[396] Vgl. http://www.peterfmayer.at/wirtschaft/artikel_20096.html [25. Feber 2007]
[397] Vgl. http://www.rechtsfreund.at/schadenersatz.htm [25. Feber 2007]
[398] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: ABGB § 1311 [25. Feber 2007]

Verschuldensformen unterschieden: Vorsatz (Absichtlichkeit, Wissentlichkeit, bedingter Vorsatz), Fahrlässigkeit (leichte Fahrlässigkeit, grobe Fahrlässigkeit, entschuldbare Fehlleistung). Die Verschuldensform ist bedeutend für den Umfang der Ersatzpflicht.

Grundsätzlich gilt im Schadenersatz das Prinzip der Zurückversetzung in den vorherigen Stand (Naturalrestitution). Nur wenn dies nicht möglich ist, muss Geldersatz geleistet werden. Das Gesetz unterscheidet hinsichtlich des Ersatzumfanges zwischen der eigentlichen Schadloshaltung (positiver Schaden) und dem entgangenen Gewinn (volle Genugtuung). Bei leichter Fahrlässigkeit ist grundsätzlich nur der positive Schaden zu ersetzen. Bei grober Fahrlässigkeit bzw. Vorsatz ist volle Genugtuung zu leisten.

Schutz vor Haftung

Ein Arbeitnehmer kann seine persönliche Haftung nur vermeiden, indem er die übertragenen Aufgaben gewissenhaft wahrnimmt und ausführt. Geschützt werden kann er bei erwiesenermaßen leicht fahrlässigem Verhalten („leichter Fehler eines sonst sorgfältigen Menschen“) oder wenn er die Geschäftsführung auf Mängel in der Informationssicherheit zeitgerecht hingewiesen und diese nicht reagiert hat.

Leitende Mitarbeiter sind sich oft nicht bewusst, dass alleine die Tatsache einer möglichen Haftung Anlass zum Tätigwerden gibt. Die technische Absicherung der Infrastruktur reicht nicht, um rechtlich außer Obligo zu sein, vielmehr müssen zudem organisatorische Maßnahmen gesetzt werden. Dazu gehört etwa, dass den IT-Mitarbeitern das sich laufende Informieren über aktuelle Entwicklungen ermöglicht wird. Die Unternehmensleitung hat hierfür die finanziellen und infrastrukturellen Rahmenbedingungen bereitzustellen. Eine weitere Aufgabe ist es, mit Sicherheitsrichtlinien und Verhaltensregeln einhaltbare Vorgaben für die Mitarbeiter zu schaffen – im Zweifel haftet das Management[399].

Ein Delegieren an qualifizierte Arbeitnehmer schützt nicht, denn diese haften nur beschränkt, nämlich bei grober Fahrlässigkeit bzw. Vorsatz. Dies gilt vor allem für Aufgaben, die nur von einem Mitglied der Geschäftsführung kraft seiner Führungs-, Handlungs- und Ressortverantwortung entsprechend wahrgenommen werden können. Delegiert die Geschäftsführung solche Pflichten, haftet sie für eingetretene IT-Schäden – unabhängig vom Verschulden eines Mitarbeiters[400].

[399] Vgl. http://www.competence-site.de/wirtschaftsrecht.nsf/cc/WEBR-646GYQ!OpenDocument [25. Feber 2007]
[400] Vgl. http://www.monitor.co.at/index.cfm?storyid=7781 [25. Feber 2007]

Exkurs: Verbandsverantwortlichkeitsgesetz

Nach diesem seit 1. Jänner 2006 in Kraft getretenen Gesetz[401] können nun auch gegen Verbände – nicht mehr nur gegen natürliche Personen – Strafverfahren geführt werden. Als Verband anzusehen sind im Wesentlichen juristische Personen – etwa Kapitalgesellschaften (AG, GmbH) und Personengesellschaften (OHG, KG), aber auch Behörden in der Ausübung privatrechtlicher Tätigkeiten. Es geht um die Rechtsprechung bei Straftaten (bundes-/landesgesetzliches Strafrecht, nicht aber Verwaltungsstrafrecht), für die ein Verband verantwortlich ist, weil sie zu seinen Gunsten begangen oder Pflichten verletzt wurden, die den Verband treffen. „*Das Gesetz tendiert in Richtung einer Erfolgshaftung, bei der die Verwirklichung eines Straftatbestands allein und ohne Rücksicht auf individuelle Schuld zur rechtlichen Verantwortlichkeit genügen kann. Ist ein Verschulden einer individuellen Person nicht nachweisbar, griff das konventionelle Strafrecht bisher nicht. Nach dem neuen Gesetz genügt es nun, wenn irgendwer im Unternehmen die objektiv gebotene Sorgfalt außer Acht gelassen hat – das erleichtert dem Staatsanwalt das Handwerk. Dieser Irgendwer kann sowohl Entscheidungsträger wie Mitarbeiter sein. Das Unternehmen ist verantwortlich, wenn Erstere eine Straftat rechtswidrig und schuldhaft begangen haben, bei Mitarbeitern vom Lehrling aufwärts geht es moderater zu: Bei Fahrlässigkeitsdelikten muss die Straftat rechtswidrig und dabei die nach den Umständen objektiv gebotene Sorgfalt außer Acht geblieben sein.*“[402]

1.7.3.2.4 Umgang mit personenbezogenen Daten

Für den sorgsamen Umgang mit Daten von Mitarbeitern (bei Verdachtsmomenten) gibt es für die Personal- bzw. Organisations-/IT-Abteilung eine Hilfestellung, die sich im „Modell der stufenweisen Kontrollverdichtung“ [Kotschy, Reimer, 2004, S 169f] [Tonninger, 2005, S 3ff] ausdrückt.

- Stufe 1: Maschinelle Überwachung zur Gewährleistung der Systemfunktionalität
  - Funktionsfähigkeit des betrieblichen IT-Systems muss gewährleistet sein,
  - die dafür notwendige Datenermittlung ist auch in personenbezogener Form zulässig, sofern es unerlässlich oder unvermeidlich,
  - Grundsatz des gelindesten Mittels verlangt eine maschinelle Routineprüfung,
  - alle Maßnahmen zur Abwehr von Viren oder sonstigen Attacken Unbefugter,
  - Arbeitgeber als Eigentümer hat das Recht, maschinelle Routineprüfungen zur Funktionserhaltung des Systems durchzuführen.
- Stufe 2: Signifikante Abweichung von der normalen IT-Nutzung – Abweichungskontrolle
  - Information über die Abweichung kann bei Stufe 1 anfallen,
  - Recht des Arbeitgebers, die Ursache der Abweichung zu ermitteln,

[401] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Verbandsverantwortlichkeitsgesetz [12. Feber 2007]
[402] Vgl. http://www.gewerbeverein.at/modules.php?name=News&file=article&sid=698 [12. Feber 2007]

  - Treuepflicht des Arbeitnehmers erfordert, dass er Arbeitsmittel nicht zum erheblichen Nachteil des Arbeitgebers verwendet,
  - Nur kostenrelevante Abweichungen dürfen zum Anlass genommen werden,
  - Grenzwerte der Abweichung sollten definiert werden,
  - Ausreichende Information der Arbeitnehmer über die Kontrolle.
- Stufe 3: Zugriff auf Kommunikationsdaten bei Verdacht auf Rechtsverletzung
  - begründeter Verdacht einer Dienstpflichtsverletzung oder einer strafrechtlich relevanten Handhabung durch Gebrauch der betrieblichen IT-Ausstattung,
  - kein Monopol gerichtlicher Untersuchungsmaßnahmen im Arbeitsverhältnis,
  - Herbeiziehung von Mitgliedern des Betriebsrates oder Datenschutzbeauftragten zum Schutz des Arbeitnehmers.

Wesentlich dabei sind die Verhältnismäßigkeit und die Wahl des gelindesten Mittels. Ein Eingriff in den Inhalt einer Kommunikation ist schwerwiegender als die Kenntnis von Verkehrsdaten. Der Vorgesetzte des betroffenen Arbeitnehmers sollte erst involviert werden, wenn es keine befriedigende Erklärung für Unregelmäßigkeiten gibt. Über zufriedenstellend aufgeklärte Kontrollanlassfälle sollte Verschwiegenheitspflicht des Systemadministrators bestehen.

„Unter Aufrechterhaltung des grundsätzlichen Verfügungsrechts des Arbeitsgebers über die von ihm zur Verfügung gestellte IT-Ausstattung kann den berechtigten Schutzanliegen der Arbeitnehmer vor unverhältnismäßiger Überwachung durch stufenweise verdichtete Kontrolle gut entsprochen werden, wobei von diesem Schutz nicht nur private Kommunikation – die ohnehin ohne Inhaltsprüfung nicht verlässlich als solche erkannt werden kann – erfasst ist, sondern auch dienstliche Nachrichtenübermittlung. Unverhältnismäßigkeit und damit auch datenschutzwidrig ist jedenfalls eine Kontrolle, die dem Arbeitnehmer den Eindruck vermittelt, unausgesetzter Überwachung zu unterliegen, deren Ergebnisse laufend ausgewertet werden und in die Beurteilung seiner Arbeitsleistung mit entsprechenden Konsequenzen und Sanktionen einfließen.“ [Kotschy, Reimer, 2004, S 172]

1.8 UNTERNEHMENSSICHERHEIT

1.8.1 ZIELE UND AUFGABEN DES INFORMATIONSSICHERHEITSMANAGEMENTS

In den bisherigen Ausführungen (siehe *1.2 Grundlagen der Informationssicherheit*) wurde der Wert Information, relevante Bedrohungen und Schutzmechanismen erläutert. Die einzelnen Risiken und Gegenmaßnahmen sind abstrakt und isoliert voneinander betrachtet worden. Die Aufgabe des Informationssicherheitsmanagements für Unternehmen – als Teil des organisationsweiten Risikomanagements – ist es, in einem kontinuierlichen Prozess die Bedrohungspotenziale zu

identifizieren und zu analysieren, die Risiken zu klassifizieren, den Schutzbedarf festzustellen und entsprechenden Schutz prioritär und nach wirtschaftlichen Kriterien mit dem Ziel der Risikominimierung aufzubauen. Es sollen Informationen in allen Varianten angemessen geschützt und wirtschaftliche Schäden sowie Vertrauens- bzw. Imageschäden (z. B.: bei Behörden) verhindert werden. Mittels Informationssicherheitsmanagement wird die Informationsinfrastruktur (Ist-Zustand) analysiert und mit Sicherheitszielen (Soll-Zustand) verglichen, die Abweichungen werden in umzusetzenden Maßnahmen festgehalten. Hilfestellung und Orientierung für Soll-Ziele und das Erreichen dieser nach dem *best practice*-Prinzip bieten Richtlinien, Normen und Standards wie der deutsche *IT-Grundschutz*[403], das *Österreichische IT-Sicherheitshandbuch* [Österreichisches Sicherheitshandbuch, 2004], die *ÖNORM A 7799:2003*[404]*, A 17799:2003*[405], die *ISO 17799:2005*[406], die *ISO 27001:2005*[407] etc. Durch Gesetze (Aktiengesetz, GmbH-Recht, Bundesabgabenordnung etc.) und Regulative (SOX, Basel II) werden die Unternehmen – in Umfang und Intensität abhängig von den Parametern Börsennotierung, Gesellschaftsform, Größe etc. – gezwungen, Maßnahmen hinsichtlich interner Abläufe, interner Kontrollsysteme, Dokumentation, Nachweisbarkeit, Revisionssicherheit, Rechnungslegung und Finanzabschluss zu setzen. Ein *Informationssicherheitsmamagement-Prozess* (siehe *1.8.2.1.1 Informationssicherheitsmanagement-Prozess*) bzw. ein normiertes *Informationssicherheitsmanagement-System* (kurz: *ISMS*) (*1.8.2.1.2 Informationssicherheitsmanagement-System*) können hier ein wesentliches Werkzeug darstellen, um diese Ziele effizient zu erreichen.

Ist ein solches ISMS erfolgreich in einem Unternehmen etabliert, kann sich das langfristig durchaus wirtschaftlich positiv auswirken. Zudem ist eine Zertifizierung möglich, womit das Unternehmen nach außen hin einen gewissen Informationssicherheits-Standard aufweist. Dadurch wird das „Funktionieren" der wichtigsten Abläufe und Prozesse entsprechend der Forderungen der Normen nachgewiesen. Ein Zertifikat kann einerseits ein Wettbewerbsvorteil für das Unternehmen sein, andererseits ein Pflichtkriterium, um neue Geschäfte lukrieren zu können. So verlangt beispielsweise der deutsche Autohersteller *BMW*[408] von seinen Zulieferpartnern bis zum Jahr 2010 eine Zertifizierung nach ISO 27001:2005 (siehe *1.8.4.1.1 ISO 27001:2005 Information security management systems – Requirements*)[409].

---

[403] http://www.bsi.de/gshb/ [14. Feber 2007]
[404] https://www.on-norm.at/ecom/;jsessionid=AH4J1M10JH0I4CQCAICCFEQ?_requestid=1479862 [15. März 2007]
[405] https://www.on-norm.at/ecom/;jsessionid=AH4J1M10JH0I4CQCAICCFEQ?_requestid=1479862 [15. März 2007]
[406] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612 [14. Feber 2007]
[407] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40&ICS3= [14. Feber 2007]
[408] http://www.bmw.com/ [14. Feber 2007]
[409] Vgl. http://www.businessportal24.com/de/SupplyOn_Sicherheitsstandards_107447.html [14. Feber 2007]

Ferner wird durch Informationssicherheitsmanagement Folgendes ermöglicht[410]:

- Ermittlung der Leistungsfähigkeit der Sicherheitsprozesse,
- Aufdeckung genereller Sicherheitsschwachstellen innerhalb der Organisation,
- präventive Verhinderung von Schäden,
- Reduzierung von Risiken,
- Erfüllung der vom Kunden erwarteten Informationssicherheit (als IT-Dienstleister),
- Erhöhung der Verfügbarkeit der IT-Systeme,
- Reduzierung von Fehlern und Störungen und deren Kosten,
- Verbesserung des Ratings gegenüber den Banken durch Nachweis der Sicherheit.

Eines der Probleme im Sicherheitsmanagement besteht darin, dass mit der Entwicklung hin zu verteilten, offenen IT-Systemen die Qualifizierung der Sicherheitslage immer schwieriger und komplexer wird. Zugleich ist das Bewusstsein für die Informationssicherheitsrisiken noch immer unzureichend. Erst langsam erkennen die Unternehmen, dass technische Maßnahmen allein nicht mehr ausreichen. Ein umfassender Umgang mit Informationssicherheit betrifft als „Querschnittsthema" demnach alle Unternehmensbereiche, womit die Verantwortung nur bei der Unternehmensführung liegen kann. Im Sinne des *IT-Governance*[411] sollte daher bei Entscheidungen, welche die gesamte Organisation betreffen, die Informationssicherheit strategisch mit eingebunden sein.
Das Managementberatungshaus *A.T. Kearney*[412] hat in einer Studie[413] erhoben, dass 70 Prozent der Befragten der Meinung sind, dass erst durch entsprechende IT-Investitionen die Realisierung ihrer Unternehmensstrategien möglich ist, wobei nur ein Drittel der Unternehmen die eigene IT-Planung als klar an der Unternehmensstrategie ausgerichtet bezeichnet. Zudem fehlt bei Großunternehmen eine Strategie „aus einem Guss", weil Unternehmensteile auf unterschiedliche Sicherheitslösungs-Anbieter setzen und diese kaum aufeinander abgestimmt werden. Das resultiert aus dem Umstand, dass der strategische Ansatz fehlt.
„*Die Informationssicherheit wird von Menschen getragen, vom Management gemessen und über die Organisation der Prozesse gesteuert.*"[414]

[410] Vgl. http://www.tct.de/index.html?out=http://www.tct.de/managementsysteme/it/bs7799.html&menuunten= [16. Feber 2007]
[411] Unter IT-Governance wird die Steuerung und Kontrolle der Unternehmens-IT durch die Unternehmensführung zur Ausrichtung der IT-Prozesse auf die Unternehmensstrategie verstanden.
[412] http://www.atkearney.de/ [13. Feber 2007]
[413] Vgl. http://www.businessportal24.com/de/IT_Sicherheit_Unternehmen_Flickwerk_45401.html August 2006 [27. März 2007]
[414] Vgl. http://www.securitymanager.de/magazin/artikel_808_lebbare_und_gelebte_informationssicherheit.html [14. Feber 2007]

1.8.2 UMSETZUNG VON INFORMATIONSSICHERHEITSMANAGEMENT

Um Informationssicherheitsmangement in einem Unternehmen etablieren zu können, ist ein planvolles Vorgehen notwendig. Es gibt verschiedene Vorgehensmodelle, die ähnlich agieren und die Sicherstellung der unternehmensweiten Informationssicherheit zum Ziel haben.

1.8.2.1 Vorgehensmodelle

1.8.2.1.1 Informationssicherheitsmanagement-Prozess

Die Aktivitäten [Österreichisches Sicherheitshandbuch, 2004, S 22] im Rahmen des Informationssicherheitsmanagement-Prozesses stellen sich wie folgt dar:

- Entwicklung einer organisationsweiten Informationssicherheitspolitik,
- Durchführung einer Risikoanalyse,
- Erstellung eines Informationssicherheitskonzeptes,
- Umsetzung des Informationssicherheitsplanes,
- Gewährleistung der Informationssicherheit im laufenden Betrieb.

Beispielhaft die Darstellung aus dem österreichischem IT-Sicherheitshandbuch:

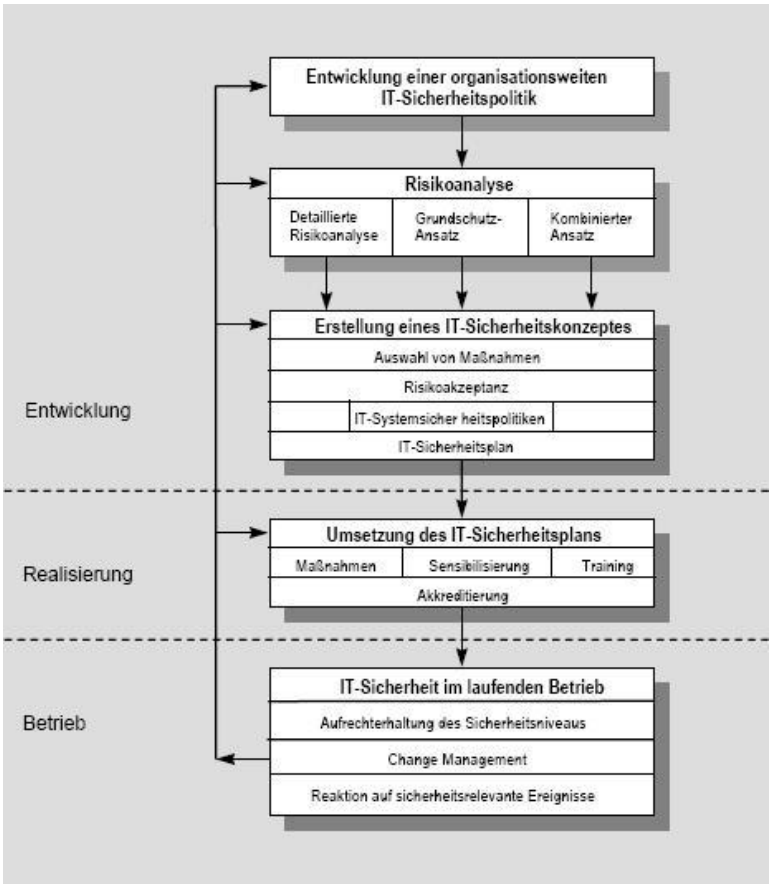


Abbildung 25: IT-Sicherheitsmanagement-Prozess

1.8.2.1.2 Informationssicherheitsmanagement-System

ISMS ist in der ISO-Norm 27001:2005 spezifiziert und standardisiert, damit zertifizierbar (siehe *1.8.4.1 Standardisierte Informationssicherheitsmanagement-Systeme*). Zur Darstellung wird mit dem *Deming-PDCA-Cycle-Modell*[415] Anleihe aus dem Qualitätsmanagement genommen.

Die wesentlichen Punkte im Rahmen des ISMS sind:

- Definition der Informationssicherheitspolitik,
- Bestimmung des Anwendungsbereichs des Managementsystems für Informationssicherheit,
- Durchführung einer angemessenen Risikoanalyse,
- Identifizierung der Risikobereiche,
- Auswahl der Sicherheitsziele und -maßnahmen,
- Dokumentation der Regelungen und Maßnahmen.

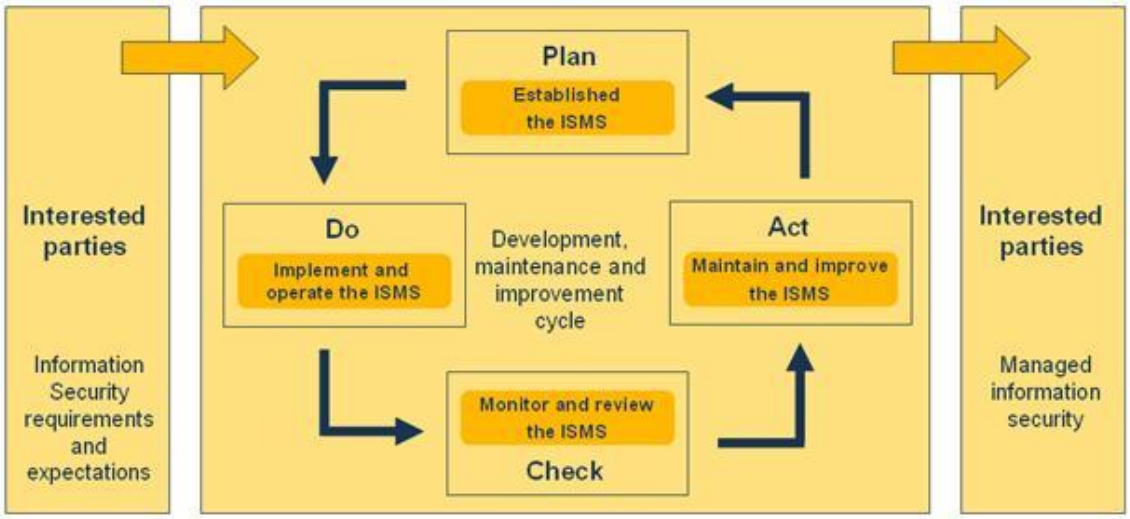


Abbildung 26: PDCA-Modell für ISMS

1.8.2.2 Entwicklung einer unternehmensweiten Informationssicherheitspolitik

Die Informationssicherheitspolitik [Österreichisches Sicherheitshandbuch, 2004, S 26] stellt die Basis für die Entwicklung und die Umsetzung eines risikogerechten und wirtschaftlich angemessenen Informationssicherheitmanagements dar. Dabei handelt es sich um ein langfristig ausgerichtetes Grundlagendokument, welches die sicherheitsbezogenen Ziele, Strategien, Verantwortlichkeiten und Methoden – unter Berücksichtigung der gegebenen Rahmenbedingungen – festlegt:

- Grundsätzliche Ziele und Strategien zur Informationssicherheit,
- Organisation, Verantwortlichkeiten und Pflichten,

[415] http://www.ifm.eng.cam.ac.uk/dstools/process/pdca.html [16. Feber 2007]

- Risikoanalysestrategien, Restrisiko und Risikoakzeptanz,
- Klassifizierung von Daten, IT-Infrastruktur, Business Continuity Planning,
- Maßnahmen zur Informationssicherheit,
- Aktivitäten zur Überprüfung und Aufrechterhaltung der Informationssicherheitspolitik.

Die Informationssicherheitspolitik soll allgemeine Festlegungen treffen, die für alle Einsatzbereiche der Informationstechnologie innerhalb einer Organisation zur Anwendung kommen.

1.8.2.3 Risikoanalyse

Eine wesentliche Voraussetzung [Österreichisches Sicherheitshandbuch, 2004, S 41f] für erfolgreiches Informationssicherheitsmanagement ist die richtige Einschätzung der Sicherheitsrisiken. In einer Risikoanalyse werden Risiken und Gefahrenpotenziale identifiziert und bewertet, um zu einer Abschätzung der Gesamtbedrohung zu kommen. Ziel ist es, dieses Gesamtrisiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizier- und akzeptierbar wird.
Wesentlicher Aspekt einer Risikoanalyse ist die systematische Erfassung versteckter Risiken[416]. Aufgrund der Komplexität von abteilungs- oder unternehmensübergreifenden Prozessen gilt es, diese Zusammenhänge hinsichtlich ihrer Gefahrenpotentiale zu erfassen und transparent darzustellen.
Für die Durchführung der Risikoanalyse werden in der Literatur viele Möglichkeiten aufgezeigt, einige Methoden [Österreichisches Sicherheitshandbuch, 2004, a.a.O.] werden im Folgenden kurz erläutert:

- Detaillierte Risikoanalyse: Beinhaltet für alle IT-Systeme die Identifikation der bestehenden Risiken sowie die Abschätzung ihrer Auftrittswahrscheinlichkeit. Diese Methode führt zu angemessenen Sicherheitsmaßnahmen, ist jedoch mit viel Zeit und Aufwand verbunden, so dass neben hohen Kosten auch die Gefahr besteht, dass für kritische Systeme nicht schnell genug Schutzmaßnahmen ergriffen werden können. Zur Reduktion des Aufwandes ist es daher in der Praxis üblich, für IT-Systeme mit niedrigem bis mittlerem Schutzbedarf auf eine detaillierte Risikoanalyse zu verzichten und mit Grundschutzmaßnahmen das Auslangen zu finden (siehe Kombinierter Ansatz).

[416] Vgl. http://www.bull.at/security/security-E.htm [17. Feber 2007]

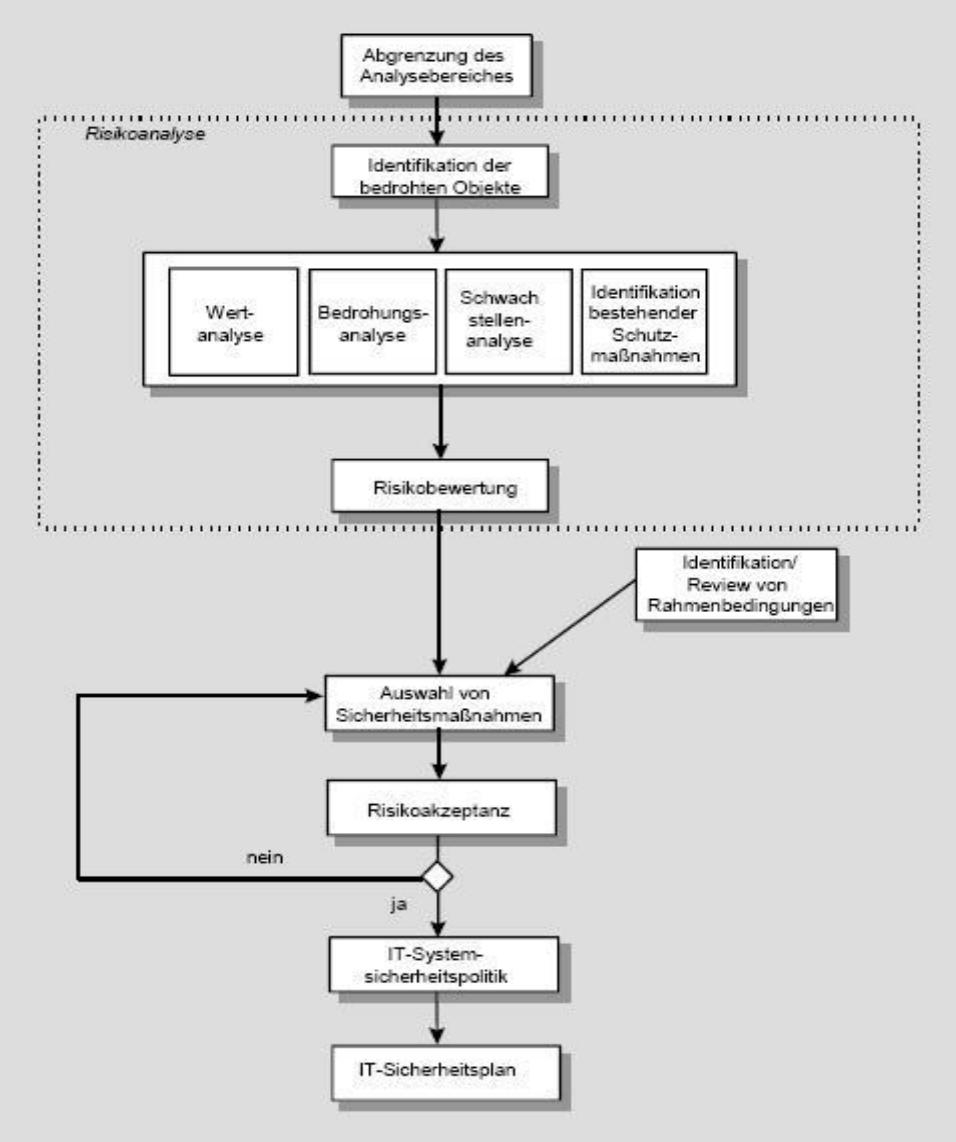


Abbildung 27: Detaillierte Risikoanalyse

- Grundschutzansatz: Unabhängig vom tatsächlichen Schutzbedarf werden alle IT-Systeme als gefährdet angesehen. Die empfohlene Vorgehensweise zur Grundschutzanalyse folgt im Wesentlichen den Vorgaben des IT-Grundschutzhandbuches des BSI (siehe *1.8.4.1.4 IT-Grundschutzhandbuch*). Bei dieser Methode wird auf eine Detaillierung verzichtet, deshalb ist sie ressourcenschonend und führt schnell zu einem relativ hohen Niveau an Sicherheit. Der Nachteil liegt darin, dass der angedachte Grundschutzlevel für das jeweilige IT-System möglicherweise nicht angemessen sein könnte.

  Eine Grundschutzanalyse besteht aus zwei Schritten:

  - Schritt 1: Nachbildung eines IT-Systems oder eines IT-Verbundes durch vorhandene Bausteine („Modellierung“),
  - Schritt 2: Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen.

- Kombinierter Ansatz: Hier werden die Stärken (ressourcensparende Grundschutzanalyse und wirksame Reduktion hoher Sicherheitsrisiken durch detaillierte Risikoanalyse) der beiden Analysemethoden genutzt. Zunächst wird ermittelt, welche IT-Systeme hohe bzw. niedrige bis mittlere Sicherheitsanforderungen haben. Werden IT-Systeme der Schutzbedarfskategorie „niedrig bis mittel“ einer Grundschutzanalyse unterzogen, bedarf es für IT-Systeme der Schutzbedarfskategorie „hoch bis sehr hoch“ einer detaillierten Risikoanalyse. Dies erlaubt einerseits eine schnelle Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus, andererseits können bedarfsgerechte, individuelle Maßnahmen angewendet werden.

Abbildung 28: Kombinierter Ansatz Risikoanalyse

Das Ergebnis einer Risikoanalyse[417] ist eine Aussage über Eintrittswahrscheinlichkeit und Schadenshöhe möglicher Risiken. Bei der Risikobewertung wird in strukturierter Form vorgegangen, um das Risiko selbst bzw. die das Risiko beeinflussenden Faktoren einzuordnen.

Ira Winkler[418] ergänzt zu dem Thema[419]: „*To manage risk, you must first define it. While there are many risk formulas, the one that I have found to be most effective is the following quasi-mathematical construction:*

*Risk = ((Threat * Vulnerability) / Countermeasure) * Value*

In this equation, value is the amount that your information and/or services are worth. Notice that I did not refer to the value of your IT, such as the hardware, software and support personnel. The fact is that hardware and software are fungible, and the cost of its replacement is trivial when compared to the value of the data on a computer. A backup tape, for example, might be costly, but it's worth millions if it's storing credit card numbers – when you consider the potential financial fraud, the cost

[417] Vgl. http://sicherheitskultur.at/Eisberg_risk.htm [17. Feber 2007]
[418] Ira Winkler ist Präsident der Internet Security Advisors Group und hat u.a. „Spies among us“ (Wiley, 2005) verfasst.
[419] Vgl. http://www.computerworld.com/securitytopics/security/story/0,10801,110643,00.html?source=NLT_VVR&nid=110643 [17. Feber 2007]

of reissuing the cards and the loss of business resulting from the loss of customer confidence." Anm.: Der Wert (engl. *Value*) der Daten läßt sich durch die Ausfallskosten ausdrücken. Bei der Berechnung der Ausfallskosten wird festgestellt, wie hoch der potenzielle Schaden (engl. *potential financial fraud*) im Falle eines Datenverlusts bzw. Systemausfalls wäre (siehe *Abbildung 30: Ermittlung der Ausfallskosten/Schadenshöhe*).

Weiters erfolgt eine Definition von Bedrohungen (engl. *Threat*) bzw. Schwachstellen/Verletzlichkeiten (engl. *Vulnerabilities*): „*Threat is the who or what that is out to get you – entities that can cause you harm if you provide them with the opportunity. Who refers to people or groups that can create loss? These might be malicious people, ranging from script kiddies to competitors to cyberterrorists. They can also be nonmalicious people, such as trusted insiders who make mistakes. What usually refers to events beyond your control, such as hurricanes, earthquakes, fires, floods and power outages.*

Vulnerabilities are weaknesses that allow threats to cause you harm. They can be operational (the way that you do business), personnel-related (the way that you hire, supervise and fire people), physical (the weaknesses in your physical assets) or technical (the way that you configure and maintain your computers). It is important to note that any vulnerability can be exploited by any threat."

Das Risikopotenzial kann durch Sicherheitsmaßnahmen nur bis zu einem gewissen Grad minimiert werden. In der Regel verbleibt ein Restrisiko. Es ist daher notwendig, dieses Restrisiko zu quantifizieren und durch die Unternehmensführung – in schriftlicher Form – akzeptieren zu lassen. Zu beachten ist jedoch, dass durch Kumulation oder gegenseitige Beeinflussung „kleine" Einzelrisiken zu einem inakzeptablen Restrisiko führen können.

Ira Winkler zum Thema Risikominimierung: „*If risk can't be eliminated, a practical security plan can reduce it to an acceptable level. Countermeasures are the only part of our formula that can be managed to reduce risk. They are security measures that aim to mitigate threats and/or vulnerabilities. Defining security programs in business terms, your security program is the implementation of countermeasures to mitigate your organization's vulnerabilities. The trick is for an information security manager to determine how to best allocate limited countermeasures to mitigate vulnerabilities and thus manage risk. The fact is that not all vulnerabilities should be mitigated. For example, it might cost millions of dollars to reduce a vulnerability that puts an asset of only small value at risk. To take an extreme example, you could assign a security guard to protect a tape 24 hours a day, but if the tape were blank, it would clearly be a waste of money.*"

Die Grafik stellt das Verhältnis von Schwachstellen und Gegenmaßnahmen dar: Je mehr Gegenmaßnahmen implementiert werden, desto weniger Schwachstellen können ausgenutzt werden. Der Bereich unter den Verletzlichkeiten repräsentiert den potenziellen finanziellen Schaden.

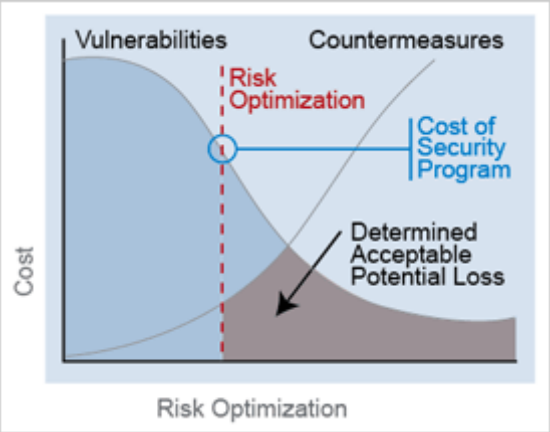


Abbildung 29: Risikooptimierung

Winkler verfeinert seine Überlegungen: „*Threats enter into this equation when they increase the probability that particular vulnerabilities will be exploited. If you understand the threats, you know what methods attackers are likely to use, what vulnerabilities they are likely to exploit and what type of value they want to compromise. As you increase countermeasures and decrease your potential loss, the cost of your countermeasures – that is, of your security program – increases. While most people assume you want to remove all vulnerabilities, the diagram shows that this is not practical. At some point, you'd spend more money implementing countermeasures than the remaining potential loss. Frankly, you never want to go past, or even come close to, the point where the cost of your countermeasures equals your potential loss. Potential loss is only potential loss, and it is unlikely it will ever be completely realized.*“

Eine Aufgabe der Informationssicherheitsverantwortlichen besteht darin, in einem Risikooptimierungsprozeß die Balance zwischen möglichen Finanzschäden und den Kosten eines Maßnahmenpakets zu finden (siehe *1.8.5 Kommerzieller Aspekt*).

Resümierend fasst Winkler zusammen: „*Optimizing risk doesn't mean that you are guaranteeing perfect security, but that you are consciously acknowledging the costs and benefits of your security program. Not only does it make your organization as secure as one can reasonably make it, it makes you more valuable as well.“*

1.8.2.4 Erstellung eines Informationssicherheitskonzepts

Auf Basis der Ergebnisse der Risikoanalyse wird ein sogenanntes Informationssicherheitskonzept erstellt. Dabei wird nach wirtschaftlichen Gesichtspunkten gereiht und es werden geeignete Gegenmaßnahmen ausgewählt, um die Risiken auf ein akzeptables Maß zu reduzieren.

Ein solches Sicherheitskonzept [Österreichisches Sicherheitshandbuch, 2004, S 62] enthält

- die Beschreibung des Ausgangszustandes einschließlich der bestehenden Risiken,
- die Festlegung der durchzuführenden Maßnahmen,

- die Begründung der Auswahl unter Kosten/Nutzen-Aspekten und hinsichtlich des Zusammenwirkens der einzelnen Maßnahmen,
- die Abschätzung des Restrisikos sowie eine verbindliche Aussage über die Akzeptanz des verbleibenden Restrisikos,
- die Festlegung der Verantwortlichkeiten für die Auswahl und Umsetzung der Maßnahmen sowie für die regelmäßige Überprüfung des Konzeptes,
- eine Prioritäten-, Termin- und Ressourcenplanung für die Umsetzung.

1.8.2.4.1 Auswahl von Maßnahmen

Sicherheitsmaßnahmen sind Mechanismen (Verfahren, Prozesse etc.), die das Ziel verfolgen, den Wert Information zu sichern. Durch Sicherheitsmechanismen wird es möglich, Risiken zu vermeiden, zu reduzieren bzw. überzuwälzen, unerlaubte Ereignisse zu entdecken, zu beschränken oder frühere Zustände wiederherzustellen.
Eine Klassifikation von Sicherheitsmaßnahmen kann nach verschiedenen Kriterien erfolgen: personell, organisatorisch, technisch, baulich, übergeordnet etc.
In der Regel stehen verschiedene Sicherheitsmaßnahmen zur Auswahl. Die Ermittlung der sichersten und zugleich wirtschaftlichsten Variante kann durch den Einsatz von Kosten-/Nutzen-Analyse-Werkzeugen bzw. im direkten Vergleich der einzelnen Maßnahmen erfolgen.
Die Auswirkungen der gewählten Maßnahmen zu analysieren ist ein wesentliches Element in der Maßnahmenbetrachtung. Damit soll deren Kompatibilität einerseits zum Gesamtsicherheitskonzept, andererseits zu den bereits installierten Maßnahmen sichergestellt werden. In diesem Stadium [Österreichisches Sicherheitshandbuch, 2004, S 66] wird die Einbeziehung der betroffenen Benutzer empfohlen, da die Wirksamkeit von Sicherheitsmaßnahmen stark davon abhängt, in welchem Maß diese akzeptiert werden. Zur Bewertung [Österreichisches Sicherheitshandbuch, 2004, a.a.O.] von Sicherheitsmaßnahmen ist wie folgt vorzugehen:

- Erfassung aller Bedrohungen, gegen die die ausgewählten Maßnahmen wirken,
- Beschreibung der Auswirkung der Einzelmaßnahmen,
- Beschreibung des Zusammenwirkens der ausgewählten und der bereits vorhandenen Sicherheitsmaßnahmen,
- Überprüfung, ob und inwieweit die Maßnahmen zu Behinderungen beim Betrieb des IT-Systems führen können,
- Überprüfung der Vereinbarkeit der Maßnahmen mit geltenden rechtlichen Vorschriften und Richtlinien,
- Bewertung, in welchem Ausmaß die Maßnahmen eine Reduktion der Risiken bewirken.

Es liegt im Verantwortungsbereich der Unternehmensführung, die Verhältnismäßigkeit der Kosten für die Umsetzung der Maßnahmen im Vergleich zur Verminderung des Risikopotenzials zu bewerten.
Die Umsetzung der Maßnahmen erfolgt im Rahmen des IT-Sicherheitsplanes (siehe *1.8.2.4.3 IT-Sicherheitsplan*).

1.8.2.4.2 IT-Systemsicherheitspolitik

Unter IT-Systemsicherheitspolitik (engl. *Policy*) – nicht zu verwechseln mit Informationssicherheitspolitik (siehe *1.8.2.2 Entwicklung einer unternehmensweiten Informationssicherheitspolitik*) – werden Dokumente verstanden, in denen grundlegende Vorgaben und Richtlinien zur Sicherheit von IT-Systemen definiert werden. Weiters beinhalten sie Details über die ausgewählten Sicherheitsmaßnahmen. Diese Policies sind jedoch nicht unveränderlich, sondern sollen regelmäßig überprüft und gegebenenfalls adaptiert werden. Abgeleitet werden die Policies von der unternehmensweiten Informationssicherheitspolitik. Bei der Erstellung ist auf bestehende Regelungen Rücksicht zu nehmen.
Eine Policy sollte enthalten [Österreichisches Sicherheitshandbuch, 2004, S 69]:

- Definition und Abgrenzung des Systems, Beschreibung der wichtigsten Komponenten,
- Definition der wichtigsten Ziele und Funktionalitäten des Systems,
- Festlegung der IT-Sicherheitsziele des Systems,
- Abhängigkeit der Organisation vom betrachteten IT-System: dabei ist zu untersuchen, wie weit die Aufgabenerfüllung der Organisation durch eine Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität des Systems bzw. von darauf verarbeiteter Information gefährdet wird,
- Investitionen in das System (Entwicklungs-, Beschaffungs- und Wartungskosten, Kosten für den laufenden Betrieb),
- Risikoanalysestrategie,
- Werte, Bedrohungen und Schwachstellen laut Risikoanalyse,
- Sicherheitsrisiken,
- Beschreibung der bestehenden und der noch zu realisierenden Sicherheitsmaßnahmen,
- Gründe für die Auswahl der Maßnahmen,
- Kostenschätzungen für die Realisierung und den laufenden Betrieb (Wartung) der Sicherheitsmaßnahmen,
- Verantwortlichkeiten.

Policies sollten für alle wesentlichen IT-Infrastruktursysteme erarbeitet werden: Internet-Policy, Netzwerk-Policy, PC-Policy etc.

1.8.2.4.3 IT-Sicherheitsplan

Hier wird beschrieben, wie die ausgewählten Sicherheitsmaßnahmen umgesetzt werden (siehe *1.8.2.4.1 Auswahl von Maßnahmen*). Die Planung umfasst das Setzen von Prioritäten, das Management von Ressourcen und einen Zeitplan. Für jedes System sollte Folgendes erstellt werden [Österreichisches Sicherheitshandbuch, 2004, S 70]:

- eine Liste der vorhandenen sowie der noch zu implementierenden Sicherheitsmaßnahmen (für jede dieser Maßnahmen sollte eine Aussage über ihre Wirksamkeit sowie möglicherweise notwendige Verbesserungen oder Verstärkungen getroffen werden),
- eine Prioritätenreihung für die Implementierung der ausgewählten Sicherheitsmaßnahmen bzw. die Verbesserung bestehender Maßnahmen,
- eine Kosten- und Aufwandsschätzung für Implementierung und Wartung der Maßnahmen,
- Detailplanung für die Implementierung (Prioritäten, Zeitplan, Budget, Verantwortlichkeiten, Schulungs- und Sensibilisierungsmaßnahmen, Test- und Abnahmeverfahren und Abnahmetermine, Nachfolgeaktivitäten),
- eine Bewertung des nach der Implementierung aller Maßnahmen zu erwartenden Restrisikos.

Weiters sollte der Sicherheitsplan zum einen Kontrollmechanismen festlegen, die den Fortschritt der Maßnahmen-Implementierung bewerten, und zum anderen Adaptierungsmöglichkeiten bei Abweichungen vom vorgesehenen Prozess definieren.

1.8.2.5 Umsetzung des IT-Sicherheitsplans

Bei der Umsetzung des Planes ist zu beachten [Österreichisches Sicherheitshandbuch, 2004, S 72], dass

- Verantwortlichkeiten rechtzeitig und eindeutig festgelegt werden,
- finanzielle und personelle Ressourcen rechtzeitig zugewiesen werden,
- die Maßnahmen korrekt umgesetzt werden,
- die Kosten sich in dem vorher abgeschätzten Rahmen halten,
- der Zeitplan eingehalten wird.

Um bei den Mitarbeitern eine entsprechende Akzeptanz der umzusetzenden Maßnahmen zu erreichen, gilt es, Schulungs- und Sensibilisierungsaktivitäten durchzuführen. Zudem sollen die Auswirkungen der gesetzten Maßnahmen überprüft werden.

1.8.2.5.1 Implementierung von Maßnahmen

Die zu implementierenden Maßnahmen sind auf Übereinstimmung mit der Sicherheitspolitik zu prüfen, zudem auf Korrektheit und Vollständigkeit zu kontrollieren. Bei der Umsetzung sollen die systemübergreifenden, unternehmensweiten Maßnahmen angemessen und nicht redundant sein, die systemspezifischen hingegen kompatibel zu der existierenden Umgebung. Besonderes Augenmerk ist auf eine detaillierte und aktuelle Dokumentation der Implementierungen zu legen.

1.8.2.5.2 Sensibilisierung und Schulung

Nur durch Verständnis bei den Mitarbeitern (siehe *1.7.1.1 Organisation/Personal*) ist eine Umsetzung und Einhaltung der Richtlinien und Vorschriften zu erreichen. Um das Sicherheitsbewusstsein aller Mitarbeiter zu wecken bzw. zu fördern, ist ein organisationsweites Sensibilisierungsprogramm erforderlich. Eine detailliertere Erläuterung zu Elementen der Sensibilisierung ist im Zuge der Ausführungen über die Unternehmenskultur zu finden (siehe *1.8.3.1.2 Exkurs: Unternehmenskultur*).
Umsetzungsbestandteil eines Sensibilisierungsprogramms sind Schulungen in den Bereichen der Informationssicherheit. Schulungsprogramme sind für jede Organisation spezifisch zu entwickeln.
Folgende Beispiele [Österreichisches Sicherheitshandbuch, 2004, S 76] sollen die im Rahmen von Schulungs- und Trainingsveranstaltungen zu behandelnden Themen zeigen:

- Sicherheitspolitik und -infrastruktur: Rollen und Verantwortlichkeiten, Organisation des IT-Sicherheitsmanagements, Behandlung von sicherheitsrelevanten Vorfällen, regelmäßige Überprüfung von Sicherheitsmaßnahmen etc.,
- Bauliche Sicherheit: Schutz von Gebäuden, Serverräumen, Büroräumen und Versorgungseinrichtungen mit besonderer Betonung der Verantwortung der einzelnen Mitarbeiter
- Personelle Sicherheit,
- Hardware- und Softwaresicherheit: Identifikation und Authentifikation, Berechtigungssysteme, Protokollierung, Wiederaufbereitung, Virenschutz etc.,
- Netzwerksicherheit: Netzwerkinfrastruktur, LANs, Inter-/Intranets, Verschlüsselung, digitale Signaturen etc.,
- Business Continuity Planning.

Sensibilisierungs- und Schulungsmaßnahmen müssen entsprechend geplant und umgesetzt werden, um Sicherheitslücken durch fehlendes Wissen oder mangelndes Sicherheitsbewusstsein zu vermeiden.

1.8.2.6 Management von Informationssicherheit

Umfassendes, holistisches Informationssicherheitsmanagement hat zur Aufgabe, alle Komponenten (wie oben beschrieben) kontinuierlich bzw. zyklisch auf seine Aktualität, Umsetzung und Wirksamkeit hin zu prüfen. Das Ziel aller Aktivitäten ist, das erreichte Sicherheitsniveau zu erhalten,

respektive zu erhöhen. Das lässt sich nur durch fortlaufende Wartung und ständiges Monitoring der Sicherheitsinfrastruktur bzw. durch die regelmäßige Überprüfung der Maßnahmen auf ihre Übereinstimmung mit dem Sicherheitskonzept erreichen. Ein Sicherheitsreport (Feber 2007) der *Nationalen Initiative für Internetsicherheit* (kurz: *NIFIS*)[420] berichtet, dass viele Sicherheitsprobleme nach wie vor entstehen, weil Firmen die Pflege und Wartung ihrer IT-Systeme vernachlässigen. Laut diesem Report sehen 86 Prozent der in Unternehmen für Informationssicherheit zuständigen Fachleute demnach in der Systembetreuung Defizite.
Neue Sicherheitsanforderungen, Änderungen oder sicherheitsrelevante Ereignisse sollen erkannt und durch entsprechende Gegenmaßnahmen behoben werden.

1.8.3 DER FAKTOR MENSCH

In Teilen (siehe *1.3.3 Menschliches Versagen* und *1.7.1.1 Organisation/Personal*) der bisherigen Ausführung wurde bereits dezidiert auf die enorme Wichtigkeit des Menschen hinsichtlich Sicherheit eingegangen bzw. aufmerksam gemacht. Im Unternehmen kommt dem Mitarbeiter eine nicht minder bedeutende Rolle zu. Die Kombination von technischen Werkzeugen, Befolgen von Grundregeln und Einsatz des „gesunden Menschenverstandes“ stellt eine gute Basis für den Schutz vor informationssicherheitstechnischen Gefahren dar. Der Anwender bestimmt den erzielbaren Grad an Sicherheit[421].

1.8.3.1.1 Unsicherheitsfaktor Mitarbeiter

Die Sicherheitstechnik hat sich enorm weiterentwickelt, für vieles gibt es bereits Lösungen, einiges steht *ante portas* (z. B.: Biometrie). Nicht selten gehen Sicherheitskonzepte davon aus, dass sich Menschen ebenso rational verhalten wie Systeme. Der Wunsch eines jeden für Unternehmenssicherheit verantwortlichen Mitarbeiters ist ein möglichst sicheres Unternehmen.
„*Seit die Informationstechnologie Einzug in die Unternehmen gehalten und die Entwicklung von Security-Routinen ihre Handhabung zum Tagesgeschäft erkoren hat, gelten Irrtum und Nachlässigkeit der eigenen Mitarbeiter als die primären Gefahrenquellen im System. Die Ursachen dieser „Fehlleistungen“ blieben bis dato jedoch unerforscht. Was also sind die „geheimen“ Faktoren, die vermeintlich sicheren IT-Systeme immer wieder auszuhebeln drohen?“* Auf Basis von morphologischer[422] Marktforschung befragte ein Psychologen-Team (Sommer 2006) in Tiefeninterviews Angestellte nach ihren Gewohnheiten und Wünschen im Umgang mit ihrer IT-gestützten Arbeit und nach ihren Vorstellungen von IT-Security und Unternehmenskultur. Das

[420] http://www.nifis.de/ [23. Feber 2007]
[421] Vgl. http://www.solnet.ch/sicherheit/mensch.html [23. Feber 2007]
[422] Die Morphologische Marktforschung versucht mit Hilfe psychologischer Beschreibungen und Analysen die geheime Logik und die Funktionsprinzipien transparent zu machen, die zu Marktgestaltungen und Marktentwicklungen führen.

Ergebnis wurde unter dem Titel „*Entsicherung am Arbeitsplatz. Die geheime Logik der IT-Security in Unternehmen*" [known_sense, 2006] von der deutschen Agentur *known_sense*[423] publiziert.

„*Unternehmen, die immer weniger rein und auch immer weniger raus lassen, minimieren ihre Entwicklungschancen und die ihrer Mitarbeiter. Durch technologische Innovationen zunehmend sachlich geprägte Arbeit, die immer weniger Eigenes, immer weniger Menschliches zulässt, erscheint leblos und fad.*"

Ein weiterer interessanter Aspekt wird herausgearbeitet: „*IT-Security beeinflusst die Unternehmenskultur in entscheidendem Maß. Wird ihre Schutzfunktion auch als positiv und notwendig erachtet, so verkehrt sich dieser Schutz nicht selten in ein Zwangssystem, das Identität und individuelle Gestaltungswünsche der Mitarbeiter ausschließt: „Auf der Arbeit habe ich nichts Persönliches auf dem PC, weil ich davon ausgehe, dass die EDV mich durchleuchten kann", sagt ein Teilnehmer der Studie.*

Der Umgang mit IT-Security und ihr unmittelbares Erleben werden zu einer Frage des Vertrauens in das Unternehmen und sind so untrennbar mit dessen Selbstverständnis verbunden. Nur wenige Unternehmenskulturen erlauben Raum für Eigenes; Arbeit, insbesondere Computerarbeit, versachlicht sich – speziell durch den geforderten Umgang mit IT-Security. Entsicherndes Handeln – „Ich mache schon mal Sachen auf, z. B.: 13 Sprüche für die Seele – mit Bildern. Einfach, damit es einem gut geht" – wird zum unbewussten Befreiungsschlag gegen die Unternehmenskultur im allgemeinen und die IT-Security im Besonderen. Je weniger Raum für Eigenes vorhanden ist, umso mehr besteht die Gefahr einer Verkehrung und damit des unkontrollierten Ausbruchs entsichernder Handlungen."

Weiters wird präzisiert: „*Die Seele greift tief in ihre eigene Trickkiste und umdribbelt mit brasilianischer Leichtigkeit alles Rationale. Dabei verkehrt sich das im Rahmen der Untersuchung entdeckte Phänomen des Sachlichen Verschließens (Schutz vor Ein- und Ausbrechern) in Ausbrüche, die dem Prinzip des Menschlichen Eröffnens folgen: Bei Mitarbeitern, die die zunehmende Entmenschlichung von Arbeit nicht länger aushalten, kommt es unbewusst zu bekannten Fehlleistungen, bei dem sich die Mitarbeiter nicht nur sich selbst, sondern auch ihr Unternehmen regelrecht entsichern. Und doch: Die Entsicherung am Arbeitsplatz stellt im Grunde etwas „Gutes" dar, dient sie doch der Versicherung der eigenen Identität. Die Mitarbeiter begehen mithin „Fehler", um durch das hiermit verbundene Menschliche Eröffnen ein wenig Menschliches in ihre Arbeit zu retten und damit ihre persönliche Produktivität zu sichern. Mitarbeiter und Unternehmen können an dieser Stelle in dem Wissen um die eigentlichen Ursachen aber auch Verbündete im Dienst der eigenen Sache werden und so Zuverlässigkeit und Sicherheit des IT-Betriebes nachhaltig stärken."*

[423] http://www.known-sense.de/ [5. Mai 2007]

Um dieses Ziel zu erreichen, empfiehlt die Studie den Unternehmen: „*sich zu immunisieren, indem sie das Menschliche eröffnen, die emotionalen und zum Teil schrägen Seiten der Mitarbeiter akzeptieren und sogar fördern. Die Unternehmenskultur muss Ausbrüche zulassen und versuchen, diese so gut wie möglich zu steuern. Gute und lebendige Awareness-Kampagnen, die eher im Unbewussten wirken, werden in diesem Zusammenhang wichtiger als offene Drohungen oder endlos wirkende IT-Schulungen. Entscheidend ist also der Impfstoff, den sich das Unternehmen mixt. Mit ausgewogenen Mitteln wird es das eigene Immunsystem stärken und damit im wahrsten Sinne des Wortes virenfrei bleiben – ohne die Substanz, die Mitarbeiter, nachhaltig zu schwächen. IT-Security muss sich mit Menschlichem aufladen und Identifikationsinhalte schaffen, um allzu sachlich geratene Awareness-Kampagnen zu optimieren. IT-Security braucht eine Story. Braucht Protagonisten. Muss für sich werben. Die Mitarbeiter sind bereit zu kämpfen. Man muss sie aber auch lassen. Denn dann klappt es auch mit der „Defense“. Dann wird IT-Security nicht nur Teil der Unternehmenskultur sein, sondern diese sogar entscheidend prägen.*“

1.8.3.1.2 Exkurs: Unternehmenskultur

Die Unternehmenskultur gilt seit einiger Zeit als der entscheidende Faktor für den Erfolg eines Unternehmens [Wojda, 2005, Inhalt der Organisationsgestaltung, S 33]. Ausgangspunkt der Überlegungen ist, dass für Erwartungen, Handlungen und Verhaltensweisen in Unternehmen „gelebte Wertesysteme“ maßgebend sind. Jedes Unternehmen entwickelt aufgrund dieser Wertvorstellungen eine eigene Kultur, die als spezifisches Muster gemeinsamer Wahrnehmungen und Überzeugungen auf neue Mitarbeiter übergeht. Unternehmenskultur kann als eine Art „gemeinsam akzeptierte Realitätsinterpretation“ gesehen werden, die sich im Laufe der Zeit herausbildet und die Handlungs- und Denkmuster der Unternehmensangehörigen und somit auch das Unternehmensgeschehen nachhaltig, aber unsichtbar beeinflusst. Inhaltlich bestimmt die Unternehmenskultur, was in einem Unternehmen Stellenwert hat, was als positiv oder negativ zu bewerten ist, wie über die eigene Vergangenheit, Gegenwart und Zukunft, wie über die Umwelt gedacht und was voneinander gehalten wird [Wojda, 2005, a.a.O.].

Die Unternehmenskultur hat enormen Einfluss auf die Effizienz eines Unternehmens. Eine starke und funktionale Unternehmenskultur trägt koordinations-, integrations- und motivationsfördernde Potenziale in sich [Wojda, 2005, Inhalt der Organisationsgestaltung, S 38]:

- größere Bindung zu den definierten Organisationszielen,
- ein gewissenhaftes Arbeiten der Mitarbeiter,
- Steigerung der durchschnittlichen Firmenzugehörigkeit,
- eine schnellere Ausführung von Plänen, Projekten und Programmen,
- eine effizientere Problemlösung auf allen Organisationsebenen,

- die Fähigkeit, schneller zu wachsen durch mehr Bemühen beim Erstellen von Plänen, Programmen und Zielen, als auch weniger Zeitaufwand für Intrigenspiele, dauernde Konflikte etc.

Bei einer ideal ausgeprägten Unternehmenskultur werden ferner:

- die Werte und Normen der Mitarbeiter in positiver Weise beeinflusst,
- die informelle Organisation unterstützt,
- das Zusammengehörigkeitsgefühl der Unternehmensmitglieder gestärkt,
- die Motivation gesteigert,
- das Betriebsklima und der Leistungswille positiv beeinflusst,
- neuen Mitarbeitern die Aufnahme und der Anschluss erleichtert,
- die Entscheidungsfindung unterstützt,
- ein besseres Betriebsklima erzielt.

Eine ungünstig ausgeprägte Unternehmenskultur hingegen hat einen negativen Einfluss auf die Effizienz des betrieblichen Leistungsprozesses. So kann die Unternehmenskultur zu einem „depressiven" Betriebsklima führen, wodurch die Motivation und der Leistungswille naturgemäß stark sinken. Weiters können durch traditionelle Anschauungen notwendige Veränderungen und Weiterentwicklungen behindert oder sogar unterdrückt werden [Wojda, 2005, Inhalt der Organisationsgestaltung, S 38].

Eine gezielte Veränderung der gewachsenen Unternehmenskultur ist daher vielfach ein Anliegen der Unternehmensführung. Bewusste, zielorientierte Kulturbeeinflussung ist ein oft notwendiger, aber gleichzeitig riskanter Schritt. Ansatzpunkt für eine partielle, nicht im Detail beherrschbare Änderung des Wertesystems bietet die bewusste Schaffung von Rahmenbedingungen für die soziale Evolution. Grundsätzlich gibt es zwei Vorgehensweisen: zum einen eine langfristig angelegte Kulturevolution, zum anderen eine kurzfristig durchführbare Kulturrevolution. Während bei der Kulturrevolution das einzig wirksame Mittel der Austausch von Personen ist, wobei der Wechsel der Führungsmannschaft bzw. *informeller Führer* am wirksamsten scheint, geht es bei der Evolution um die Schaffung von Rahmenbedingungen, die die Entwicklung der Unternehmenskultur in eine ganz bestimmte Richtung lenken: Personalselektion (Vorbilder etc.), Symbolisches Management (Führung lebt Werte und Einstellungen vor), Anreiz- und Belohnungssystem, Aus- und Weiterbildung, Rituale, geeignete Gestaltung der Unternehmensorganisation und Auswahl entsprechender Symbole, die Werte und Normen der anzustrebenden Kultur zum Ausdruck bringen.

Die Unternehmenskultur hat demnach massiven Einfluss auf die strategischen Entscheidungsprozesse in einer Organisation. Da jede Veränderung in einem Unternehmen, sei es in der Organisationsstruktur, im Führungsverhalten, in der verwendeten Technologie oder in anderen Bereichen, immer etwas Neues mit sich bringt, ist eine solche Veränderung immer auch mit einem Lernprozess für viele oder sogar für alle Mitarbeiter verbunden. Um hier eine übermäßige Frustration

und mögliche Reibungsverluste zu verhindern, besteht die Notwendigkeit, die davon betroffenen Mitarbeiter frühzeitig in die Entwicklung mit einzubeziehen und sie auch von der Notwendigkeit und Richtigkeit dieser strategischen Entscheidung zu überzeugen.
Ob und wie die vorhandene Unternehmenskultur eine geplante Veränderung positiv oder negativ beeinflusst, hängt dabei weitgehend von den Ausprägungen, Werten und Normen der einzelnen Mitarbeiter ab.
Veränderungsfördernde Kräfte:

- eine allgemeine Unzufriedenheit mit der gegenwärtigen Situation,
- die Überzeugung der Mitarbeiter, dass die geplanten Veränderungen nicht nur Vorteile für das Unternehmen, sondern auch für den einzelnen bringen können,
- eine weitgehende Aufgeschlossenheit gegenüber Neuerungen, sowohl bei den Führungskräften, als auch bei den Mitarbeitern,
- flexible, anpassungsfähige und veränderungsbereite Mitarbeiter.

Veränderungshemmende Kräfte:

- infolge mangelnder Aufklärung und Überzeugung auftretende Unsicherheiten und Ängste,
- negative Erfahrungen der Mitarbeiter in der Vergangenheit,
- organisierter Widerstand durch Interessenskonflikte zwischen Firmenleitung und Belegschaft,
- mangelndes Interesse und Motivation,
- Bequemlichkeit, Selbstzufriedenheit,
- festgefahrene Abläufe und Strukturen,
- stark ausgeprägtes Status- und Besitzdenken.

Ein probates Mittel bei der Beeinflussung der unternehmensbezogenen Werte ist die Aus- und Weiterbildung [Wojda, 2005, Inhalt der Organisationsgestaltung, S 45f].

Sensibilisierung[424]
Sicherheitskultur soll als Teil der Unternehmenskultur gesehen werden. Eine Kulturveränderung, unterstützt durch das Informationssicherheitsmanagement, herbeizuführen, ist Aufgabe der Führungskräfte. Sensibilisierungsmaßnahmen sind unabdingbar: Sicherheitsmarketing, Sensibilisierungs-Trainings, PR-Maßnahmen etc.
Schritt 1: Ist-Analyse auf sozialer Ebene. Definition der Mitarbeiter-Konstellation im Unternehmen. Umfrage, wie Mitarbeiter die bestehende Kultur wahrnehmen.

[424] Vgl. http://www.securitymanager.de/magazin/artikel_810_informationssicherheitskultur_umgesetzt.html [23. Feber 2007]

Schritt 2: Zieldefinition. Wie muss die Unternehmenskultur sein, damit sie dem strategischen Ziel „Risikominderung und Schadenseingrenzung“ entspricht? Wie sollen sich Mitarbeiter verhalten, welche Werte sollten gemäß Sicherheitskultur wichtig sein? Wohin können sich emotional bewegte Mitarbeiter wenden?
Schritt 3: Erarbeitung der Strategie. Erforderliche Kompetenzen erarbeiten, um die Werte und Verhaltensweisen von Mitarbeitern zu verstehen. Mitarbeiter im Veränderungsprozess begleiten. Basis bildet das eigene Verständnis des Veränderungsprozesses. Themen wie Konfliktmanagement, Emotionale Intelligenz, Kommunikationsverhalten, Kommunikations-und Team-Fähigkeit gehören ebenfalls dazu.

Das Sensibilisierungsprogramm [Österreichisches Sicherheitshandbuch, 2004, S 74] sollte systemübergreifend sein und folgende Punkte umfassen:

- Information aller Mitarbeiter über die Informationssicherheitspolitik der Organisation (Informationssicherheitsziele und -politik, die Bedeutung der Informationssicherheit für die Institution, Organisation und Verantwortlichkeiten im Bereich der Informationssicherheit, die Risikoanalysestrategie, die Sicherheitsklassifizierung von Daten, ausgewählte Sicherheitsmaßnahmen),
- die wichtigsten Ergebnisse der Risikoanalysen (Bedrohungen, Schwachstellen, Risiken etc.),
- die Pläne zur Implementation und Überprüfung der Sicherheitsmaßnahmen,
- die Auswirkungen von sicherheitsrelevanten Ereignissen für einzelne Anwender und für die gesamte Institution,
- die Notwendigkeit, Sicherheitsverstöße zu melden und zu untersuchen,
- die Konsequenzen bei Nichteinhaltung von Sicherheitsvorgaben,
- regelmäßige Veranstaltungen zum Thema Informationssicherheit,
- Publikationen,
- schriftliche Festlegung der Berichtswege und Handlungsanweisungen im Falle eines vermuteten Sicherheitsproblems.

Die Sensibilisierungsaktivitäten sollten jeden Mitarbeiter auf seine Verantwortlichkeit für Informationssicherheit hinweisen. Dabei ist insbesondere die Verantwortung des Managements zu betonen. Zudem ist das Sensibilisierungsprogramm regelmäßig auf seine Aktualität hin zu prüfen.

1.8.3.1.3 Sicherheitsfaktor Mitarbeiter

Für die Planung, Erstellung und Durchführung des Informationssicherheitsmanagements muss es klar definierte Verantwortlichkeiten geben. Die entsprechende Organisation für das

Informationssicherheitsmanagement ist für jedes Unternehmen – abhängig von Größe und Struktur – individuell festzulegen und in der Informationssicherheitspolitik festzuhalten.
Während bei größeren Unternehmen die Sicherheitsaufgaben von mehreren Personen wahrgenommen werden, gibt es bei kleineren und mittleren Betrieben meist nur einen zuständigen Mitarbeiter, der diese Agenden zusätzlich zu anderen Aufgaben übernimmt [Österreichisches Sicherheitshandbuch, 2004, S 28ff].

- *Informationssicherheitsbeauftragter* (engl. *Chief Information Security Officer* (kurz: *CISO*). Dieser ist zentraler Ansprechpartner für alle informationstechnischen Sicherheitsfragen innerhalb einer Organisation und trägt die fachliche Verantwortung für diesen Bereich. Zu seinen Pflichten gehören etwa die Mitwirkung an der Erstellung des Informationssicherheitskonzeptes, die Realisierung der ausgewählten Sicherheitsmaßnahmen, die Koordination von Schulungs- und Sensibilisierungsveranstaltungen oder die Gewährleistung der Informationssicherheit im laufenden Betrieb. Der Informationssicherheitsbeauftragte kann zwar Aufgaben delegieren, bleibt jedoch in der Gesamtverantwortung für die Informationssicherheit.
- *Informationssicherheitsmanagement-Team*: Diese Personen sind verantwortlich für die Regelung der organisationsweiten Informationssicherheitsbelange sowie für die Erarbeitung von Plänen, Vorgaben und Richtlinien zur Informationssicherheit (Entwicklung einer organisationsweiten Informationssicherheitspolitik, Überprüfung des Konzeptes auf Erreichung der Sicherheitsziele, Festlegung der personellen und finanziellen Ressourcen für Informationssicherheit). Das Team sollte in der Informationssicherheitspolitik verankert sein und setzt sich typischerweise unter anderem aus einem Mitglied der Unternehmensleitung, dem Informationssicherheitsverantwortlichen und einem Vertreter der IT-Anwender zusammen.
- *Datenschutzbeauftragter*: Auch wenn es gesetzlich nicht zwingend vorgeschrieben ist, ist es empfehlenswert, einen Verantwortlichen für die Einhaltung der Datenschutzbelange zu nominieren.

1.8.4 INFORMATIONSSICHERHEITSSTANDARDS UND -VORSCHRIFTEN

In diesem Kapitel soll eine Übersicht auf Basis des Dokuments „*Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk*“ [Bitkom, 2006-1] über die relevanten Informationssicherheitsstandards und -vorschriften gegeben werden.
Die Auswahl und die Anwendung eines angemessenen IT-Sicherheitsstandards ist Teil des Informationssicherheitsmanagements (siehe *1.8.1 Ziele und Aufgaben des Informationssicherheitsmanagements*). Die Erstellung eines umfassenden Informationssicherheitsmanagements ist eine anspruchsvolle Aufgabe (siehe *1.8.2 Umsetzung von Informationssicherheitsmanagement*). Vorgehensweisen selbst zu entwickeln, ist aufwendig und teuer

in der Umsetzung. Es ist sinnvoll, auf bewährte, in Normen und Standards festgehaltene, Vorgehensweisen zurückzugreifen.

Wesentliche Ziele und Nutzen beim Einsatz von Normen und Standards:

- Kostensenkung
  - Nutzung vorhandener und praxiserprobter Vorgehensmodelle,
  - Methodische Vereinheitlichung und Nachvollziehbarkeit,
  - Ressourceneinsparung durch Kontinuität und einheitliche Qualifikation,
  - Interoperabilität.
- Einführung eines angemessenen Sicherheitsniveaus
  - Orientierung am Stand der Technik und Wissenschaft,
  - Gewährleistung der Aktualität,
  - Verbesserung des Sicherheitsniveaus durch die Notwendigkeit der zyklischen Bewertung.
- Wettbewerbsvorteile
  - Zertifizierung des Unternehmens sowie von Produkten,
  - Nachweisfähigkeit bei öffentlichen und privatwirtschaftlichen Vergabeverfahren,
  - Verbesserung des Unternehmensimage,
  - Stärkung der Rechtssicherheit.

Es gibt eine Reihe von Standards, Normen und Vorschriften. Das *Deutsche Normungsinstitut*[425] hat eine Klassifizierung in Informationssicherheitsmanagement-Systeme, Sicherheitsmaßnahmen und Monitoring, Evaluierung von IT-Sicherheit, kryptographische und IT-Sicherheitsverfahren bzw. physische Sicherheit vorgenommen. Im Folgenden sollen die gängigsten Standards zum IT-Sicherheits- und Risikomanagement erläutert werden. Auf Aspekte der Evaluierung von Informationssicherheit (Stichwort: *Common Criteria*), Normen für kryptografische Sicherheitsverfahren (Verschlüsselung, Hash, Zeitstempeldienste etc.) und spezielle Sicherheitsfunktionen (Brandschutz, Einbruchshemmung etc.) wird nicht näher eingegangen.

1.8.4.1 Standardisierte Informationssicherheitsmanagement-Systeme

Die grundlegende Norm für ein ISMS ist die ISO 27001:2005 (siehe *1.8.2.1.2 Informationssicherheitsmanagement-System*). Sie beschreibt die Anforderungen an ein Informationssicherheitsmanagement-System in einem Unternehmen oder in einer Behörde. In der *ISO 13335:2004*[426] wird die Methodik, in der ISO 17799:2005 werden die Maßnahmen und in der *ISO*

[425] Vgl. http://www.nia.din.de/ni27 [24. Feber 2007]
[426] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39066 [24. Feber 2007]

27004:200x[427] (in Entwicklung, Status Dezember 2006) wird künftig die Qualitätsmessung für ein ISMS erläutert. Der deutsche IT-Grundschutz erläutert ebenfalls die Anforderungen eines ISMS und ist mit der ISO 27001:2005 kompatibel. Das Österreichische IT-Sicherheitshandbuch ist auf Basis des deutschen IT-Grundschutzhandbuches entstanden. Es wurde um österreichische Gegebenheiten, Normen und Gesetze[428] erweitert bzw. ergänzt.

1.8.4.1.1 ISO 27001:2005 Information security management systems – Requirements

Die ISO 27001:2005 ist aus dem zweiten Teil des BS 7799-2 hervorgegangen. Ziel des Standards ist es, die Anforderungen an ein ISMS darzustellen. Da das Dokument generisch gehalten ist, um es auf alle Organisationen anwenden zu können, haben diese Anforderungen einen niedrigen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse genau definiert sind. Das Dokument basiert auf dem PDCA-Modell (siehe *1.8.2.1.2 Informationssicherheitsmanagement-System*), das im Kontext eines ISMS angewandt wird. Ein ISMS erlaubt es, ermittelte Risiken durch geeignete, in die Organisationsprozesse eingebettete Kontrollmechanismen zu reduzieren, zu verlagern oder zu kontrollieren. Hierbei sind die Geschäftsziele und die resultierenden Sicherheitsanforderungen als Input sowie *gemanagte* Informationssicherheit als Output anzusehen. Die transformierenden Systemprozesse sind das Aufbauen, das Umsetzen und Betreiben, das Überprüfen sowie das Aufrechterhalten und Verbessern.
Der Standard wendet sich an die Geschäftsleitung und den Informationssicherheitsbeauftragten, weniger an die Umsetzungsverantwortlichen (Techniker, Administratoren).
Der Grad der Umsetzung des ISMS kann von internen oder externen Auditoren kontrolliert werden. ISO 27001:2005 ist die erste internationale Norm zum Informationssicherheitsmanagement, die auch eine Zertifizierung ermöglicht. Aufbauend auf der Norm können nationale Zertifizierungsschemata definiert werden.

1.8.4.1.2 ISO 13335:2004 Management of information and communications technology security

Diese Norm versteht sich als allgemeine Leitlinie für die Initiierung und Umsetzung des Informationssicherheitsmanagement-Prozesses. Er gibt Anleitungen, jedoch keine Lösungen für das Management von Informationssicherheit. Die Norm stellt ein Basiswerk dar und ist Ausgangspunkt für eine Reihe von Dokumenten zum Informationssicherheitsmanagement. Sie besteht derzeit aus drei Teilen, wobei folgende zwei besondere Relevanz haben:
Part 1: Concepts and models for information and communications technology security management

427 http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42106&scopelist=PROGRAMME [24. Feber 2007]
428 Vgl. http://www.a-sit.at/downloads/20031124_SIHA_A-SIT_mh.pps November 2003 [24. Feber 2007]

In diesem Teil werden sicherheitsrelevante Begriffe wie Werte, Bedrohungen, Schwachstellen, Schäden, Risiken, Sicherheitsmaßnahmen und deren Beziehung zueinander sowie Ziele, Strategien und Leitlinien vorgestellt. Neben organisatorischen Aspekten wie beispielsweise Rollen und Zuständigkeiten werden Sicherheitsmanagement-Funktionen erläutert, sowie die Notwendigkeit von Risikomanagement betont.

Part 2: Techniques for information security risk management

Dieser Teil geht auf das Risikomanagement (Rahmenbedingungen festlegen, Risiken bewerten und Behandlung von Risiken) ein. Die Aktivitäten der Risikobewertung (Risikoermittlung, -analyse und -abschätzung) werden detailliert beschrieben. Weitere Sicherheitsmanagement-Funktionen (Kommunikation von Risiken, deren Überwachung und Nachverfolgung) werden dem Risikomanagement-Prozess zugeordnet. Die informativen Anhänge geben Hilfestellungen bei der Bearbeitung der einzelnen Prozessschritte.

Im Vergleich zu ISO 27001:2005 und ISO 17799:2005 beschreibt die ISO 13335:2004 den Sicherheitsprozess ausführlicher und zeigt insbesondere Ansätze für die Durchführung einer Risikobewertung auf.

Es ist geplant, beide Teile der ISO 13335 in die ISO 27000-Reihe zu überführen. Teil 1 soll zum ISO 27000-Standard "*Information security management system fundamentals and vocabulary*" und Teil 2 zum ISO 27005-Standard "*Information security risk management*" überarbeitet werden (Anfang 2008).

1.8.4.1.3 ISO 17799:2005 Code of practice for information security management

Die ISO 17799:2005 ist aus dem ersten Teil des *British Standard BS 7799-1*[429] („*Code of Practise*") hervorgegangen. Grundsätzlich ist dieser Standard dort anzuwenden, wo Schutzbedarf für Informationen besteht. Ziel ist es, Informationssicherheit als Gesamtaufgabe darzustellen und ein Rahmenwerk für das Informationssicherheitsmanagement zu definieren. ISO 17799:2005 befasst sich daher hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Informationssicherheitsmanagement aufzubauen und in der Organisation zu verankern[430]. Die Empfehlungen sind für die Managementebene bzw. den Informationssicherheitsbeauftragen aufbereitet und enthalten kaum konkrete technische Hinweise. Ihre Umsetzung ist eine der Möglichkeiten, die Anforderungen der ISO 27001:2005 zu erfüllen. Der Standard legt Richtlinien und allgemeine Prinzipien für das Initiieren, Umsetzen, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements in einer Organisation fest.

Die ISO-Norm befasst sich mit den folgenden Bereichen:

[429] http://www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/ICT/Information-Security/ [27. März 2007]

[430] Vgl. http://www.kes.info/archiv/online/05-6-006.htm [27. März 2007]

- *information security policy*: Informationssicherheitsrichtlinie,
- *organization of information security*: Organisatorische Sicherheitsmaßnahmen,
- *asset management*: Umgang mit Informationswerten,
- *human resources security*: Personelle Sicherheit,
- *physical and environmental security*: Physische Sicherheit,
- *communications and operations management*: Kommunikations- und Betriebssicherheit,
- *access control*: Zugriffskontrolle,
- *information systems acquisition, development and maintenance*: Beschaffung, Entwicklung und Wartung,
- *information security incident management*: Umgang mit Sicherheitsvorfällen,
- *business continuity management*: Notfallvorsorgeplanung,
- *compliance*: Einhaltung rechtlicher Verpflichtungen, von Sicherheitsrichtlinien und Überprüfungen durch Audits.

Aufgrund der Bestrebungen, alle Standards, die ISMS betreffen, in die ISO 27000-Reihe zusammenzuführen, soll die ISO 17799:2005 ab Sommer 2007 in die ISO 27002:2007 übergeführt werden.

1.8.4.1.4 IT-Grundschutzhandbuch

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) als nachgeordnete Behörde des Innenministeriums bietet seit 1994 das IT-Grundschutzhandbuch (kurz: IT-GSHB) an, welches detailliert IT-Sicherheitsmaßnahmen aus verschiedenen Bereichen (Technik, Organisation, Infrastruktur und Personal) sowie Anforderungen an das IT-Sicherheitsmanagement beschreibt. Damit auch der internationale Standard für Informationssicherheitsmanagement-Systeme abgedeckt werden kann, wurde das IT-Grundschutz-Handbuch entsprechend modifiziert und ist vollständig kompatibel zur ISO 27001:2005.
Sowohl ISO 13335:2004 als auch ISO 27001:2005 und ISO 17799:2005 sind als Leitfäden zum Informationssicherheitsmanagement anzusehen und bieten keine konkreten Lösungen. ISO 13335 und das IT-GSHB sind zueinander kompatibel, wobei das IT-GSHB eine konkretere Handhabung zum Sicherheitsmanagement liefert.
Die IT-Grundschutz-Vorgehensweise[431] beschreibt Schritt für Schritt, wie ein IT-Sicherheitsmanagement in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des IT-Sicherheitsmanagements und der Aufbau einer IT-Sicherheitsorganisation sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein IT-

[431] Vgl. http://www.bsi.de/literat/bsi_standard/index.htm [27. März 2007]

Sicherheitskonzept in der Praxis zu erstellen ist, angemessene IT-Sicherheitsmaßnahmen auszuwählen sind und worauf bei der Umsetzung des IT-Sicherheitskonzeptes zu achten ist. Es gibt ebenfalls praktische Ansätze für die Aufrechterhaltung und Verbesserung der Informationssicherheit im laufenden Betrieb.
IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der ISO-Standards 13335-1:2004, 17799:2005 und 27001:2005 und hilft Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrundwissen und Beispielen. In den sogenannten IT-Grundschutz-Katalogen wird nicht nur erklärt, was gemacht werden sollte, sondern es werden konkrete Hinweise gegeben, wie eine Umsetzung aussehen kann. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen der genannten ISO-Standards nachzukommen.
Seit Anfang 2006 können ISO 27001:2005-Zertifikate auf der Basis von IT-Grundschutz beim BSI beantragt werden.

1.8.4.2 Standards mit Informationssicherheitsaspekten

Im Folgenden wird mit *Control Objectives for Information and Related Technology* (kurz: CobiT)[432] ein allgemein akzeptierter, vielfach angewendeter Standard angeführt, der im Sinne von best practice von Verbänden und Interessenvereinigungen für ihre Mitglieder erstellt worden ist. Der Schwerpunkt solcher Standards liegt bei der Unterstützung zur Erreichung von Unternehmenszielen. Als „Nebeneffekt" tragen sie zur Erhöhung der Informationssicherheit bei. ITIL, das in diesem Sinne mit CobiT vergleichbar ist, wurde bereits bei den Gegenmaßnahmen behandelt (siehe *1.7.1.2.1 Information Technology Infrastructure Library (ITIL)*).

1.8.4.2.1 CobiT

Zur Unterstützung der Unternehmensleitung und der damit befassten Fachabteilungen bei der Wahrnehmung ihrer Verantwortung (Erreichung der Geschäftsziele, effizienter und effektiver Ressourceneinsatz, Einhaltung rechtlicher Rahmenbedingungen) wurde mit CobiT ein umfassendes Kontrollsystem bzw. Rahmenwerk geschaffen, das alle Aspekte des IT-Einsatzes von der Planung über den Betrieb bis hin zur Entsorgung berücksichtigt und somit eine ganzheitliche Sicht auf die IT gibt. CobiT unterstützt die Ziele der IT-Governance im Unternehmen: die Ausrichtung der IT auf die Geschäftstätigkeit, den wirtschaftlichen Einsatz von IT-Ressourcen und ein angemessenes Management IT-bezogener Risiken.
Der Standard stellt sich als Sammlung von Informationen, Werkzeugen und Richtlinien dar, die die Sichtweisen der einzelnen durch IT-Governance angesprochenen Gruppen umfassend und spezifisch abbilden. Das CobiT-Framework enthält Anforderungen an die Geschäftsprozesse in den Kategorien Qualität, Sicherheit und Ordnungsmäßigkeit und den sieben Zielkriterien – Vertraulichkeit,

Verfügbarkeit, Integrität, Effektivität, Effizienz, Zuverlässigkeit und Einhaltung rechtlicher Erfordernisse. Diese werden mit den verwendeten IT-Ressourcen in den Kategorien Daten, Anwendungen, Technologien, Anlagen und Personal in Zusammenhang gestellt und in die Gesamtsicht des zyklischen Prozesses „Planung & Organisation, Beschaffung & Implementierung, Betrieb & Unterstützung und Überwachung“ eingefügt, der den gesamten Lebenszyklus aller Ressourcen umfasst. Dabei steht das Ziel im Vordergrund, dass IT-Ressourcen kontrolliert geplant, entwickelt, implementiert sowie betrieben und überwacht werden. Diese vier übergeordneten Prozesse sind in insgesamt 34 kritische IT-Prozesse unterteilt, die für ein angemessenes Management der IT ausschlaggebend sind.

1.8.4.3 Gesetze und Vorschriften

Es gibt Gesetze und Vorschriften die im Zusammenhang mit Informationssicherheit bzw. Risikomanagement stehen: Datenschutzgesetz, Verbandsverantwortlichkeitsgesetz etc. (siehe *1.7.3 Gesetzeslage*), Basel II, Sarbanes Oxley Act, 8. EU-Richtlinie[433] etc.
Einige davon sind seit längerem in Kraft, andere sind in der Umsetzung (z. B.: Basel II in der ersten Etappe für die Mitgliedsländer der Europäischen Union). Den betroffenen Unternehmen drohen bei Nicht-Einhaltung der Vorschriften zum Teil schwerwiegende – finanzielle, auch strafrechtliche – Konsequenzen.
In den folgenden Ausführungen werden mit Basel II und Sarbanes Oxley Act zwei repräsentative Regulative (*Compliance*) vorgestellt.

1.8.4.3.1 Basel II

Basel II steht für die Gesamtheit der Eigenkapitalvorschriften, die vom *Basler Ausschuss für Bankenaufsicht*[434] in den letzten Jahren erarbeitet wurden. Die primären Ziele sind die Sicherung einer angemessenen Eigenkapitalausstattung von Banken und die Schaffung einheitlicher Wettbewerbsbedingungen für das Kreditgeschäft.
Die Regeln sind gemäß der *EU-Richtlinie 2006/49/EG*[435] in den Mitgliedsstaaten der Europäischen Union anzuwenden: mit 2007 auf freiwilliger Basis, ab 2008 verpflichtend[436].
Basel II basiert auf drei Säulen:

- Die erste Säule repräsentiert den minimalen notwendigen Eigenkapitaleinsatz. Dabei soll speziell das tatsächliche Risiko für die Banken berücksichtigt werden.

[432] http://www.isaca.org/ [24. Feber 2007]
[433] http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31984L0253:DE:HTML [25. Feber 2007];
http://www.8-eu-richtlinie.de/ [24. Feber 2007]
[434] http://www.bis.org/bcbs/index.htm [25. Feber 2007]
[435] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 32006L0049 [25. Feber 2007]
[436] Vgl. http://www.oenb.at/de/finanzm_stab/basel_II/basel_ii.jsp [1. März 2007]

- Die zweite Säule behandelt die bankenaufsichtlichen Überprüfungsprozesse.
- Die dritte Säule befasst sich mit der Transparenz der Bilanzen für die Öffentlichkeit.

Basel II bezieht sich zunächst auf interne Bankvorschriften. Es wird jedoch allgemein erwartet, dass jene Maßstäbe, die an das Kreditrisiko für Banken geknüpft werden, auch an die Kunden weitergegeben werden. Das kann bedeuten, dass für den Erhalt eines Kredites sogar die nachgewiesene Informationssicherheit entscheidend sein kann. Mit Inkrafttreten von Basel II hängt die Kreditvergabe vom Rating eines Unternehmens ab und dieses unter anderem auch von dessen Informationssicherheitsmanagementniveau.
Die Einrichtung von internen Kontrollen und Informationssicherheitsmaßnahmen, die Risiken für das Unternehmen mindern, werden sich aufgrund von Basel II positiv auf Kreditkonditionen auswirken.

1.8.4.3.2 Sarbanes Oxley Act

Der Sarbanes-Oxley Act (kurz: SOA oder SOX) ist ein US-amerikanisches-Gesetz zur verbindlichen Regelung der Unternehmensberichterstattung. Es wurde im Jahr 2002 von den beiden Senatoren *Paul Sarbanes* und *Michael Oxley* als Reaktion auf diverse Finanzskandale in den USA initiiert. Ziel ist es, Investoren zu schützen und verlorengegangenes Vertrauen der Anleger in die Richtigkeit der veröffentlichten Finanzdaten wiederzugewinnen, indem die Genauigkeit und Verlässlichkeit der Rechnungslegung in Übereinstimmung mit Sicherheitsgesetzen verbessert wird. Das Gesetz gilt für inländische und ausländische Unternehmen, die an einer US-Börse notieren.
Das Gesetz gliedert sich in sogenannte *Sections*. Aus IT-Sicherheitssicht wird die größte Relevanz der *Section 404*[437] zugemessen. Der Abschnitt will sicherstellen, dass die Ordnungsmäßigkeit der Verarbeitung und die Integrität der verarbeiteten relevanten Finanzdaten jederzeit gewährleistet ist. Weiterhin sollte der Zugriff auf die Finanzdaten insbesondere zu Zeiten von fälligen Quartalsberichten oder Jahresabschlüssen sichergestellt sein.
Section 404 schreibt folgende Prozesse vor:
1. Auswahl und Beurteilung eines Regelwerks für ein internes Kontrollsystem,
2. Dokumentation des internen Kontrollsystem (IKS),
3. Überwachung des IKS.

Über die Funktionsfähigkeit dieses IKS muss in den periodischen Unternehmensreports berichtet werden. Hierbei wird auf die Managementverantwortung zur Einrichtung und zum Betrieb vom IKS und zu den Prozessen zum Finanz-Reporting hingewiesen. Der Einsatz eines IT-Risikomanagements spielt dabei eine wichtige Rolle.

[437] http://www.soxlaw.com/s404.htm [25. Feber 2007]

EuroSOX

Abgeleitet vom amerikanischen SOX wird die europäische Version umgangssprachlich als EuroSox bezeichnet. Es dreht sich dabei um die *8. Europäische Richtlinie*[438], welche am 17. Mai 2006 beschlossen wurde. Die Richtlinie ist von allen EU-Mitgliedsstaaten bis 29. Juni 2008 in nationales Recht umzusetzen. Dabei geht es um Vorgaben für nationale Gesetze über Aktionärssicherheit sowie unabhängige Rechnungs- und Abschlussprüfung von Unternehmen bestimmter Rechtsformen. Ziel von EuroSox ist es, Transparenz darüber zu schaffen, wer auf welche Informationen im Unternehmensnetzwerk zugreifen kann und von wem wann welche Berechtigungen dazu erteilt wurden[439].

1.8.4.4 Einführung von Informationssicherheitsstandards im Unternehmen

Die Einführung von Standards im Unternehmen erfolgt in drei generischen Schritten:

1. Auswahl de(r)/(s) Norm/Standards: In der Regel entscheidet die Geschäftsführung mit Unterstützung des IT-Verantwortlichen und – falls vorhanden – Informationssicherheitsbeauftragten den IT-Betrieb an einem Informationssicherheitsstandard auszurichten. Welcher Standard der richtige für ein Unternehmen ist, hängt von der Art des Unternehmens, vom relevanten Unternehmensbereich für die Standardisierung und von den relevanten Charakteristika des Standards ab.
2. Einführung: Die Einführung von Informationssicherheitsstandards im Unternehmen erfolgt nach dem jeweiligen Vorgehensmodell des ausgewählten Standards.
3. Betrieb: Nach der Einführung des Standards müssen die getroffenen Maßnahmen in den regulären Betrieb übergehen. Hierfür sind beispielsweise Mitarbeiterschulungen sowie möglicherweise Prozessanpassungen erforderlich. Im Rahmen des regulären IT-Betriebs kann die Einhaltung des Standards durch zwei aufeinander aufbauende Verfahren überprüft und gewährleistet werden:
   - Auditierung: Im Rahmen eines Audits vergleicht ein Auditor (extern, zertifiziert) anhand der Vorgaben des gewählten Standards bzw. der Dokumentation des IT-Betriebs den Ist-Stand mit dem Soll-Konzept. Empfehlungen für die Verbesserung der Informationssicherheit werden ausgesprochen (siehe *1.7.1.1.3 Audits und Revision*).
   - Zertifizierung: Einige Informationssicherheitsstandards (siehe *1.8.4.1 Standardisierte Informationssicherheitsmanagement-Systeme*) können als Grundlage für eine Zertifizierung herangezogen werden. Ein Zertifikat ist eine objektive und unabhängige Bestätigung für die im Standard geforderten und auch tatsächlich dokumentierten bzw. umgesetzten

[438] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0087:01:DE:HTML [16. Dezember 2007]
[439] Vgl. http://www.iam-wiki.org/Euro_Sox [16. Dezember 2007]

Sicherheitsmaßnahmen. Der Aufwand für die Zertifizierung ist abhängig vom Unternehmen und dem Zertifizierungsziel. Der interne Aufwand (Vorbereitung, Durchführung) ist dabei in den meisten Fällen sehr hoch.

1.8.5 KOMMERZIELLER ASPEKT

Unternehmen benötigen umfassende, präzise Informationen für den laufenden Betrieb bzw. für die Entscheidungsfindung. Diese Informationen werden – je nach Anforderung – von IT-Systemen rund um die Uhr und ortsungebunden bereitgestellt. Jedes Unternehmen hat unterschiedliche Anforderungen an die Verfügbarkeit der Informationen. Fällt die IT-Infrastruktur aus, so ist dies in der Regel mit erheblichen Kosten verbunden. Längere Ausfälle können für ein Unternehmen sogar existenzbedrohend sein. Die Kosten, die durch die Nichtverfügbarkeit der IT entstehen, hängen sehr stark von der jeweiligen Anwendung und vom Geschäftsfeld des Unternehmens ab. Es ist daher für jedes Unternehmen elementar, die monetären Auswirkungen eines System-Stillstands (engl. *Downtime*) der wesentlichen IT-Komponenten zu kennen. Das ist vor allem bei kleinen und mittelständischen Unternehmen häufig nicht der Fall. Viele Unternehmen kennen weder die Kosten eines geplanten noch die finanziellen Konsequenzen einer ungeplanten Downtime. Bei der Bestimmung des möglichen finanziellen Gesamtschadens ist darauf zu achten, dass alle kostenbeeinflussenden Faktoren berücksichtigt werden[440]:

- Interne Kosten (Personalkosten bei System- und Arbeitsstillstand nach einem Ausfall, Umsatzverlust durch fehlende Geschäftsfähigkeit),
- Externe Kosten (Schadenersatzanforderungen, Konventionalstrafen, höhere Kreditzinsen durch Basel II),
- Indirekte Folge bei Nichtbeachtung (Haftungsrisiken, Freiheitsstrafen bei nicht-korrekter Bilanzierung laut SOA), bei nicht-korrekter Behandlung von Daten, bei Datenverlust oder Datenmanipulation kann die Gefährdung der Existenz von Unternehmen sein,
- Gefährdung der allgemeinen Sicherheit Dritter,
- Verlust der Glaubwürdigkeit und Zuverlässigkeit,
- Verlust von Marktanteilen und Image,
- Minderung der Wettbewerbsfähigkeit,
- Mögliche Haftung für Folgeschäden von Partnern und Lieferanten.

Schematisch kann die Bewertung folgendermaßen dargestellt werden:

[440] Vgl. http://www.securitymanager.de/magazin/artikel_1281_it_ausfaelle_vermeiden.html [25. März 2007]

Abbildung 30: Ermittlung der Ausfallskosten/Schadenshöhe

Die so ermittelten Ausfallskosten geben eine Größenordnung des zu erwartenden Gesamtschadens auf finanzieller Seite bei Systemstillstand wieder.

Im Zuge der Risikoanalyse (siehe *1.8.2.3 Risikoanalyse*) werden die Risiken – gewichtet nach Eintrittswahrscheinlichkeit und Schaden – herausgearbeitet. Gegenmaßnahmen werden logischerweise zunächst dort eingesetzt, wo das Risiko am höchsten ist. Die Neutralisierung der Risiken ist nur bis zu dem Zeitpunkt sinnvoll, bei dem die Risikominderung größer als die Investition ist.

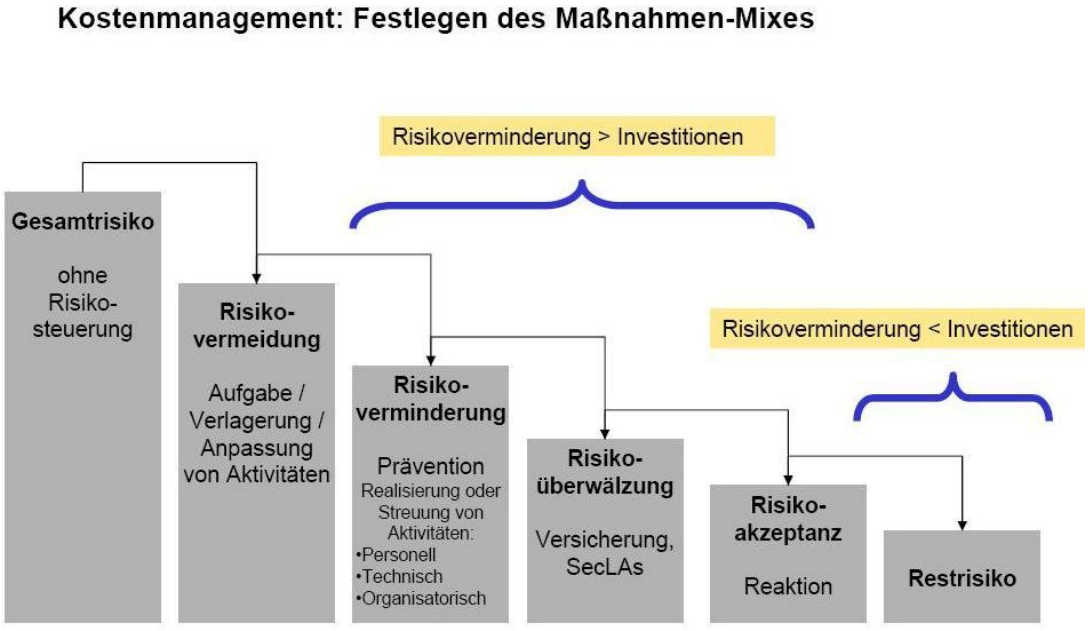


Abbildung 31: Risikominimierung

Jede Investition ist zu begründen. Dabei kann unter Zuhilfenahme von Metriken gezeigt werden, ob sich eine Ausgabe „rechnet“, respektive welche der angedachten Lösungen die beste Alternative im Sinne des Preis/Leistung-Verhältnisses ist. Eine gängige Kennzahl ist die *Return on Security Investment*- (kurz *ROSI*) Methode. In Anlehnung an eine Standard-*Return on Investment*- (kurz: *ROI*) Berechnung (erwarteter Nutzen–Investmentkosten/Investmentkosten) wird eine einfache Gleichung für ROSI [Sonnenreich, 2002, S 1] (es gibt noch weitere Ansätze für ROSI in der Literatur) angegeben:

ROSI = ((Risk Exposure * Risk Mitigated in Percent) – Solution Cost) / Solution Cost

Legende:

Risk Exposure = Schadenshöhe

Risk Mitigated = Risikominderung

Solution Cost = Kosten der Gegenmaßnahme

Zur Erläuterung ein Beispiel [Sonnenreich, 2002, S 1f]: Ein Unternehmen hatte einen Virenvorfall. Die Schadenshöhe wurde mit 25.000 Euro beziffert. Das Unternehmen nimmt an, dass ohne Schutz ein in dem Ausmaß stattfindender Virenbefall einmal pro Quartal eintreten würde. Durch den Kauf einer 25.000 Euro teuren Virenschutzsoftware erwartet sich der Betrieb, zumindest drei von vier Vorfällen verhindern zu können.

Werden die Werte in die Formel eingesetzt (Risk Exposure = 25.000 Euro, Risk Mitigated = 75%, Solution Cost = 25.000 Euro), ergibt sich ein ROI von 200 Prozent. In diesem Fall lohnt sich die Investition.

Das sehr vereinfachte Beispiel repräsentiert zwar nicht die Komplexität der Berechnung bei realen Situationen, zeigt aber dennoch, dass diese Kennzahl eine wertvolle Orientierungshilfe bei Investitionen sein kann [Sonnenreich, 2002, S 6].

1.9 EXKURS: GOOGLE

„*Seit Gutenberg die moderne Druckerpresse vor mehr als fünfhundert Jahren erfand, wodurch literarische und wissenschaftliche Werke für die Massen erschwinglich und weithin verfügbar wurden, hat keine Erfindung die Möglichkeiten von Individuen derart vergrößert und den Zugang zu Informationen so grundlegend umgewandelt wie Google. Mit dem bunten, kindlichen Logo vor rein weißem Hintergrund, seiner Fähigkeit, täglich blitzartig Millionen relevanter Antworten auf Suchanfragen zu liefern, hat es die Art und Weise, wie man sich heute informiert und auf dem Laufenden bleibt, radikal verändert. Als Teil unseres Alltagslebens ist Google unentbehrlich geworden. Millionen Menschen benutzen es täglich in über hundert Sprachen und viele setzen Google*

mit dem Internet gleich.“ Ein Auszug aus der Einführung im Buch die „*Die Google-Story*“ [Vise, 2006, S 15] soll die Bedeutung von Google[441] in der heutigen Internet-Gesellschaft wiedergeben.

1.9.1.1.1 Services und Geschäftsmodell von Google

Google ist ein stark expandierendes Unternehmen (Zukäufe[442], Partnerschaften), dessen Umsatzzahlen (1999: 220 Tsd. US-Dollar, 2004: 3,2 Mrd. US-Dollar [Vise, 2006, S 284]) und Marktwert (Stand März 2008[443]: ca. 100 Mrd. US-Dollar) sich seit der Gründung im Jahre 1998 vervielfacht haben. Durch den eingeschlagenen Weg, umfangreiche Kooperationen mit großen Anbietern im Internetbereich (eBay, AOL, Myspace) und Medienkonzernen (*NewsCorp*[444], *New York Times*[445], *MTV*[446]) einzugehen, können immer wieder große Werbeaufträge und Geschäfte lukriert werden. Google selbst investiert kein Geld in Werbung, das Wachstum von Google stützt sich ausschließlich auf Mundpropaganda [Vise, 2006, S 15].

Eine Untersuchung[447] des Unternehmens *comScore World Metrix*[448] im Jahr 2006 ergab, dass die Suchmaschine Google mit 156,3 Millionen Einzelbesuchern im Monat Juli die meistbesuchte Webseite Europas ist, zudem nannten 75 Prozent der Internetuser (60 Prozent in den USA) Google als ihre präferierte Suchmaschine.

Finanziert werden die kostenlosen Services durch Werbung und Lizenzverkauf. Inserenten zahlen bei Google nur dann Gebühren [Vise, 2006, S 116], wenn ihre Anzeigen angeklickt wurden, dadurch entsteht ein transparentes Verrechnungssystem. Bei jedem Klick eines Benutzers auf ein gezeigtes Inserat verdient Google Geld[449]. Die Kosten einer Anzeige bei Google werden nicht im vor hinein fixiert, sondern durch eine Online-Auktion bestimmt. Auf diese Weise stellt Google sicher, dass es einen konkurrenzfähigen Preis für jede Anzeige erzielt, die täglich millionenfach im Internet platziert wird. Firmen jeglicher Art nehmen an den Schlüsselwortauktionen teil und zahlen Google dafür Millionen von Dollar[450]. Damit wurde die traditionelle Werbung auf den Kopf gestellt, denn die

[441] http://www.google.com/ [23. Jänner 2007]
[442] Im März 2008 hat die EU der Übernahme des weltweiten Marktführers für Online-Werbung DoubleClick zugestimmt. Datenschützer warnen vor einer übergroßen Datenkonzentration. Sie sorgen sich, dass die beiden Unternehmen durch die Übernahme Zugang zu einer beispiellosen Menge von Kundendaten bekommen würden, damit das Surf-Verhalten von Millionen von Internetusern beobachten können.
[443] http://quotes.nasdaq.com/asp/SummaryQuote.asp?selected=GOOG&symbol=GOOG [16. März 2008]
[444] http://www.newscorp.com/ [23. Jänner 2007]
[445] http://www.nytimes.com/ [23. Jänner 2007]
[446] http://www.mtv.com/ [23. Jänner 2007]
[447] http://www.zdnet.de/news/tkomm/0,39023151,39146783,00.htm [27. März 2007]
[448] http://www.comscore.com/ [23. Jänner 2007]
[449] Googles Einnahmenschemen heißen Cost per Click bzw. Cost per Action. Im Rahmen des Programms AdWords, zu dem sich jeder anmelden kann, wird exakt eruiert, wie oft auf eine Seite geklickt wurde und welche Werbebotschaften bei den Internet-Usern ankommen. Als „Goldenes Dreieck der Internetsuche“ wird jenes Feld bezeichnet, auf das die Mehrzahl der Benutzer klickt. Das ist das Dreieck vom ersten bis zum fünften Treffer, dann schräg rechts nach oben zu den sogenannten sponsored Links.
[450] Eines der teuersten Worte mit etwa 90 Dollar pro Klick ist „Mesothelioma“ (Krebserkrankung aufgrund von Asbest). Amerikanische Anwälte erwarten sich durch einen gewonnenen Mesothelioma-Prozess eine Million

Inserenten bestimmen den Preis. Der Selbstbedienungscharakter des Systems und die niedrigen Mindestpreise ermöglichen es auch kleinen Unternehmen, sich der mächtigen Google-Werbeplattform zu bedienen. Das Höchstgebot garantiert bei Google jedoch nicht, dass eine Anzeige in einer Spitzenposition erscheint. Neben dem Preis, den ein Inserent bereit ist zu zahlen, ist die Häufigkeit [Vise, 2006, S 118], mit der potenzielle Käufer eine Anzeige anklicken, entscheidend.

Frei nach einem der beiden Google-Gründer *Sergey Brin* „*Ich will das gesamte Web auf meinen Computer herunterladen und indizieren*." [Vise, 2006, S 25] geht es im Wesentlichen um die Suche nach und die Bereitstellung von Information.

Google ist nicht nur die meistgenutzte Suchmaschine im Netz, sondern bietet unter anderem auch Online-Office-Software[451], eine Desktop-Suche (Google Desktop[452]), E-Mail und Instant Messaging (*Gmail*[453]), Intranet (*Sites*[454]), Videoplattform (Youtube[455]) und Satellitenbilder (*Google Earth*[456]) an. Das Unternehmen ist ständig auf der Suche nach neuen Möglichkeiten, sein Geschäft zu erweitern. Seit Herbst 2006 bietet Google ein Nachrichtenarchiv mit Artikeln über die vergangenen 200 Jahre (Suche nach Epoche bzw. Einzelpublikation) an. Mit „*Google Lokale Anzeigen*" und „*Google Maps Branchencenter*" gibt es seit Herbst 2006 sind zwei weitere neue Produkte. Hierbei folgt Google dem Bedürfnis der User, ihre Suche lokal spezifizieren zu können.

Google bietet den Usern die Möglichkeit, ihre Individualität und Kreativität mit der Suchmaschinen-Plattform „*Custom Search Engine*"[457] auszuleben. Damit können die Benutzer ihre eigenen Suchmaschinen zusammenbauen. Vom Aufbau der Suchmaschine bis hin zu den Prioritäten der einzelnen Suchergebnisse können die Nutzer alles selbst bestimmen.

Zwei der faszinierendsten Bereiche, an denen Google arbeitet, sind die Bereiche Molekularbiologie und Genetik. Millionen von Genen in Verbindung mit zahllosen biologischen und anderen naturwissenschaftlichen Daten sind eine Herausforderung für die Google-Suchmaschine und deren Datenbank. Google hat bereits eine Karte des menschlichen Genoms heruntergeladen und arbeitet mit Wissenschaftlern zusammen, das könnte bedeutende Fortschritte im Gesundheitswesen bringen. Mit anderen Worten: „Wir nähern uns vielleicht einer Zeit, in der man seine eigenen Gene googeln kann" [Vise, 2006, S 22, 268f].

Diese Liste würde sich beliebig erweitern lassen. Der wesentliche Punkt dabei ist, dass Google durch das ständig steigende Angebot mit jeder Eingabe und jeder Suchabfrage neue Daten zur Verfügung gestellt werden. Der Umgang mit diesen soll im Kapitel „Datenschutz" erläutert werden.

Dollar. Aus diesem Grund erkaufen sie sich einen Platz an vorderster Stelle der Suchergebnisse, um im Falle einer Erkrankung angeklickt zu werden.

[451] http://docs.google.com [23. Jänner 2007]
[452] http://desktop.google.com/ [23. Jänner 2007]
[453] http://gmail.google.com/ [17. März 2008]
[454] http://sites.google.com/ [29. Feber 2008]
[455] http://www.youtube.com/ [23. Jänner 2007]
[456] http://earth.google.com/ [23. Jänner 2007]

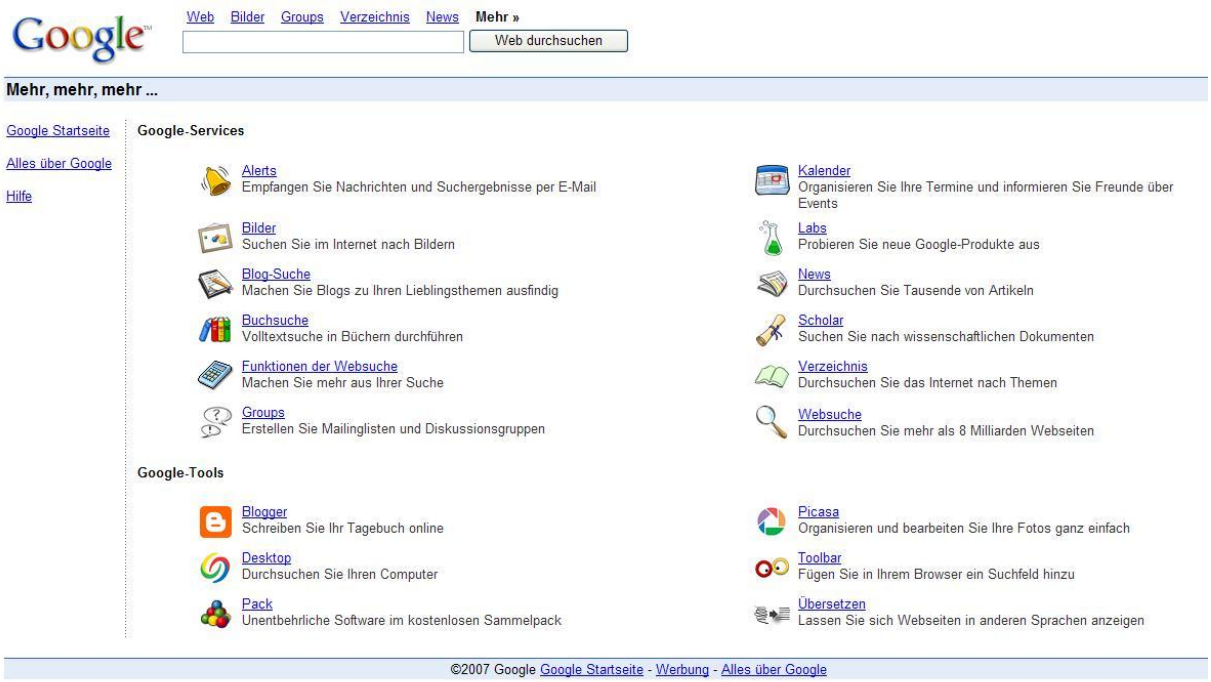


Abbildung 32: Google-Services

1.9.1.1.2 Datenschutz bei Google

Google wird von vielen als ein Produkt gesehen, gegenüber dem die Menschen eine Art von Vertrauen empfinden [Vise, 2006, S 15]. Google überwindet Unterschiede von Kultur, Sprache und Herkunft und ist inzwischen in der Wahrnehmung vieler Menschen eins mit dem Internet geworden. Der Umstand, dass dadurch viele persönliche Informationen auf einem unbekannten Speicher zusammenlaufen, scheint nur wenige zu kümmern. Die Geschäftspraktiken von Google geben immer wieder Anlass zu Kritik, weil sich das Unternehmen weigert, Internas und damit konkrete Aussagen zum praktizierten Datenschutz preiszugeben. Im Juni 2007 hat beispielsweise die Bürgerrechtsorganisation *Privacy International* (kurz: *PI*)[458] Google als einzigem renommierten Unternehmen das Prädikat „datenschutzfeindlich“ verliehen. Ein Bericht [Maurer, 2007] deutscher und österreichischer Forscher beschreibt Google kritisch als „die größte und mächtigste Datei der Welt“. Ein strittiger Punkt ist die Verwendung von individuellen Cookies (siehe *2.3.3.2.3 Cookie*). Laut Google dienen diese nur dazu, Einstellungen zu speichern. In der Realität wird für jeden Webbrowser eine eindeutige und 30 Jahre gültige Nummer vergeben. Die Kritik geht dahin, dass diese Identifikationsnummer nicht den Cookie-Einstellungen dient, sondern dazu, Suchanfragen jedes Users zu protokollieren. Der Free-E-Mailer Gmail steht im Visier von Konsumentenschützern, weil sich die automatische Auswertung von Nachrichten nicht nur dazu verwenden lässt, um kontextbezogene Werbung einzublenden, sondern auch, um detaillierte Benutzerprofile anzufertigen [c’t, 2006-1, S

[457] http://www.google.com/coop/cse [23. Jänner 2007]

162f]. Vor dem Gebrauch der Desktopsuchmaschine Google Desktop wird gewarnt, weil die Inhalte von Dateien der Benutzer auf Google-Servern hinterlegt werden[459]. Mit *Google Analytics*[460] wird Webseiten-Betreibern eine Technik angeboten, die Logdaten von Online-Angeboten auswertet und Besucherströme aufschlüsseln kann. Der Einsatz dieses kostenlosen Tools wirft ebenfalls datenschutzrechtliche Fragen auf [c't, 2006-2, S 192f].

Im Essay „*Ways Google is shaking the security world*“[461] wird unter anderem auf Google Hacking (siehe *1.4.3.8 Hacking*) eingegangen, wo Informationen generiert werden können, indem „*… using search engines to find systems vulnerabilities. Hackers can use carefully crafted searches to find things like open ports, overly revealing error messages or even (egads) password files on a target organization's computer systems.“*

Die Suchabfragen in der Volltextsuchmaschine sowie das Anklicken von Treffern und kontextbezogene Anzeigen offenbaren, für welche Produkte sich die Benutzer interessieren, welche Käufe in nächster Zeit geplant sein könnten etc. Jede Recherche in *Google News*[462], jeder Eintrag in *Blogger.com*[463], jede Aktieninfo in *Google Finance*[464], das Informieren in Google Earth über seinen Wohnort, jede Kommunikation über Gmail[465], alle im Sozial-Network *Orkut*[466] hinterlassenen persönlichen Fakten gibt Google Daten in die Hand. Google wäre demnach in der Lage, über einzelne Benutzer genaue Profile zu erstellen und sie somit zum „gläsernen Kunden“ zu machen[467]. In Deutschland wirft das *Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein*[468] der meistgenutzten Suchmaschine in einem diesbezüglichen Tätigkeitsbericht vor, dass „*ernsthafte Befürchtungen durch die Vorstellung hervorgerufen werden, dass sämtliche erhobene Daten der vielen Dienste von Google zusammengeführt werden“*.

Googles nächste Ziele[469] sind zum einen „*Alle Informationen dieser Erde so zu organisieren, dass sie für die Menschen zugänglich und nützlich sind. Wir arbeiten an der Demokratisierung der Informationen“*, zum anderen die „*ultimative Suchmaschine*“ zu entwickeln: „*eine Suchengine, die*

[458] http://www.privacyinternational.org/ [10. Juni 2007]
[459] Vgl. http://www.heise.de/ct/06/10/168/ [15. Feber 2007]
[460] http://www.google.com/analytics/ [24. Jänner 2007]
[461] Vgl. http://www.csoonline.com/read/050106/google_security.html [14. Feber 2007]
[462] http://news.google.com/ [24. Jänner 2007]
[463] http://www.blogger.com/ [24. Jänner 2007]
[464] http://finance.google.com/ [24. Jänner 2007]
[465] Der Autor hat sich am Beginn der Arbeit ein Gmail-Konto angelegt, um selbst Erfahrungen mit Google zu machen. Über diesen Account wurde unter anderem die Bestellung für Musik abgewickelt. Auffällig ist, dass in den neben den Suchergebnissen geschalteten Anzeigen tendenziell jene Musik zuerst aufscheint, die der bevorzugten Musikrichtung des Autors bzw. seiner Töchter fallen.
[466] https://www.orkut.com/ [24. Jänner 2007]
[467] Die Bürgerrechtsbewegung Public Information Research nominierte Google 2003 für ihre Nicht-Transparenz für den „Big Brother Award“.
[468] http://www.datenschutz.de/ [12. Juni 2007]
[469] Vgl. http://www.kuppingercole.de/sections/privacy - Interview mit Google-Europachef Arora [27. März 2007]

nicht nur Informationen findet, die auf dem basieren, was die User eintippen, sondern auf dem, was sie wirklich wollen".

Als Replik auf alle Diskussionen hinsichtlich Privatsphäre und Benutzeridentität verweist Google auf sein Firmencredo „*Don't be evil!*". Google betont, dass die Privatsphäre der Nutzer schon seit Beginn an ein zentrales Thema ist. Das Unternehmen möchte den Usern der zahlreichen Online-Dienste mehr Kontrolle über ihre eigenen Daten geben. Beispielsweise wird dem Benutzer eine Exportfunktion für Gmail zur Verfügung gestellt und Funktionen, die es erlauben, auf Google-Server gespeicherte Informationen zu löschen. Aufgrund eines Rechtsstreits im Feber 2007 in Belgien geht Google hinsichtlich Indizierung von Webseiten in die Offensive. „*Wenn Verleger nicht wollen, dass ihre Websites in den Suchresultaten erscheinen, helfen ihnen technische Standards wie robots.txt und Metatags ganz automatisch dabei, zu verhindern, dass ihre Inhalte in den Index einer Suchmaschine aufgenommen werden*."[470] Mit „robots.txt"[471] ist es möglich, Suchmaschinen den Zugriff auf bestimmte Seiten oder Verzeichnisse einer Website zu verbieten. Die Arbeitsweise bzw. das Einrichten einer robots.txt wird ebenso wie weitere Werkzeuge – unter anderem auch zum Löschen von Inhalten aus dem *Cache*[472] auf Google Servern – auf der Google-Website[473] dargestellt.

Im März 2007 hat Google verschärfte Richtlinien zum Schutz der Privatsphäre seiner Nutzer bei Suchanfragen bekannt gemacht. Daten wie IP-Adresse und Cookies sollen zukünftig nicht mehr unbegrenzt gespeichert und nach 18 bis 24 Monaten anonymisiert werden[474]. Nach weiteren Vorwürfen gab Google in einem Schreiben and die Europäische Union im Juni 2007 bekannt, die Nutzerdaten nur mehr 18 Monate lang zu speichern[475].

Google möchte damit den zunehmenden Bedenken hinsichtlich der Übermacht des Unternehmens entgegentreten und vor allem eventuellen Regulierungsversuchen von Regierungen zuvorkommen.

1.10 FAZIT

Die erarbeiteten Informationssicherheitsabhandlungen bilden die Grundlage für den Aufbau eines Identitätsmanagementsystems (kurz: IMS). Da der Schutz der Identität und der personenbezogenen Daten oberstes Sicherheits-Prinzip ist, ist ein umfassendes, auf die Unternehmensbedrohungen hin abgestimmtes Informationsmanagementsystem unabdingbare Voraussetzung für die Umsetzung eines IMS.

Es gilt, die wesentlichen Systeme (E-Mail, Web, Datenspeicher) und wertschöpfenden Prozesse (Einkauf, Produktion, Verkauf) abzusichern. Ebenso müssen Antworten auf die steigende Mobilität

[470] Vgl. http://futurezone.orf.at/business/stories/171766/ [14. Feber 2007]
[471] Beispiel: http://www.whitehouse.gov/robots.txt [14. Feber 2007]
[472] Unter Cache wird ein schneller Puffer-Speicher verstanden.
[473] Vgl. http://www.google.com/webmasters/ [14. Feber 2007]
[474] Vgl. http://www.zdnet.de/security/news/0,39029460,39152710,00.htm [18. März 2007]

und flexible Durchführung von Arbeit gefunden und gegeben werden. Technische Lösungen wie digitale Zertifikate oder biometrische Verfahren stellen wichtige Komponenten eines funktionierenden IMS dar. Bei der Etablierung eines IMS sind die gesetzlichen Vorgaben für Datenschutz, Betriebsratsmitbestimmungen oder Personalinformationssysteme (siehe *1.7.3.2.2 Personalinformationssysteme*) strengstens zu beachten. Für immer mehr Unternehmen gelten besondere Regeln im Umgang mit Bilanzierung und Revision (SOX, Basel II). Schlussendlich bestimmt der Mitarbeiter den Erfolg eines IMS. Alle technischen und administrativen Vorteile eines solchen Systems können nicht zur Geltung kommen, wenn es vom Mitarbeiter nicht akzeptiert wird. Neben entsprechenden Schulungs- und Sensibilisierungsmaßnahmen im Bereich Informationssicherheit ist vor allem eine passende Unternehmenskultur von eminenter Bedeutung.

Im Besonderen ist das Thema Informationssicherheit in Unternehmen (siehe *1.8 Unternehmenssicherheit*) mit der vom Autor erworbenen Praxis abgehandelt worden. Im Zuge der nach dem Österreichischen IT-Sicherheitshandbuch durchgeführten Umsetzung von Informationssicherheitsmanagement beim Arbeitgeber des Autors sind die folgenden Erkenntnisse ergänzend zu den bisherigen Ausführungen bemerkenswert.

Obwohl Informationssicherheit das gesamte Unternehmen betrifft, sollte für eine effektive Etablierung eines ISMS ein Geltungsbereich definiert und auch eingehalten werden. Dadurch sollte klar herausgearbeitet werden, *was nicht* untersucht wird.

Bei der Umsetzung des ISMS erweist sich eine Vereinfachung der komplexen Risikoanalyse als sinnvoll. Zu beachten ist jedoch, dass kein Bereich außer Acht gelassen bzw. vernachlässigt werden darf. Im Zuge der Risikoanalyse wurden daher zum einen vorhandene Dokumentationen geprüft, zum anderen erfolgte die Analyse toolunterstützt in Form von Interviews, Besprechungen, Begehungen und der repräsentativen Untersuchung von IT-Systemen und Applikationen. Die Bewertung erfolgte nach Parametern wie Plattform, Betriebssystem, Standort, Anzahl der verantwortlichen IT-Mitarbeiter, Anzahl der davon abhängigen Unternehmensmitarbeiter, Art der Daten oder Dateneigentümer. Das Ergebnis pro System oder Applikation wurde in einer Matrix mit – sinngemäß – folgendem Aussehen festgehalten:

[475] Vgl. http://www.pressetext.at/pte.mc?pte=070612031 [12. Juni 2007]

Gesamtbewertung (erfolgt nach dem Maximumprinzip)

	offen	vertraulich	geheim	sensibel
Vertraulichkeit				
	Klasse 1	Klasse 2	Klasse 3	Klasse 4
Verfügbarkeit				
	Klasse 1	Klasse 2	Klasse 3	Klasse 4
Integrität				

Abbildung 33: Bewertung Risikoanalyse

Bei der Klassifizierung der Daten muss zwischen Dateneigentümer und IT-Dienstleister unterschieden werden. Nur der Dateneigentümer kennt den Wert seiner Daten und kann den Schaden bei Nichtverfügbarkeit beziffern, daher obliegt die Bewertung allein dem Eigentümer, sprich der Fachabteilung. Bei der Durchführung der Klassifizierung ist zu entscheiden, welcher Vertraulichkeitslevel und welche Risikoklasse einer Information zugewiesen werden. Die Klassifizierung ist mit der erforderlichen Sorgfalt durchzuführen. Eine zu niedrige Einstufung kann Missbrauch ermöglichen, eine zu hohe zu einem nicht zu rechtfertigenden Aufwand führen. Die IT-Abteilung tritt lediglich als Datenhalter bzw. *Informationstreuhänder* auf.

Die bereits erwähnte Einbeziehung und Sensibilisierung der Mitarbeiter sowie die Verankerung des Themas Informationssicherheit beim Management können vom Autor aufgrund seiner Erfahrungen für einen nachhaltigen, erfolgreichen Fortgang eines ISMS nachdrücklich bestätigt werden.

Das Marktforschungsunternehmen Gartner hat die objektiv größten Informationssicherheitsrisiken der nächsten zehn Jahre vorgestellt[476]. Laut dem Report werden besonders gezielte Attacken, Spyware und Identitätsdiebstahl in den Vordergrund treten. Neben diesen externen Angriffen steigt laut einer Studie[477] von CA ebenso die Zahl der internen Risiken. Für immer mehr Unternehmen stellen unsichere Kennwörter, mangelnde Nachvollziehbarkeit von Zugriffsberechtigungen, nicht gelöschte Benutzerkonten ausgeschiedener Mitarbeiter, sowie die Vielzahl an Benutzerkonten und den damit verbundenen hohen Administrationsaufwand Sicherheitsprobleme dar. Zudem erhöht sich aufgrund der wachsenden Compliance-Anforderungen auf die Geschäftsführung bzw. IT-Leitung der Druck, das interne Sicherheitsniveau zu erhöhen. Werden außerdem Technologien wie *starke* Authentifizierung, Single-Sign-On, Benutzer- und Berechtigungsmanagement in Betracht gezogen, dann ist Identitätsmanagement die passende Lösung für diese Aufgaben. Im folgenden, zweiten Kapitel wird der Themenkreis „Digitale Identität und Privacy“ erläutert.

[476] Vgl. http://www.gartner.com/2_events/conferences/sec7i.jsp [26. Feber 2007]
[477] Vgl. http://www3.ca.com/de/Press/PressRelease.aspx?CID=95335 [27.März 2007]

Der Autor will diesem Fazit eine persönliche Aussage zum Thema Informationssicherheit beifügen. Alle Diskussionen, Beiträge, Initiativen, Lösungen etc. hinsichtlich Informationssicherheit haben ihre Berechtigung. Doch scheint es, dass – zumindest dem subjektiven Empfinden und Erfahrungen des Autors nach – aufgrund eines gewissen Marktmomentums der Begriff Informationssicherheit überstrapaziert und teilweise sogar mißbräuchlich verwendet wird. Marktschreierisch werden Lösungen für Bedrohungen und Sicherheitslücken mit medialer Verstärkung angeboten und forciert, die vorderhand noch gar nicht existieren bzw. künstlich konstruiert werden. Es empfiehlt sich daher, genau zu hinterfragen, welches Maß an Informationssicherheit für (s)ein Unternehmen erforderlich ist.

2 DIGITALE IDENTITÄT UND PRIVACY

2.1 PROBLEMSTELLUNG UND HERAUSFORDERUNG

Während in den bisherigen Ausführungen die Datensicherheit im Vordergrund stand, geht es in diesem Abschnitt um den Schutz personenbezogener Daten im informationellen Umfeld. Datensicherheit stellt die Basis für den Datenschutz dar. Datenschutz betrifft gesetzliche Regulierungen, die das Recht der Individuen auf Privatheit (engl. *Privacy*) und die legitimen Interessen des Staates und anderer Organisationen gegeneinander abwägen [Fleissner, 2005, S 4]. Die digitale Identität (engl. *Identity*) bildet den formalen Rahmen für Privatheit: „*Privacy is the protection of the attributes, preferences and traits associated with an identity from being disseminated beyond the subject's needs in any particular transaction.*“ [Windley, 2005, S 11]. Weiters erklärt Windley die Zusammenhänge zwischen Informationssicherheit, Privatheit und Identität folgendermaßen: „*In a circular manner, privacy is built upon a foundation of good information security, which is, in turn, dependent on a good digital identity infrastructure.*“

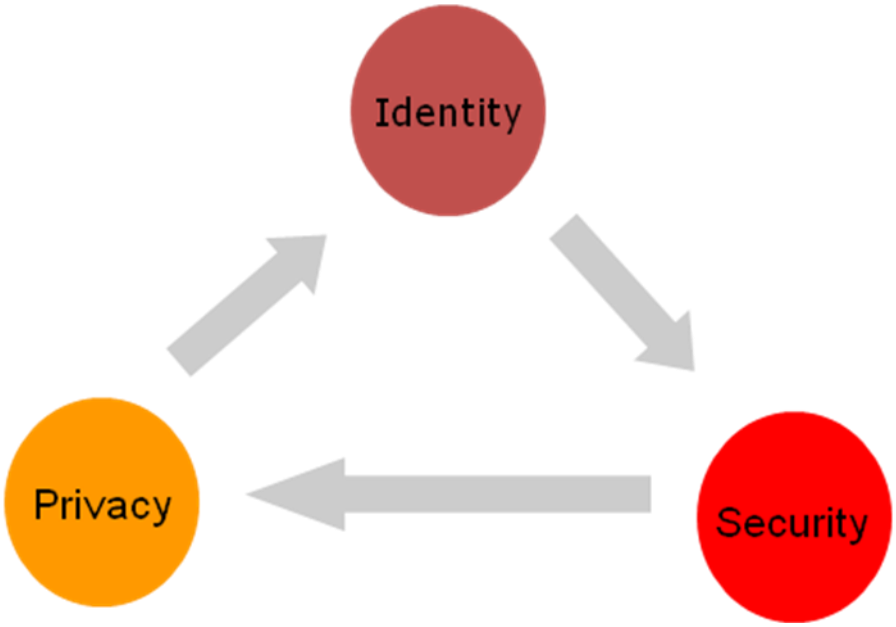


Abbildung 34: Das "identity, security, privacy triangle"

Dementsprechend sind die Anforderungen hinsichtlich Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit an den Datenschutz in Analogie zu jenen der Informationssicherheit zu sehen (siehe *1.2.2 Anforderungen an die Informationssicherheit*). *Fleissner* [Fleissner, 2005, S 4f] verfeinert und ergänzt diese Grundanforderungen mit Fokus auf den Schutz personenbezogener Daten und formuliert die „Fünf Dimensionen der Verlässlichkeit“.

Abbildung 35: Fünf Dimensionen der Verlässlichkeit

Zehentner [Zehentner, 2002, S 10] definiert zudem noch Verdecktheit[478] (auch: Steganographie) und Erreichbarkeit[479] als Anforderungen.

Wörndl [Wörndl, 2003, S 23f] gruppiert die einzelnen Elemente in Schutzziele. Anonymität und Pseudonymität werden der Kategorie „Identitätsziele" zugeordnet. Zu den „Vertraulichkeitszielen" gehören neben Vertraulichkeit auch Verdecktheit und Unbeobachtbarkeit. Integrität, Verbindlichkeit und Zurechenbarkeit ergeben die „Absicherungsziele". Noch nicht berücksichtigt ist ein bei der Verwaltung von personenbezogenen Daten wichtiger Gesichtspunkt: Wie weiß der Benutzer, welches Attribut (z. B. Name, Adresse – siehe *2.2.1 Digitale Identität*) zu irgendeinem Zeitpunkt überwacht wird? Dies kann als „Transparenzziel" bezeichnet werden und ergibt sich auch aus den rechtlichen Rahmenbedingungen für den Datenschutz (siehe *1.7.3.1 Datenschutz, 2.3.2 Rechtliche Belange*). All diese Aspekte betrachten eher die Absicherung gegenüber unbefugten Dritten als die Verwendung von Profilen beim Benutzer der Informationen. Eine Berechtigung zum Zugriff auf Daten wird als Autorisierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*) bezeichnet und durch ein Zugriffskontrollsystem (siehe *3.5.1 Anforderungen*) umgesetzt. Die besprochenen Kategorien lassen sich wie folgt zusammenfassen:

- Absicherungsziele: Integrität, Verbindlichkeit, Zurechenbarkeit.
- Autorisierungsziele: Bereitstellung einer geeigneten Zugriffskontrolle.

[478] Unautorisierten bleibt nicht nur der Inhalt, sondern auch die Existenz einer Kommunikation verborgen (siehe 1.7.2.1 Kryptologie). Verdecktheit ist der Vertraulichkeit zuzurechnen.
[479] Durch Erreichbarkeit wird sichergestellt, dass eine Instanz kontaktiert werden kann. Erreichbarkeit ist der Verfügbarkeit zuzurechnen.

- Identitätsziele: Anonymität, Pseudonymität.
- Transparenzziele: Überwachungs- und Kontrollfunktionen für Benutzer.
- Vertraulichkeitsziele: Vertraulichkeit, Verdecktheit, Unbeobachtbarkeit.

Diese Ziele müssen sowohl gegenüber dem Kommunikationspartner als auch gegenüber potentiellen Dritten betrachtet werden. In der Literatur wird in diesem Zusammenhang von *mehrseitiger Sicherheit* gesprochen [Wörndl, 2003, S 22f]. Die Schutzziele stehen in Wechselwirkung zueinander. Zum Beispiel wird Vertraulichkeit durch Unbeobachtbarkeit impliziert, Verdecktheit verstärkt Anonymität und diese ist komplementär zu Zurechenbarkeit.

Beim Datenschutz bzw. Schutz der Privatsphäre geht es um die Abwägung zwischen den „*Interessen von Privatpersonen, einen intimen Bereich in Anspruch nehmen zu können, in dem sie keine Eingriffe dulden*“ und den „*Interessen der staatlichen und privaten Institutionen, zum Zwecke der Erfüllung ihrer Aufgaben Informationen zu sammeln und zu verarbeiten*“ [Fleissner, 2005, S 15]. Das bedeutet für den Anwender, dass er selbstbestimmt über seine Daten verfügen können sollte. Der vertrauenswürdige Umgang mit den Daten setzt vollständige Transparenz für ihn selbst bei strikter Geheimhaltung gegenüber Dritten voraus. Welche Daten in welcher Weise und an wen weitergegeben werden, obliegt allein dem Anwender. An diesen Grundsätzen müssen sich Sicherheitslösungen ausrichten[480].

Realität ist, dass im Alltag laufend persönliche Daten über die Menschen gesammelt werden[481]. Videokameras an öffentlichen Plätzen und *Section Control*[482] auf der Autobahn halten den Tagesablauf fest. Mit Kundenkarten, *GPS*[483], Handy-Gesprächen und Chipkarten (z. B.: E-Card) werden eine Reihe von Informationen preisgegeben. Vor allem durch die Verwendung des Mediums Internet – besuchte Seiten, durchgeführte Tätigkeiten (Onlinebanking, Käufe etc.), E-Mail, Teilnahme an Diskussionsforen, Blogging etc. – werden viele digitale Spuren hinterlassen. All das führt zunehmend mehr zu einem Verlust der Privatheit, wodurch der viel zitierte „gläserne Mensch“ entsteht. Für aussagekräftige Personenprofile, aggregiert aus den Datenspuren, gibt es eine Menge von Interessenten [Stamer, 2005, S 3]:

- Marktforschungs- und Marketing-Unternehmen, die an Benutzerprofilen interessiert sind, um Angebote speziell auf bestimmte Nutzergruppen zuzuschneiden oder Benutzerprofile zu verkaufen.

[480] http://www.bsi.de/sichere_plattformen/trustcomp/infos/tcgi.htm [2. Juni 2007]
[481] Vgl. http://www.ammering.org/ [17. April 2007]; http://www.quintessenz.at/ [17. April 2007]; http://stop1984.com/ [17. April 2007]; http://www.ard.de/ratgeber/special/-/id=322978/7kqsc8/index.html [17. April 2007]
[482] http://www.vignette.at/index.php?idtopic=95 [16. April 2007]
[483] Unter GPS (steht für: Global Positioning System) wird ein satellitengestütztes Navigationssystem verstanden.

- Betreiber von Webseiten, die wissen möchten, warum und wie oft Benutzer ihre Webseite besucht haben, um ihr Angebot zu verbessern.
- Strafverfolger, die im Netz nach Straftätern fahnden oder diese überwachen wollen.
- Kriminelle, die sensible Informationen (z. B.: Passwörter, Kreditkartennummern) in Erfahrung bringen wollen oder Malicious Code einschleusen möchten.

„*Da das Internet niemandem gehört, unsicher, dezentral, unkontrolliert und frei zugänglich ist, muss dem Nutzer die Möglichkeit gegeben werden, dass seine Daten nicht an unbefugte Dritte weitergereicht werden.*“ [Rickert, 2004, S 24]. Die Vielfalt der Datenspuren und die Möglichkeit der Verkettung – „*dazu noch in einem globalen Raum ohne weltweite Datenschutzbestimmungen mit entsprechender Durchsetzbarkeit – sind für den Einzelnen nicht transparent und überfordern ihn in ihrer Komplexität.*“ [Köhntopp, 2000, S 44]

Das Recht auf Privatheit steht seit jeher im Zentrum des Persönlichkeitsschutzes. Als Recht auf Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung*) über die Preisgabe personenbezogener Informationen ist es eine wesentliche Bedingung der freien Entfaltung der Persönlichkeit. Inhalt und Aufgabe des Privatheitsschutzes haben sich allerdings im Zeitalter der Informationsgesellschaft grundlegend verändert. Personenbezogene Informationen, zu denen neben den Einzelangaben über persönliche Verhältnisse einer Person auch deren Persönlichkeitsattribute, wie Name, Bild oder Stimme zu zählen sind, erlangen heute zunehmend wirtschaftliche Bedeutung – die Persönlichkeit wird zur Ware. Eine Verletzung des Rechts auf Privatheit betrifft damit neben ideellen Integritätsinteressen häufig auch materielle Verwertungsinteressen [Amelung, 2002, Abstract]. Die digitale Vernetzung verändert die Rahmenbedingungen der zum Teil über Jahrhunderte gewachsenen gesetzlichen und moralischen Regeln im Umgang mit Schrift, Bild und Ton. Davon betroffen sind Datenschutz und Urheberrecht, Zensur und Kontrolle sowie Zugang zu und Austausch von elektronisch kodifizierten Sendungen aller Art[484].

Wissenschaftler des *Fraunhofer-Instituts für System- und Innovationsforschung*[485] haben in einer Studie[486] (November 2006) die Chancen und Risiken intelligenter Umgebungen, sogenannter *Ambient Intelligence* (kurz: *AmI*), in Hinblick auf ihren Datenschutz untersucht, wie weit er für den Erfolg oder Misserfolg von AmI entscheidend ist. Hinter Ambient Intelligence steht ein weit reichendes Konzept, das die heutige nutzerorientiert arbeitende Alltagstechnologie der gesamten informationsverarbeitenden Welt in sich vereint. Die Vernetzung unsichtbarer und allgegenwärtiger Computer erleichtert das Sammeln und Verknüpfen von Daten zu Persönlichkeitsprofilen. Als

[484] Vgl. http://www.capurro.de/infoger.htm [12. April 2007]
[485] http://www.isi.fraunhofer.de/ [12. April 2007]
[486] Vgl. http://www.isi.fraunhofer.de/pr/2006de/pri16/pri16.htm [12. April 2007];
http://swami.jrc.es/pages/index.htm [12. April 2007]

Quintessenz des Projekts wurden Handlungsempfehlungen für Politik, Wissenschaft und Wirtschaft erarbeitet, insbesondere zum Schutz der Privatsphäre: Eine flächendeckende Aufklärung über die Möglichkeiten und Risiken bestehender und neuer Technologien ist unabdingbar. Die teilweise überalterten Datenschutzgesetze sollten an die heutigen technischen Möglichkeiten angepasst werden.
In diesem Kapitel sollen Technologien, welche die Privatsphäre betreffen, identifiziert und Antworten gegeben werden, wie insbesondere die informationelle Freiheit gewahrt bzw. ausgebaut werden kann.

2.2 GRUNDLAGEN

2.2.1 DIGITALE IDENTITÄT

Der Begriff der Identität wurde in der Literatur [Köhntopp, 2000; Windley, 2005; et al.] vielfach von philosophischen, psychologischen oder soziologischen Gesichtspunkten aus betrachtet. Köhntopp etwa definiert Identität folgendermaßen: „*Identität ist aus soziologischer Sicht das dauernde innere Sich-Selbst-Gleichsein, die Kontinuität des Selbsterlebens eines Individuums, die im wesentlichen durch die dauerhafte Übernahme bestimmter sozialer Rollen und Gruppenmitgliedschaften sowie durch die gesellschaftliche Anerkennung als jemand, der die betreffenden Rollen inne hat bzw. zu der betreffenden Gruppe gehört, hergestellt wird*." Für Windley sind zwei Elemente entscheidend: „*The identity has two elements: a sense of belonging and a sense of being separate*."
Technisch gesehen repräsentiert eine digitale Identität einen Ausweis eines Subjekts/Objekts mit (persönlichen) Attributen. Der Ausweis sorgt gemäß den Anforderungen an den Datenschutz (siehe *1.2.2 Anforderungen an die Informationssicherheit* und *Abbildung 35: Fünf Dimensionen der Verlässlichkeit*) dafür, dass die Person oder das Objekt als echt und vertrauenswürdig identifiziert werden kann. Eine digitale Identität entsteht erst dann, wenn ein Subjekt/Objekt mindestens ein Authentifizierungsmerkmal wie zum Beispiel Passwort, Fingerprint oder Zertifikat besitzt[487].
Ausprägungen eines Subjekts/Objekts können sein:

1. Physische Person (Mitarbeiter, Kunde, Lieferant).
2. Juristische Person (Lieferant, Partner, Kunde).
3. Virtuelle Person (*Avatar*, Dienst).
4. Objekte (Gerät, IT-System).

„*A Digital Identity consists of two parts: 1. Who one is (identity, short: ID) and 2. The credentials that one holds (attributes of that identity). These credentials define a digital Identity, and they can be quite*

[487] Vgl. http://www.iam-wiki.org/Digitale_Identit%C3%A4t [12. Mai 2007]

varied, of widely differing value, and have many different uses. The full digital Identity is quite intricate and has legal as well as technical implications."[488]

Die einfachste Form der digitalen Identität besteht aus einer ID (z. B.: Benutzername) und einem Authentifizierungsgeheimnis (z. B.: Passwort).

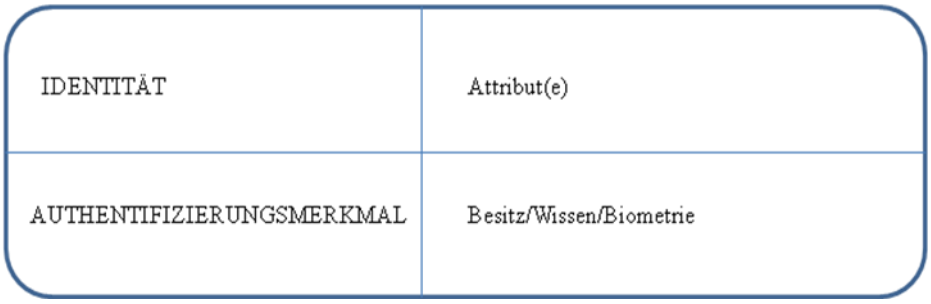


Abbildung 36: Komponenten einer digitalen Identität

Attribute (Teilmengen) des Subjekts/Objekts können sein: Familienname(n), Vorname(n), biometrische Merkmale, Pseudonym(e), Akademische(r) Titel, Wohnadresse(n), Geburtstag, Geburtsort, ZMR-Zahl, E-Mail-Adresse(n), Telefonnummer(n), publizierte Webseite(n), besuchte Webseite(n) (mit Verweildauer), Session-Key(s), IP-Adresse(n), Skype-Name(n), ICQ-Nummer(n), Blog-URL(s), Public Key(s), Kreditkartennummer(n), Bankverbindung(en), Sozialversicherungsnummer, E-Card-Nummer, Blutspendekartennummer, Gesundheitszustand, Interessensgebiet(e), Vorliebe(n), politische Einstellung, Religionsbekenntnis, Familienstand, Staatsbürgerschaft, Nummer(n) von Vorteilskarten (z. B.: Einkauf), Mitgliedschaft(en) bei Organisation/Gewerkschaft/Verein, Arbeitgeber, Benutzername(n), Personalnummer, Abteilung, Schulausbildung, beruflicher Werdegang etc.

Nähere Erläuterung zum Tupel Authentifizierung siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*.

Digitale Identitäten sind das Fundament für die Abwicklung von Geschäftstätigkeiten über das Internet (E-Business). Ohne die Kenntnis und das Vertrauen in die Identität von Partnern gibt es kein elektronisches Geschäft. Digitale Identitäten sind nicht nur für die elektronische Geschäftsabwicklung im Unternehmen und zwischen Unternehmen, sondern für viele (neue) Anwendungsfelder essentiell. Sie bilden demnach wesentliche Voraussetzungen für den Bankverkehr (E-Banking), im Gesundheitsbereich (E-Health), bei digitalen Behördengängen (E-Government) (siehe *2.4.7 Bereichsspezifisches Personenkennzeichen und Bürgerkarte im E-Government*) oder bei der Wahrnehmung von Bürgerrechten via elektronischer Kanäle (E-Voting)[489]. *Corporate Governance*[490]

[488] Vgl. http://www.digitalidworld.com/local.php?op=view&file=aboutdid [18. April 2007]
[489] Vgl. http://www.itsolution.at/DE/news/collection/2006/061106-Digitale_Identitaet.html [18. April 2007]
[490] Z. B.: Der Österreichische Arbeitskreis für Corporate Governance hat mit dem Österreichischen Corporate Governance Kodex ein internationalen Standards entsprechendes Regelwerk für die verantwortungsvolle

(Risikomanagement, gesetzliche Bestimmungen) lässt sich nur erfüllen, wenn sichergestellt ist, *wer wann was gemacht hat*[491] (siehe Verbindlichkeit *Abbildung 35: Fünf Dimensionen der Verlässlichkeit*).

Der Zweck digitaler Identitäten besteht darin, bestimmte Attribute für bestimmte Situationen bereit zu stellen. Das Attribut E-Mail in Verbindung mit dem Authentifizierungsmerkmal Passwort reicht in der Regel für eine Anmeldung bei einem Webdienst aus. Erstellt der Benutzer darüber hinaus noch Attribute (Wohnadresse, Telefon, Kreditkarteninformation etc.) entsteht ein Profil, das für Webportale (Wareneinkauf, Online-Auktionen etc.) verwendet werden kann. Zudem können Webdienste ihrerseits digitale Identitäten mit Attributen anreichern, die nicht durch den Benutzer eingegeben werden. Ein solches Attribut kann beispielsweise das Interessensgebiet des Benutzers sein, welches aufgrund von via Webdienst gekauften Produkten ermittelt wird (siehe *2.2.4 Personalisierung*) [Rickert, 2004, S 18f].

Eine Person kann unterschiedliche Rollen ausfüllen (z. B.: beruflich und privat) und somit mehrere Identitäten gleichzeitig annehmen. Der – oft unbewusste – Wechsel der Identität lässt sich auch in der realen Welt beobachten: Beispielsweise kann eine Person tagsüber die Rolle als Angestellter einer Firma ausüben, danach anonym Einkäufe tätigen und am Abend die private Identität in der Familie einnehmen [Wörndl, 2001, S 5]. Eine Abbildung der gesamten realen Identität einer Person in der realen Welt in eine digitale Identität ist nicht möglich. Soziale Aspekte wie Gefühle oder Gedanken sind nicht abbildbar. *Floyd* [Floyd, 1997, S 237f] beschreibt diesen Umstand als eine „*operationale Rekonstruktion*“ bzw. als „*Reduktion von Vorgängen auf das Wirken von Operationen sowie die Nachbildung der Vorgänge durch Verknüpfung von Operationen.*“ Nur zweckmäßige und wiederverwendbare Daten (Namen, Adresse, Kreditwürdigkeit, Interessensgebiete etc.) werden in digitalen Identitäten gespeichert [Rickert, 2004, S 18]. Ferner unterscheidet sich die digitale von der realen Identität dadurch, dass sich aus einer Teilmenge der digitalen Identität wieder eine digitale Identität erzeugen läßt.

Identitäten können in folgenden Formen auftreten [Rickert, 2004, S 20]:

- *Leere Identität* (*=Anonymität*): Eine leere Identität enthält keine Attribute. Eine vollständige Anonymität ist jedoch schwer zu erreichen (siehe *2.2.3 Anonymität*).
- *Pseudo-/Teilidentität (=Pseudonymität)*: ist eine von einer Person selbst gewählte Repräsentation ihrer selbst. Die Person hat von ihrem Recht auf individuelle Selbstbestimmung Gebrauch gemacht und nutzt ein Pseudonym, um sich zu präsentieren. Die Pseudoidentität spiegelt eine Teilidentität einer Person wider, die meist ein Interessensgebiet oder Wunschbild der Person

Führung und Leitung von Unternehmen in Österreich geschaffen. http://www.corporate-governance.at/ [18. April 2007]

[491] Vgl. http://www.kuppingercole.de/ [18. April 2007]

repräsentiert (Onlinespiele, Diskussionsforen etc.). Pseudoidentitäten unterliegen dann dem Datenschutz, wenn die Identität bestimmt oder bestimmbar ist (siehe *1.7.3.1 Datenschutz*).

- *Vollständige Identität*: definiert eine Person mit all ihren Werten. Sie stellt das technische Ideal dar und enthält alle Attribute einer Identität. Die (persönliche) Identität besteht aus persönlichen Daten jeglicher Art und ist datenschutzrechtlich geschützt.

Die Übergänge zwischen leerer Identität, Pseudoidentität und vollständiger Identität sind fließend. Es ist wichtig, nicht automatisch alle Attribute einer Identität preis zu geben, sondern immer nur jene, die der Kommunikationspartner verlangt. Diese Form des Datenaustausches wird als *datensparsam* (siehe *2.4.2.2 Datensparsamkeit*) bezeichnet.

Ein Praxisbeispiel aus China zeigt[492], wie hinsichtlich Identität Transparenz geschaffen werden kann. Die chinesische Regierung hat eine frei abrufbare Datenbank[493] geschaffen (Ende 2006), wo alle 1,3 Milliarden Chinesen erfasst sind. Die Einwohner Chinas werden darin mit ihrem Namen, ID-Kartennummer und Foto verzeichnet. Der Abruf kann via Web bzw. SMS erfolgen. Jedermann ist berechtigt, die Angaben einer Person zu überprüfen. Damit soll unter anderem der Identitätsbetrug eingedämmt werden.

Weiterführende Abhandlungen zu diesem Thema werden an späterer Stelle erläutert (siehe *2.2.2 Pseudonymität*, *2.2.3 Anonymität*, *3.6.3 Von der Identität* zur Rolle).

2.2.1.1 Lebenszyklus einer Identität

Die Aussagen zum Lebenszyklus einer Identität (siehe *3.4.4.2.7 SPML*) gelten sowohl für Identitätsmanagementsysteme im betrieblichen Umfeld (siehe *3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*) als auch – vereinfacht – für den Benutzerzugang am Heim-PC [Windley, 2005, S 29].

[492] Vgl. http://futurezone.orf.at/it/stories/171149/ [19. Juni 2007]
[493] http://www.mps.gov.cn/cenweb/portal/user/anon/page/policeWeb_HomePage.page [11. Juni 2007]

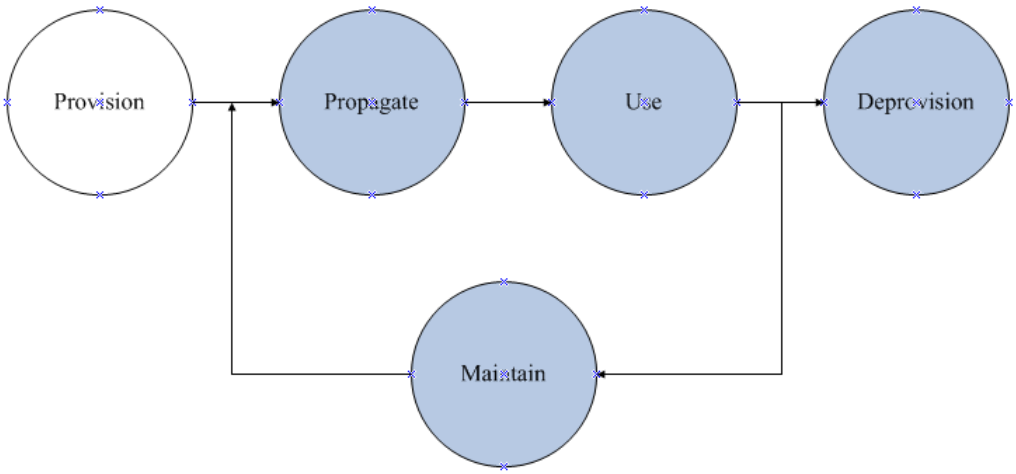


Abbildung 37: Lebenszyklus digitale Identität

Die Bereitstellung (engl. *Provisioning*) beschreibt den Prozess der Erstellung einer digitalen Identität mit Attributen und Berechtigungen (Name, Ort, E-Mail, Telefonnummer, systemspezifische Merkmale etc.). Provisioning kann durch einen Administrator oder im Zuge eines sogenannten *Self-Service* durch den Benutzer selbst erfolgen. „*Zero-day start*" bezeichnet das rasche Zurverfügungstellen von Ressourcen für einen neuen Mitarbeiter. Dabei werden in der Regel auf verschiedenen Systemen (Personalinformation, Büroverwaltung, Hardwaremanagement, E-Mail etc.) durch Administratoren Benutzerkonten (engl. *Accounts*) angelegt. Für den privaten Gebrauch ist es üblich, sich für Services auf diversen Webseiten selbst zu registrieren.

Beim Ausbringen (engl. *Propagate*) wird die digitale Identität für verschiedene Systeme verfügbar gemacht. Eine Vereinfachung auf ein gemeinsames Identitätsverzeichnis stellt hohe technische Anforderungen dar (siehe *3.4.1 Verzeichnistechnologien*).

Während der Verwendung (engl. *Use*) können sich die Attribute einer Identität im Laufe der Zeit ändern.

Beim Verwaltungsprozess (engl. *Maintain*) werden bei Veränderungen von Subjekten/Objekten die Inhalte und Werte der Attribute aktualisiert: Jobwechsel einer Person, Standortwechsel eines Laserdruckers etc. Die Verwaltung der Identitäten ist eine der kostenintensivsten Aktivitäten einer IT-Abteilung (siehe *3.6.2 Aufteilung der Verwaltung der Benutzerdaten*). Allein das Passwortmanagement verursacht Kosten von 300 Dollar pro Benutzer und Jahr [Stiller-Erdpresser, 2005, S 5] bzw. beansprucht 16 Minuten pro Benutzer und pro Tag an (Helpdesk-) Zeit[494].

Das Entfernen (engl. *Deprovisioning*) einer Identität beschließt den Lebenszyklus. Dieser Vorgang wird vielfach vernachlässigt, die so entstehenden „Karteileichen" erhöhen zum einen den

[494] Vgl. http://www.cryptoshop.com/index.php [2. Juni 2007]

Administrationsaufwand, zum anderen stellen sie aus informationssicherheitstechnischer Sicht eine Bedrohung dar.

2.2.2 PSEUDONYMITÄT

Pseudonyme (auch: Pseudoidentitäten oder Nicknames) werden zum Schutz von Personen vergeben, deren Identität beliebigen Dritten nicht bekannt werden soll bzw. darf, deren Identität über das Pseudonym jedoch einem bestimmtem Personenkreis bekannt sein muss. Selbst wenn Pseudonyme aus alphanumerischen Symbolfolgen bestehen, gibt es einen Unterschied zwischen Pseudonym und Symbolfolge. Symbole, wie die Personalnummer, werden zur eindeutigen Identifizierung eingesetzt und sind grundsätzlich in beide Richtungen zuordenbar. Pseudonyme stellen dahingehend eine unidirektionale Zuordnung von Identität und Pseudonym her, die nur von einem berechtigten Personenkreis genutzt werden kann[495].

Bei der Betrachtung von Pseudonymen sind insbesondere folgende drei Eigenschaften von Bedeutung [Köhntopp, 2000]:

- Zuordnung/Zurechenbarkeit: Wie wird ein Pseudonym einer Person zugeordnet? Kann das Pseudonym frei gewählt werden? Ist es auf eine andere Person übertragbar?
- Verkettbarkeit: Ist es ersichtlich, ob mehrere Transaktionen von dem gleichen Benutzer getätigt wurden? (Anm.: Ist keine Verkettung möglich, spricht man von Anonymität.)
- Aufdeckbarkeit: Wer kann wie die Zuordnung eines Pseudonyms zu einer Person aufdecken?

Diese Eigenschaften spielen bei den verschiedenen Ausprägungen von Pseudonymität eine Rolle.

Es gibt eine Reihe von Abstufungen bei Pseudonymen [Rickert, 2004, S 26f]. Auf der einen Seite steht die Anonymität und auf der anderen Seite die vollständige Identifizierung der Identität des Benutzers.

Hinsichtlich Datenschutz ist die Verkettbarkeit relevant [Wörndl, 2003, S 8f]:

- Preisgabe der/einer Identität.
- Personen-Pseudonym: z. B.: Nickname.
- Rollen-Pseudonym: z. B.: eine Rolle in einem Unternehmen.
- Beziehungs-Pseudonym: ein Pseudonym pro Kommunikationspartner.
- Transaktions-Pseudonym: ein neues Pseudonym für jede Transaktion.

Grundsätzlich gilt: Je mehr Attribute einer Identität preisgegeben werden, umso *besser* wird der Komfort für den Benutzer (z. B.: das Wiedererkennen des Users auf einer Webseite erspart erneute Dateneingabe – siehe *2.2.4 Personalisierung*) und umso *schwächer* der Schutz seiner Daten. Die Anonymität des Pseudonyminhabers hängt davon ab, wie viel unmittelbar über die Zuordnung des

[495] Vgl. http://www.bsi.bund.de/literat/anonym/wasist.htm [18. April 2007]

Pseudonyms zur Person bekannt ist und inwieweit sich ein Personenbezug durch Beobachtung der Pseudonymverwendung, d. h. die Verkettung einzelner Aktionen, erschließen lässt. Generell bieten sowohl Rollen- als auch Beziehungs-Pseudonyme stärkere Anonymität als Personenpseudoyme. Die stärkste Anonymität lässt sich mit Transaktions-Pseudonymen erreichen [Köhntopp, Pfitzmann, 2001, S 3].

Ein bekanntes Beispiel für ein digitales Pseudonym ist ein selbst generierter Public Key, wie es beispielsweise bei PGP zutrifft (siehe *1.7.2.1 Kryptologie*) [Pfitzmann, Hansen, 2005, S 18].

Informationstechnik (siehe *2.4.6 Pseudonym Surfen und Mailen*) kann hier unterstützen, indem je nach Situation und Kontext unterschiedliche Pseudonyme statt der vollständigen Identität verwendet werden. Anwendung finden Pseudonyme im Internet bei diversen Diensten (z. B.: Chats, Diskussionsforen, Versteigerung).

Im Rahmen dieser Arbeit soll überlegt werden, wie Pseudonyme im betrieblichen Umfeld zur Anwendung kommen können (siehe *3.6.4.2 Private Rolle*).

2.2.3 ANONYMITÄT

Die Identität einer an einem anonymen Vorgang beteiligten Instanz ist nicht bestimmbar, weil sie entweder

- den anderen beteiligten Instanzen nicht bekannt ist (*Nichtbekanntsein*),
- gegenüber den anderen beteiligten Instanzen nicht in Erscheinung tritt (*Nichtgenanntsein*) oder
- innerhalb des anonymen Vorgangs ohne erkennbaren Namen agiert (*Namenlosigkeit*)[496].

Pfitzmann [Pfitzmann, Hansen, 2005, S 5] beschreibt Anonymität als *„[...] state of being not identifiable within a set of subjects, the anonymity set*". Das bedeutet, dass ein anonymer Benutzer ohne Identitätsattribute gegenüber einem Dienst auftritt. Damit kann der Dienst den Benutzer nicht identifizieren. Anonymität ist somit die geeignetste Form des Schutzes vor Missbrauch personenbezogener Daten [Rickert, 2004, S 24f].

Ursprünglich basierte das Internet auf der Annahme, dass der Benutzer anonym bleibt. Die meisten Internetuser fühlen sich bei ihrer Arbeit anonym und unbeobachtet. Sie ahnen in der Regel nicht, wie viele Spuren sie hinterlassen, die auf ihre Person zurückführbar sind. Im Alltag ist eine völlige Anonymität schwer umsetzbar (siehe *2.3 Privacy*). Zwischen Identität und Anonymität gibt es viele Abstufungsmöglichkeiten. Der Grad der Anonymität wird dadurch bestimmt, ob es möglich ist bzw. wie leicht es ist, auf Teile der Identität zu schließen[497] (siehe *2.2.2 Pseudonymität*).

In einigen Anwendungsbereichen, wie z. B. bei anonymen Abstimmungen oder Wahlen, bei der Inanspruchnahme von seelsorgerischen oder psychologischen Beratungsangeboten, beim Abruf von

[496] Vgl. http://www.bsi.de/literat/anonym/wasist.htm [22. Mai 2007]

medizinischen Daten, bei der Diskussion von umstrittenen Themen oder beim Aufdecken von Missständen hat die Gewährleistung von Anonymität eine besonders große Bedeutung. Der Wunsch nach Anonymität kann auf bestimmte Phasen einer Anwendung beschränkt sein. Wenn beispielsweise bei einer Auktion die Abgabe der Angebote möglichst allen gegenüber anonym sein soll, gilt dies jedoch nicht mehr für den Moment, in dem der Auktionszuschlag gegeben wird. Anonymität reicht dann nicht aus, wenn verschiedene Nutzungen eines Teilnehmers verkettet und in Beziehung gesetzt werden können bzw. sollen. Dies ist etwa beim E-Commerce der Fall, wenn sich ein Güteraustausch nicht unmittelbar vornehmen lässt und die Möglichkeit bestehen soll, die andere Partei zur Rechenschaft ziehen zu können [Köhntopp, 2000, S 46f].
Die Idee, die hinter all diesen für den Privatbereich eines Anwenders angestellten Überlegungen steckt, soll als Basis für die Anwendbarkeit in einem Unternehmensumfeld genommen werden.

2.2.4 PERSONALISIERUNG

In diesem Zusammenhang wird unter Personalisierung folgendes verstanden: „*Abhängig von den zur Verfügung stehenden Benutzerinformationen werden aus einer Menge anzubietender Informationen auf Websites nur diejenigen ausgewählt und dem Benutzer präsentiert, die entsprechend dem Benutzerprofil für den Anwender interessant sind*.“ [Zehentner, 2002, S 5].
Durch Personalisierung wird für den Benutzer auf Basis seiner persönlichen Vorlieben und Abneigungen, Bedürfnisse und Fähigkeiten eine persönliche Umgebung geschaffen. Bei häufigen Besuchen stellt es einen gewissen Komfort dar, wenn das Gesuchte ohne Navigation angezeigt wird. Auf diese Weise wird eine Anbieter-Benutzer-Beziehung aufgebaut, welche eine höhere Verweildauer, Zufriedenheit, Besuchshäufigkeit und Kundenbindung zur Folge hat[498]. Im Bereich des E-Commerce können durch die Personalisierung die Angebotsgestaltung und der Kundenservice optimiert werden. In Betrieben hat Personalisierung den Vorteil, dass Informationen gezielt an den gewünschten Benutzerkreis weitergegeben werden können (Stichwort: Wissensmanagement).
Zunächst muss der Bezug zum Anwender hergestellt werden. Dies kann entweder durch Beobachtung der Aktionen eines Benutzers (*implizite Personalisierung*) oder durch Angabe von Präferenzen durch den User selbst geschehen (*explizite Personalisierung*). In beiden Fällen wird ein Benutzerprofil aufgebaut, welches in der Folge ausgewertet werden kann. Bei einer Personalisierung werden oftmals Empfehlungssysteme (engl. *recommender systems*) verwendet, die meist auf einer der folgenden Techniken basieren [Wörndl, 2003, S 14; Zehentner, 2002, S 6f]:

- Inhaltsbasiertes Filtern: Inhalte, wie z. B. Dokumente, werden mit Schlüsselwörtern versehen, die mit – explizit erstellten oder implizit abgeleiteten – Interessen eines Benutzers verglichen werden.

[497] Vgl. http://www.bsi.bund.de/literat/anonym/wasist.htm [18. April 2007]
[498] Vgl. http://www.contentmanager.de/magazin/artikel_12_personalisierung_von_websites.html [7. Juni 2007]

- Kollaboratives Filtern: Es wird versucht, Benutzer mit ähnlichen Interessen zu finden und abzugleichen, z. B.: bei Onlineshops wie Amazon.
- Regelbasiertes Filtern: Die Generierung von Empfehlungen geschieht auf Basis von benutzerspezifischen Regeln.
- Suchweg-Verkürzung: Öfter verfolgte Links werden höher bewertet. Auf diese Art wird die Dauer der Navigation zu mehr benötigten Informationen verkürzt.

In allen Fällen werden verschiedene Informationen über den Benutzer aus dessen Profil benötigt. Unabhängig davon, ob ein Benutzer seine persönlichen Daten selbst bereitstellt oder ob bestimmte automatisierte Mechanismen zur Datenkollektion Verwendung finden, die Weiterverwendung dieser Daten von Internetdiensten sowie deren Weitergabe an andere Dienstanbieter muss der Benutzer selbst bestimmen können [Zehentner, 2002, S 7].

2.2.5 DATA MINING

Data Mining spielt eine wichtige Rolle bei der Verarbeitung von personenbezogenen Daten [Rickert, 2004, S 27f]. Hinterlässt ein Benutzer im Internet Spuren und ist es möglich, diese miteinander in Beziehung zu setzen, entstehen entsprechend detaillierte Profilinformationen über den Benutzer. Das Sammeln von Daten zu einer Identität führt auch zu einem genaueren Bild der Person, die hinter dieser Identität steckt (z. B.: Interessen, Vorlieben). Das *Institut für Technikfolgen-Abschätzung* (kurz: *ITA*)[499] [Cas, Peissl, 2002, S 39 ff] versteht unter *Data Mining* Techniken zum Finden von interessanten und nützlichen Mustern und Regeln in großen Datenbanken. Ein wesentliches Kriterium des Data Mining ist es, dass unterschiedliche Verfahren eingesetzt werden, um Beziehungen innerhalb der Daten zu entdecken, deren Existenz von vornherein nicht bekannt ist. In der Praxis werden bei Data Mining sowohl vermutete Beziehungen aufgrund von Erfahrungen und Vorwissen überprüft als auch neues Wissen generiert. Ziel ist es, in einem großen Datenbestand die Elemente zu extrahieren, die für den Besitzer der Daten von Relevanz sind. Die durch Data Mining gewonnenen Informationen lassen sich üblicherweise den folgenden Typen zuordnen: Assoziationen, Sequenzen, Klassifikationen, Cluster und Prognosen. Ein typisches Beispiel für Assoziationen ist die Analyse von Warenkörben, gemeint ist die Bestimmung der Häufigkeit, mit der unterschiedliche Produkte gemeinsam gekauft werden. Bei den Sequenzen stehen Regelmäßigkeiten im zeitlichen Ablauf im Vordergrund, etwa die Anschaffung von Haushaltsgeräten nach dem Bezug einer neuen Wohnung. Klassifikationsregeln dienen dazu, neuen Objekten aufgrund der Eigenschaften bestehender Objekte Klassen zuteilen zu können: z. B.: das Zuordnen von Neukunden zu unterschiedlichen Kreditwürdigkeitseinstufungen auf Basis der Analyse der bestehenden Kundendatei. Beim Clustering wird im Unterschied zur

[499] http://www.oeaw.ac.at/ita/ [17. Juni 2007]

Klassifikation nicht von Klasseneinteilungen ausgegangen, die Gruppen werden anhand der Objekteigenschaften gebildet. Zusätzlich wird versucht, verständliche und verwertbare Beschreibungen der Gruppen und Klassifikationsregeln zu finden. Ein mögliches Ergebnis könnten beispielsweise Kundengruppen mit besonders hoher Neigung zum Anbieterwechsel sein, für die dann spezifische Kundenbindungsprogramme entwickelt werden. Prognosen stellen weniger eine eigene Kategorie von gewonnenen Informationen dar, sondern vielmehr eine auf die Zukunft ausgerichtete Art der Datenauswertung.

Die Einsatzgebiete von Data Mining sind aufgrund der Vielfalt der Verfahren und der Art der erhobenen Daten entsprechend mannigfaltig. Sie reichen von Mustern im Konsumentenverhalten, Assoziationen zwischen demographischen oder regionalen Charakteristika von Konsumenten, Vorhersagen über Reaktionen auf Werbekampagnen über die Identifikation von besonders loyalen oder ausgabefreudigen Konsumenten bis hin zum Aufdecken von Konsumenten, die höhere Kosten verursachen können, weil sie etwa Dienste besonders häufig in Anspruch nehmen werden oder weil sie ein höheres Risiko von Zahlungsunfähigkeit oder betrügerischen Verhaltens aufweisen. Das Wissen über die Kunden dient nicht nur dazu, deren Bedürfnissen entgegenzukommen, sondern es wird natürlich auch dazu genutzt, deren Verhalten im Sinne des Unternehmens zu steuern (siehe *2.2.4 Personalisierung*).

Personenbezogene Daten (Attribute im Sinne der digitalen Identität – siehe *2.2.1 Digitale Identität*) können in drei Klassen eingeteilt werden:

- Nicht-identifizierbare Daten sind Daten einer Person, die auch auf viele andere Personen zutreffen (z. B.: Vorname, Geburtstag).
- Schlüsseldaten sind einmalige Daten (z. B.: öffentliche Schlüssel), mit Schlüsseldaten können Aktionen von Personen verkettet werden.
- Identifizierende Schlüsseldaten sind einzigartige Daten, die eine Person eindeutig identifizieren (z. B.: Personalausweisnummer).

Je weniger identifizierbare Informationen herausgegeben werden, umso geringer ist die Wahrscheinlichkeit, dass Daten zu einem genauen Profil zusammengesetzt werden können. Es ist aber durchaus möglich, dass mehrere nicht-identifizierbare Daten zusammen ein Schlüsseldatum ergeben, beispielsweise die Menge aus Vorname, Nachname, Geburtstag und Geburtsort. Sind identifizierbare Daten herausgegeben worden, gibt es kaum Möglichkeiten, diese zu löschen (siehe *2.4.2.3.2 Löschen von Userdaten*).

Voraussetzung für die Anwendung von Data Mining-Techniken ist, dass Daten in möglichst umfassender Weise vorhanden sind. Die Zusammenführung aller nutzbaren Daten in einem vereinheitlichten Datenpool wird als *Data Warehousing* bezeichnet. Im Data Warehouse werden die

Daten losgelöst von ihrer ursprünglichen Verwendung gespeichert und für Data Mining-Analysen zugänglich gemacht. Data Warehousing umfasst drei Aufgaben:

- das zentrale Sammeln der in den einzelnen Abteilungen eines Unternehmens verarbeiteten und gespeicherten Daten,
- die Überführung dieser Daten in ein einheitliches Format,
- die Bereinigung der Daten von eventuellen Fehlern und Inkonsistenzen.

Die Integration der Daten in einem Data Warehouse ermöglicht auch die unternehmensweite Anwendung konventioneller Analyseverfahren und unterstützt den Einsatz von Wissensmanagement-Tools.

Die durch Data Mining gewonnenen Informationen lassen sich in vielfältiger Weise zur Optimierung unternehmerischer Prozesse und externer Beziehungen nutzen. In diesem Zusammenhang ist die Verwertung der extrahierten Informationen im Rahmen des Kundenbeziehungsmanagement (engl. *Customer Relationship Management*, kurz: *CRM*)[500] relevant.

Es gibt eine Reihe von Bereichen, in denen besonders viele Kundendaten anfallen. Diese Sektoren weisen daher ein entsprechend hohes Potenzial auf, die Daten im eigenen Interesse auszuwerten oder an andere Parteien weiterzugeben bzw. zu veräußern. Um den globalen Austausch von Kundenprofilen zu vereinfachen, wurde ein offener Standard spezifiziert. Der *Customer Profile Exchange* (kurz: *CPEX*)-Standard[501] ermöglicht zwar die Berücksichtigung von individuellen oder nationalen Vorgaben zum Schutz der Privatsphäre, stößt aber wegen der grundlegenden Zielsetzung und der Effekte auf Kritik von Datenschutzorganisationen. Der globale Austausch von Kundenprofilen widerspricht dem Prinzip der Zweckbindung bzw. droht diese zu unterlaufen (siehe *2.3.2 Rechtliche Belange*). Er verhindert jede Möglichkeit für Konsumenten, Übersicht darüber zu bewahren, wo und bei wem welche Daten gespeichert und verarbeitet werden – gleichzeitig bedeuten mehr Daten, dass präzisere und aussagekräftigere Profile erstellt werden können.

Die datenschutzrechtliche Bedenklichkeit beginnt nicht erst mit der Analyse personenbezogener Daten durch Data Mining-Verfahren oder der Nutzung der dabei gewonnenen Informationen, sondern sie betrifft auch vorgelagerte Prozeduren der Datensammlung und Bevorratung. Die Speicherung in allgemein verwendbaren Data Warehouses entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar (siehe *2.3.3.1.2 Vorratsdatenspeicherung*). Inwiefern eine anonyme oder pseudonyme Durchführung von Data Mining-Prozessen unbedenklich ist, lässt sich nur in Zusammenhang mit der Verwendung der Resultate beantworten.

[500] Unter Kundenbeziehungsmanagement wird ein umfassendes Unternehmenskonzept verstanden, welches unter Einbeziehung von IT alle kundenbezogenen Prozesse integriert und optimiert.
[501] http://xml.coverpages.org/cpex.html [8. Juli 2007]

Der einzelne Konsument kann kaum wissen und umso weniger beeinflussen, inwieweit seine Daten in Data Mining-Prozessen erfasst und verarbeitet werden. Damit sind auch der individuellen Verantwortlichkeit enge Grenzen gesetzt. Data Mining findet im Verborgenen statt und entzieht sich weitgehend der Kenntnis und dem Bewusstsein der Betroffenen. Der aufgeklärte Konsument geht davon aus, dass die meisten größeren Unternehmen, mit denen man in geschäftlichen Kontakt tritt, Data Mining betreiben. Eine bestehende Geschäftsbeziehung ist jedoch keine notwendige Bedingung, um von Datenanalysen erfasst zu werden. Das Gegenteil ist anzunehmen: die Daten professioneller Anbieter werden vielfach bei gezielten Werbeaktionen, bei der Selektion potentieller Neukunden oder der individuellen Angebotserstellung und Preisgestaltung herangezogen. Profilhändler sind mittlerweile in der Lage, ganz spezifische Persönlichkeitsprofile zu liefern. Hierfür werden hochsensitive Daten aus der privaten Lebenssphäre erfasst, mit vielfältigen öffentlich zugänglichen Daten kombiniert und für Marketing- und andere Zwecke weiterverkauft/angeboten.

Wie bei Datensammlungen im Allgemeinen besteht auch bei Data Mining ein großes Gefahrenpotential darin, dass bei entsprechender Datenbasis sehr umfassende Persönlichkeitsprofile erstellt werden können. Der Umfang der Datenbasis ist durch eine zeitliche Dimension und die Menge an Beobachtungen determiniert. Die zeitliche Dimension lässt sich durch ein Verbot langfristiger Speicherung personenbezogener Daten einschränken. Die Menge an Daten, die Data Mining-Analysen zugeführt werden kann, hängt einerseits von den Möglichkeiten ab, auf Fremddaten zuzugreifen, andererseits vom Umfang der Geschäftstätigkeit des betroffenen Unternehmens. Kritische Bereiche sind hier etwa Telekommunikationsunternehmen; insbesondere wenn traditionelle Telekommunikation, Mobilkommunikations- und Internetdienste von einem Unternehmen bezogen werden, sind reale Gefahren des gläsernen Menschen nicht von der Hand zu weisen. Ein weiterer zu hinterfragender Bereich entsteht bei der Auslagerung von Geschäftsprozessen an externe Unternehmen (Stichwort: Outsourcing). Ein bekanntes Beispiel hierfür ist die Kundenbetreuung durch Call Centers. Da hier Kunden unterschiedlicher Unternehmen auf derselben technischen Infrastruktur betreut werden, ist rechtlich und organisatorisch dafür Sorge zu tragen, dass keine unternehmensübergreifenden Datenauswertungen stattfinden können. Analoge Vorkehrungen sind im öffentlichen Bereich zu treffen, wenn im Rahmen von E-Government-Initiativen One-Stop-Zugangsmöglichkeiten zu öffentlichen Diensten realisiert werden (siehe *2.3.3.1.1 E-Government*).

Wie in vielen Bereichen des Rechts auf Privatsphäre ist auch hier nicht eine grundsätzlich fehlende Regulierung das vorrangige Problem. Es geht in erster Linie darum, die Effektivität bzw. Durchsetzungskraft rechtlicher Normen zu erhöhen und gegebenenfalls geltende Regeln an neue technische Herausforderungen anzupassen. Data Mining ist in wesentlichen Schritten ein unternehmensinterner Prozess, der auch ohne rechtlich unzulässige Verwendungen von Fremddaten oder von Daten mit Personenbezug durchgeführt werden kann. Viele, auch für Unternehmen wertvolle, statistische Aussagen und Zusammenhänge können auf Basis anonymisierter Daten

ermittelt werden. Freiwillige Einschränkungen auf Seite der Unternehmen können daher einen großen Beitrag zur Wahrung der Privatsphäre liefern. Allerdings widerspricht ein allgemeiner Verzicht auf personalisierte Auswertungen grundsätzlichen unternehmerischen Interessen. Für eine Vielzahl von Verwendungen, beispielsweise individualisierte Angebote oder gezielte Werbemaßnahmen im Rahmen des CRM, ist eine Personalisierung unumgänglich.

Ein freiwilliger Verzicht auf personenbezogene Auswertungen oder Anwendungen ist ohne entsprechende regulative Beschränkungen oder öffentlichen Druck bzw. einem drohenden Verlust an Reputation kaum realistisch. Die Bereitschaft seitens der Unternehmen, die Privatsphäre der Kunden zu achten, wird zu einem wesentlichen Teil davon abhängen, ob es gelingt, den in zahlreichen empirischen Erhebungen festgestellten hohen Stellenwert des Datenschutzes den Unternehmen in spürbarer Weise zu vermitteln. Eine Voraussetzung dafür ist, die Konsumenten auch in diesem Bereich zu sensibilisieren und ihnen Unterstützung dabei anzubieten, wie sie Informationen einholen oder ihre Interessen durchsetzen können. Den Unternehmen müssen Möglichkeiten geboten werden, datenschutzkonformes Verhalten und die Einhaltung freiwilliger Vereinbarungen auf einfache Weise zu kommunizieren, sowohl um ihnen einen Wettbewerbsvorteil zu verschaffen als auch den Konsumenten eine Entscheidungshilfe zu bieten. Beim Zustandekommen von wirksamen Formen der Selbstregulierung ist der Gesetzgeber gefragt, indem er etwa Leitlinien und zu erfüllende Mindeststandards vorgibt und durch die Androhung von Zwangsausübung untermauert [Cas, Peissl, 2002, S 74 ff].

2.2.6 AUTORISIERUNG, AUTHENTIFIZIERUNG UND AUTHENTIZITÄT

Unter *Autorisierung* wird die Überprüfung und Zuweisung von Zugriffsrechten auf Daten und Systeme an Benutzer verstanden. Wörndl [Wörndl, 2003, S 24f] spricht in diesem Zusammenhang vom *Autorisierungsziel*, worin er die Bereitstellung einer geeigneten Zugriffskontrolle versteht (siehe *3.5.1 Anforderungen*).

Die *Authentifizierung* (auch: Authentifikation, engl. *authentication*)[502] bezeichnet den Vorgang, die Identität eines Subjekts/Objekts an Hand eines bestimmten Merkmals zu überprüfen. Dies kann zum Beispiel mit einem Passwort, einem Fingerprint oder einem anderen Berechtigungsnachweis erfolgen. Die Authentifizierung kann auf drei unterschiedlichen Wegen erfolgen:

- Besitz: Schlüssel, Karte („*something you have*“)
- Wissen: Passwort, PIN („*something you know*“)
- Biometrisches Merkmal: Fingerabdruck, Aussehen (siehe *1.7.2.3 Biometrie*) („*something you are*“)

[502] Vgl. http://www.zdnet.de/glossar/0,39029897,70009705p-39001691q,00.htm [7. Juni 2007]

Zudem ist eine Kombination dieser drei Authentifizierungs-Faktoren, z. B.: Zwei-Faktoren-Authentifizierung, möglich. Grundsätzlich gilt, je mehr Authentifizierungs-Faktoren, desto höher die Sicherheit.

Die Integration der Authentifizierung in Applikationen wird als „*Authentication Token*“ bezeichnet. Die zwei meist verbreiteten sind *Kerberos*[503] für Windows-Umgebungen und *Security Assertion Markup Language* (kurz: *SAML*)[i] für Web Service-Architekturen (Anm.: Im Bereich Identität ist SAML ein wichtiger technischer Baustein) [Evidian, 2007, S 11].

Die sichere Zuordnung einer Information zum Absender und der Nachweis, dass die Informationen nach dem Versand nicht mehr verändert worden sind, wird als *Authentizität* bezeichnet (siehe *Abbildung 35: Fünf Dimensionen der Verlässlichkeit*).

Ein wesentlicher Term in diesem Zusammenhang ist der des Berechtigungsnachweises (engl. *Credentials*). Damit soll einem System die Identität eines Benutzers bzw. eines anderen Systems bestätigt werden. Das passiert in der Regel in Form eines Benutzernamens in Verbindung mit einem Authentifizierungsmerkmal. Beispiele für Berechtigungsnachweise sind Zertifikate oder physikalische Komponenten wie Chipkarten (siehe *1.7.2.1.6 Digitale Zertifikate, 2.2.1 Digitale Identität, 3.4.2.3 Chipkarten*).

2.3 PRIVACY

2.3.1 HERAUSFORDERUNG UND BEGRIFFSBESTIMMUNG

Privacy wird sehr treffend von Warren und Brandeis in ihrem 1890 erschienenen Artikel „*The Right to Privacy*“ [504] als „*Individual's right to be left alone*“ definiert. Weiter gefasste Definitionen sprechen von dem aktiven Recht, „*darüber zu bestimmen, welche Daten über sich von Anderen gebraucht werden und welche Daten auf einen selbst einwirken dürfen*“. Der zentrale Aspekt ist dabei der der Zugangskontrolle – privat ist dann etwas, wenn das betroffene Subjekt dazu in der Lage und berechtigt ist, den Zugang zu Daten, Wohnungen, Entscheidungen oder Handlungsweisen zu kontrollieren. Oder einfach ausgedrückt, es meine eigene freie Entscheidung ist, der Öffentlichkeit etwas über mich, mein Privatleben, meine Interessen etc. mitzuteilen oder eben auch nicht. Was die Entstehung des Privatheitsbegriffs anbelangt, gibt es mehrere mögliche Sichtweisen. Eine ist, dass sich das Recht auf Privatheit aus dem Recht auf Eigentum ableitet, dass also Informationen aus der Privatsphäre einer Person als ihr Eigentum zu betrachten sind. Eine andere Sichtweise leitet das Recht auf Privatheit aus dem Recht auf die Unversehrtheit der eigenen Person ab, ist demnach eher auf den möglichen Schaden bezogen, den private Informationen in den falschen Händen an der eigenen Person verursachen könnten [Beier, 2005, S 4].

[503] Kerberos ist ein Authentifizierungsdienst für ein ungesicherte TCP/IP-Netzwerke.

Das Zeitalter der Informationsgesellschaft erfordert jedoch eine veränderte Definition von Privacy, „[…] *denn es geht nicht mehr nur darum „in Ruhe gelassen zu werden". Die Debatte sollte um zwei Komponenten erweitert werden. Einerseits geht es dabei um persönliche Daten in Form von Interaktionsdaten, die beim Umgang mit interaktiven Informationssystemen und bei elektronischen Transaktionen unweigerlich anfallen. „Privacy can be defined as a capability to determine what one wants to reveal and how accessible one wants to be". Damit geht es nicht mehr wie bislang um die Frage, wie viele persönliche Daten gesammelt, gespeichert und ausgewertet werden. Vielmehr rückt in einer dynamischen und operativen Definition von Privacy die aktive Kontrolle in den Vordergrund. Kontrolle über die während dem Prozess der Informationsaufnahme und -abgabe und durch die Interaktion anfallenden Daten. Andererseits geht es um die Kontrolle eingehender Daten. So sind Kontrollmechanismen notwendig, mit deren Hilfe Endnutzer die Konsequenzen ihrer elektronischen Transaktionen in Informationsmedien durchschauen und kontrollieren können, und zwar inwieweit sie und ihre persönlichen Daten für andere identifizierbar und erreichbar sind.*"[505]

Um Privatsphäre zu definieren, wurden verschiedene Modelle entwickelt [Fleissner, 2005, S 15f]:

1. *Sphärenhyptothese*: Dieses Modell geht davon aus, dass sich der „Datenschatten" einer Person in Bereiche unterschiedlicher Sensibilität zerlegen lässt, z.B. in: Individual-, Privat- und Geheimsphäre oder Öffentlichkeits-, Sozial-, Vertrauens-, Intim- und Geheimsphäre. Neben einer absolut geschützten Intimsphäre, in die kein Eingriff erlaubt sein soll, gibt es weniger sensible Datenbereiche, die sich in Sektoren aufteilen lassen. (Anm.: Löser [Löser, 2007, S 2f] spricht in diesem Zusammenhang von der *Sphärentheorie*, wobei eine Unterscheidung in Sozial-, Privat- und Intimsphäre erfolgt.) Nach *Rössler* [Rössler, 2001, S 11f] hängt die Definition der Privatsphäre von Konvention, Kultur oder Recht einer Gesellschaft ab.
2. *Mosaikhypothese*: Diese ist eine Erweiterung der Sphärenhypothese, die zusätzlich verlangt, dass auch jene Daten geschützt werden, die für sich allein nicht in den Intimbereich eines Menschen fallen, aber bei Verknüpfung wesentlich zur Erstellung von Persönlichkeitsbildern beitragen. „*Zumindest in der Theorie beachtet die Mosaikhypothese jedoch eine wesentliche Eigenschaft der EDV: Der Verknüpfung von Informationen sind technisch so gut wie keine Grenzen gesetzt. Das Problem liegt somit nicht mehr nur in der Datenerfassung, sondern betrifft auch den Bereich der Datenverarbeitung*."
3. *Rollenhypothese*: Dabei wird „*davon ausgegangen, dass der einzelne Mensch in einer Gesellschaft immer Träger mehrerer Rollen ist, die bestimmte (Daten-) Spuren hinterlassen*" und dass sich eine Persönlichkeit aus der Gesamtheit dieser Rollen zusammensetzt. Demgemäß setzt sich die Privatsphäre aus verschiedenen „Bildern" zusammen, deren subjektiv empfundene Sensibilität auch vom jeweiligen sozialen Interaktionspartner abhängt. Somit sind prinzipiell alle Daten eines

[504] http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html [12. April 2007]

Individuums schutzwürdig und es sollte jedem selbst überlassen bleiben, wie viel er wem gegenüber preisgibt. „*Datenschutz hat im Rahmen dieser Theorie den Zweck, die Zusammenfügung der einzelnen Bilder zu verhindern und die Trennung der verschiedenen Einzelbilder zu sichern. Die Rollenhypothese trägt der Relativität des Begriffs Privatsphäre und dem subjektiven Empfinden von Schutzwürdigkeit am besten Rechnung, die praktische Umsetzbarkeit ist allerdings schwierig.*“ Die individuelle Relativierung mag zwar im Freundeskreis funktionieren, gegenüber einer Behörde ist es aber nicht möglich, sich auf eine subjektiv empfundene Privatheit zu berufen. Das Rollenmodell wird deshalb im wesentlichen nur – wie im deutschen „Recht auf informationelle Selbstbestimmung“ (siehe *2.3.2.1 Informationelle Selbstbestimmung*) – im Sinne eines prinzipiellen Rechts gefordert, das dann durch eine Fülle von gesetzlichen Ausnahmebestimmungen eingeschränkt wird.

Eine weitere Präzisierung des Begriffs kann nach Rössler [Rössler, 2001, S 5ff] durch die Einteilung in informationelle, dezisionale und lokale Privatheit erfolgen. Bei der informationellen Privatheit geht es um den Umgang mit persönlichen Daten. Unter dezisionaler Privatheit ist die Freiheit eines Subjekts gemeint, Entscheidungen zu treffen. Die physische Privatheit definiert den privaten, territorialen Bereich eines Individuums, zu dem nicht jeder Zugang hat und zu dem der Zugang von der betreffenden Person kontrolliert werden kann.

Vorrangig betrachtet werden soll die informationelle Privatheit. „*Hier geht es um die Privatheit von Informationen über die betroffene Person, also die Privatheit persönlicher und vor allem personenbezogener Daten. Entscheidend für informationelle Privatheit sind der Schutz von persönlichen Daten, also der Schutz von Daten vor unberechtigtem fremdem Zugriff und – noch um einiges kritischer – der Schutz des betroffenen Subjekts vor persönlichen Daten, besser gesagt der Schutz vor deren mißbräuchlicher Anwendung und dem dadurch potentiell entstehenden Schaden an der betroffenen Person. Die Kernfrage hier ist: Was wissen andere über mich?*“ [Rössler, a. a. O]

Bei der gesellschaftlichen Betrachtung informationeller Privatheit geht es unter anderem „*um den zentralen Aspekt der Zugangskontrolle zu Informationen zur eigenen Person: beispielhaft sind die Weitergabe persönlicher Daten, wissentlich oder auch unwissentlich gefilmt zu werden, oder einfach die Frage „Was plaudern meine Freunde über mich aus?“ Zugangskontrolle, jetzt speziell bezogen auf informationelle Privatheit, läßt sich in zwei Kernpunkten darstellen: erstens, zu wissen oder wenigstens abschätzen zu können, was andere über einen wissen, und zweitens, gemäß diesem Wissen oder Annahmen diesen anderen gegenüber entsprechend agieren zu können. Die „Anderen“ können hierbei die Polizei, der Staat, das Unternehmen oder einfach der Freundeskreis sein. Diese zwei*

[505] Vgl. http://www.nethics.net/nethics/de/themen/privacy/begriffserlaeuterung.html [8. Juni 2007]

Kernpunkte sind Fundament und Basis informationeller Privatheit und damit wiederum Voraussetzung informationeller Selbstbestimmung und letztendlich Freiheit."

Als Fazit sieht Rössler: „[…] *Der Kernpunkt ist, dass die individuelle Freiheit des Einzelnen essentiell für die gesamtgesellschaftliche Freiheit ist. Nehmen nun Bürger Einschränkungen ihrer Privatheit und in der Folge Freiheit hin, so wird das Aufgeben eines gewissen Maßes an Privatheit zur gesellschaftlichen Norm, so werden im Rahmen dieser Gesellschaft selbstbestimmte Handlungen immer schwieriger, die ganze Gesellschaft verliert an Privatheit, an Autonomie und Selbstbestimmung, und damit an Freiheit*." [Rössler, 2001, S 8, S 11].

Das *European Parliamentary Technology Assessment* (kurz: *EPTA*)[506]-Institut hat in einer Studie (publiziert: Oktober 2006) die Situation hinsichtlich Informations- und Kommunikationstechnik (kurz: IKT) und Privacy in sieben europäischen Ländern untersucht [EPTA, 2006]. Dabei wurden folgende Privacy-betreffende Felder analysiert: Informationssicherheit, Zugang zu Information und Services, gesellschaftliche Interaktion und ökonomischer Nutzen. Im *Executive Summary* [EPTA, 2006, S 10f] werden die wesentlichen Ergebnisse wiedergegeben: „*Dealing with privacy in terms of trade-offs helps to illustrate that a balance has to be found between conflicting societal values and rights. Our analysis points to some important challenges and corresponding policy options:*

- ***Review of surveillance systems by independent body**: An important task for governments is to provide their citizens with a high level of security. However, they need to consider whether more surveillance is justified. It is important that surveillance systems are properly assessed. Their value depends on them being effective, not easily circumvented and resulting in a real security benefit. One option is periodical review of surveillance systems by an independent publicly accountable body.*
- ***Citizens' access to their own records and logs**: E-Government increases the flow of information between different public units, in order to provide desired services. It has the potential to dramatically increase the amount of personal information officials hold about citizens. A vital challenge is how the technology can be used not only to increase efficiency for the public administration; but also to strengthen privacy for the citizen. Governments could consider a mutually transparent system that gives citizens access to their own records and logs, and allows them actively to control the flow of their own personal data.* (Anm.: Eine beispielgebende Umsetzung wurde in Estland mit dem *E-Citizen*-Portal (Stichwort: *direct information exchange, e.g. residency registration*) realisiert [Tallo, 2007, S 9].)
- ***Empowering data protection agencies**: The mandate of data protection agencies remains weak in many countries. As long as ignoring data protection rules bear no consequence, there will be no incentive for industries and public bodies to incorporate privacy principles into their IT systems*

[506] http://www.eptanetwork.org/EPTA/ [9. Juni 2007]

and services. A crucial question is the capacity of these agencies to handle complaints in due time. Governments may need to consider seriously whether data protection agencies should be able to proactively conduct investigations, impose effective penalties and monitor the activities of public and private organizations and their approach to data management.

- ***Mandatory privacy impact assessments**: The study shows that privacy threats could often be avoided if data protection concerns were built into information systems development from the start. Mandatory Privacy Impact Assessments* (kurz: *PIAs*) *can contribute to ensuring that privacy is taken into consideration. In the public sector, PIAs could become a prerequisite for IT project procurement. Although they will involve financial costs, the benefits may be significant. It is cheaper to include privacy concerns in the design phase of systems than to make them privacy compliant at a later stage. Privacy enhancing technologies* (kurz: *PETs*) (siehe *2.4.2 Säule 2: Bewusstseinsschaffung und Selbstbeschränkung*) *could be systematically integrated into systems development. An important PET principle is that systems should only collect data on a need to know – not a nice to know – basis* (siehe *2.4.2.2 Datensparsamkeit*). *Delivering services without collecting excess data is cost-effective as well as socially desirable. International privacy standards can enhance consumer trust and promote equal privacy protection worldwide; and they encourage corporate response.*

There is a rapid development of E-Services and a new security situation. New technologies such as RFID, biometrics and pervasive computing (siehe *2.3.3 Technologien und Entwicklungen mit Einfluss auf* Privacy) *are also developing rapidly and thus create new possibilities and threats. This report shows that the value of privacy is underestimated by citizens, policy makers and enterprises. It concludes that there is need for more research on mid- and long-term effects of weakened privacy, and more public dialogue is needed on these issues.*“

Im Unterschied zur Offline-Welt hinterlässt jede Aktivität in der Online-Welt digitale Spuren, die gespeichert, gesammelt, kombiniert und ausgewertet werden können. Daraus lassen sich (umfassende) Informationssammlungen bilden, die nicht nur Auskunft über den Kommunikationspartner und Aufenthaltsort geben, sondern auch persönliche Interessen, politische Einstellungen oder sexuelle Vorlieben preisgeben können. Sind diese Daten einmal digital erfasst, bleiben sie in der Regel für lange Zeiträume im Zugriff und damit verwertbar. Dadurch wird Missbrauch ermöglicht. Dieses Problem wird durch die zunehmende Nutzung von E-Commerce- bzw. E-Government-Anwendungen für eine immer größere Anzahl von Anwendern/Kunden/Bürgern relevant. Angesichts der zunehmend unmerkbaren und daher nicht bewussten Erhebung von Daten, der Weitergabe und Nutzung in anderen Kontexten und der Zeitspanne, die zwischen Erhebung und Auswertung liegt, werden diese klaren Vorgaben meist nicht eingehalten [Cas, Peissl, 2002, S 11].

2.3.2 RECHTLICHE BELANGE

An dieser Stelle kann auf die entsprechenden Ausführungen im vorigen Kapitel verwiesen werden: Rechtliche Belange im Bereich der Computerkriminalität (siehe *1.3.5.1 Rechtlicher Rahmen*) und allgemeine Erläuterungen zum Online-Recht (*1.7.3 Gesetzeslage*), im speziellen Datenschutz (*1.7.3.1 Datenschutz*). Auf Basis dieser Grundlagen werden kontextuelle Verfeinerungen hinsichtlich Privacy angeführt.

Der Datenschutzstandard für die personenbezogenen Daten des Nutzers wird von den Gesetzen des Landes bestimmt, in dem der für die Verarbeitung Verantwortliche seinen Wohn- bzw. Geschäftssitz hat. Obwohl in Europa der sorgfältige Umgang mit Personendaten gesetzlich geregelt ist[507], gibt es keine Sicherheit, was (Web-)Diensteanbieter mit den personenbezogenen Daten machen, wenn ihr Sitz außerhalb der Europäischen Union und damit außerhalb des Einflussbereichs europäischen Rechts ist [Rickert, 2004, S 24]. Die Situation in den USA bezüglich rechtlicher Rahmenbedingungen ist im Hinblick auf Privatheit von einem etwas anderen Rechtsverständnis als in Europa geprägt. Es gibt weniger gesetzliche Regelungen, es wird von einer Selbstregulierung des Marktes ausgegangen. Verstöße gegen Privatheitsansprüche werden daher in erster Linie als Bruch einer Vereinbarung zwischen einem Unternehmen und einem Kunden bzw. als Betrug gewertet und erst in zweiter Linie als Missachtung eines Gesetzes angesehen.

Um die aus EU-Sicht nicht ausreichenden gesetzlichen Vorschriften anzugleichen und für EU-Bürger ein angemessenes Schutzniveau gegenüber Drittstaaten wie den USA zu gewährleisten, wurde das Safe-Harbor-Abkommen getroffen (siehe *1.7.3.1 Datenschutz*). Dabei fehlen zwar einige Punkte beispielsweise gegenüber dem deutschen Datenschutzrecht wie Datensparsamkeit oder das Verbot des Ausschlusses von Benutzern bei Verweigerung der Zustimmung einer Speicherung personenbezogener Daten, dennoch können die Safe Harbour-Grundsätze als eine hinreichende Grundlage für die Speicherung und Nutzung personenbezogener Daten aus rechtlicher Sicht angesehen werden. [Wörndl, 2003, S 21f].

Zurzeit gibt es allerdings kaum weltweit gültige Rechtsvorschriften und die Anwendung nationaler Gesetze im grenzüberschreitenden Internet stellt sich als problematisch dar.

Wie im Kapitel Datenschutz ausgeführt ist, werden unter personenbezogenen Daten Angaben über Betroffene verstanden, deren Identität bestimmt oder bestimmbar ist. Entscheidend ist also die Verknüpfung von Daten mit der Identität einer Person.

Die dem Österreichischen Datenschutzgesetz zugrundeliegende Datenschutz-Richtlinie der EU definiert einige allgemeine Grundsätze über den Umgang mit personenbezogenen Daten [Rickert, 2004, S 23f] (Anm.: auf Basis der „Empfehlung des Rates über Leitlinien für den Schutz des

[507] Vgl. http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm [16. Juni 2007]

Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“[508] der OECD):

- Zweckgebundenheit: Personenbezogene Daten dürfen nur für den angegebenen Zweck verwendet werden. Der Zweck einer Datenerfassung muss sich entweder aus den gesetzlichen Regelungen ergeben oder der Benutzer hat für die Erhebung und Nutzung zu einem spezifizierten Zweck seine ausdrückliche Einwilligung erteilt. Daten dürfen nur für diesen Zweck verwendet werden.
- Datenqualität (auch Datensparsamkeit oder Erforderlichkeit der Datenerfassung): Nur korrekte und für den Verwendungszweck erforderliche Daten dürfen gehalten werden. Dabei muss ein Diensteanbieter sicherstellen, nur die für die Erbringung des vom Benutzer erwünschten Dienstes notwendigen personenbezogenen Daten zu erheben und zu verarbeiten. Darunter fällt auch die Möglichkeit – sofern technisch möglich – Dienste, die anonymes bzw. pseudonymes Anmelden erlauben, anzubieten.
- Transparenz: Gründe für die Erfassung und der Verantwortliche müssen dem Betroffenen bekannt gemacht werden.
- Sicherheit: Gegen unautorisierten Zugriff müssen Maßnahmen ergriffen werden.
- Zugriffsrechte: Jeder darf auf seine erfassten Daten zugreifen, diese korrigieren und für weitere Zwecke sperren und löschen.

2.3.2.1 Informationelle Selbstbestimmung

Informationelle Selbstbestimmung lässt sich nach Köhntopp [Köhntopp, 2000] folgendermaßen beschreiben: „[…] *Jeder soll grundsätzlich wählen können, was dem jeweiligen Kommunikationspartner über sich offenbart wird und in welcher Rolle er auftritt. Das betrifft den Austausch von Untermengen der Informationen, die die eigene Identität ausmachen. Damit ist der Umgang mit Identitäten eng mit dem Recht auf Informationelle Selbstbestimmung verwandt: Jeder soll wissen können, wer was über ihn weiß. Dafür muß sich der Betroffene der ständig wechselnden Kontexte seines Lebens bewußt sein* […]“

Beier [Beier, 2005, S 3f] erläutert: „[…] *Selbstbestimmung meint die Fähigkeit des autonomen Subjekts, der Gesellschaft oder des Staates, frei der eigenen Vernunft gemäß zu handeln und auch die Gesetze und Regeln dieses Handelns zu entwerfen. Selbstbestimmung ist letztlich die Aufhebung der Fremdbestimmung.* […] *Für den Themenbereich Informationelle Selbstbestimmung besonders wichtig sind insbesondere die Meinungs- und Informationsfreiheit.* […]“

Bei der herkömmlichen Kommunikation in der *Offline-Welt* sind die Menschen durch entsprechende Sozialisierung gewohnt, bei ihrem Auftreten intuitiv zu entscheiden, wem welche Informationen von sich gegeben werden. Damit können sie den Eindruck, den andere Personen von ihnen haben,

[508] http://www.datenschutz-berlin.de/infomat/heft24/bde.htm [13. Juni 2007]

beeinflussen oder sich zumindest bewusst machen. Der alltägliche Umgang mit den eigenen Identitäten der Offline-Welt ist nicht direkt übertragbar auf die *Online-Welt*, in der jeder Nutzer – meist unbewusst – Datenspuren hinterlässt und in der es einfacher ist, digital vorliegende Daten aus verschiedenen Anwendungen zu verknüpfen und zu Profilen zu aggregieren[509].

Das Recht auf informationelle Selbstbestimmung ist in Deutschland im Gegensatz zu Österreich im Datenschutzgesetz verankert. Im deutschen Recht bezeichnet gemäß Bundesverfassungsgericht (Volkszählungsurteil vom 15.12.1983[510]) die informationelle Selbstbestimmung „[…] *das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig*." [Löser, 2007] Es besteht demnach ein „*Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten"*. Das Grundrecht auf informationelle Selbstbestimmung wird als besondere Ausprägung des zuvor grundrechtlich geschützten allgemeinen Persönlichkeitsrechts angesehen. Wie dieses wird es verfassungsrechtlich aus Art. 2 Abs. 1 (allgemeine Handlungsfreiheit) in Verbindung mit Art. 1 Abs. 1 GG (*Menschenwürde-Garantie*) hergeleitet.

In Österreich stellt sich die Situation anders dar. Hier regeln das *Meldegesetz* (kurz: *MeldeG*) [511] und die dazu ergangene *Durchführungsverordnung*[512] den entsprechenden Bereich. Das *Zentrale Melderegister* (kurz: *ZMR*)[513] wurde im Zusammenhang mit der Volkszählung (Stichtag 15.5.2001) geschaffen und ist zeitgleich mit dem Inkrafttreten (Anm.: 1.3.2002) des aktuell gültigen Meldegesetz in Echtbetrieb gegangen. Dabei handelt es sich um eine zentrale Datenbank mit der Möglichkeit der österreichweiten Gesamtsicht über alle Wohnsitz-Meldungen einer Person. Das ZMR ist eine Evidenz, in der alle gemeldeten Menschen einmal erfasst sind. Es werden jedem Menschen bundesweit sein Wohnsitz oder seine Wohnsitze zugeordnet: neben nur einem möglichen Hauptwohnsitz sind gegebenenfalls weitere Wohnsitze vermerkt. Diese Meldungen werden laufend von den Gemeinden und Städten Österreichs aktualisiert. Allen Behörden und Körperschaften öffentlichen Rechts, einschließlich der Gemeindeverbände, ist die Möglichkeit zu einem Online-Zugriff eingeräumt worden. Darüber hinaus können Personen, die regelmäßig Meldeauskünfte benötigen, wie etwa Notare, Rechtsanwälte, Banken und ähnlichen Institutionen, ein Online-Zugriff auf die Meldedaten des ZMR, für die keine Auskunftssperre besteht, eingeräumt werden. Den Bürgern wird durch die Einbindung der elektronischen Abfrage in Behördenverfahren die Vorlage des Meldezettels erspart. Das ZMR ist ein Informationsverbundsystem i. S. *§4 Zif. 13 DSG 2000*. Für statistische Zwecke ist

[509] Vgl. http://www.informationelle-selbstbestimmung-im-internet.de/ [19. April 2007]; http://www.informationelle-selbstbestimmung.com/ [31. Mai 2007]
[510] http://www.servat.unibe.ch/law/dfr/bv065001.html [31. Mai 2007]
[511] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Meldegesetz [15. Juni 2007]
[512] http://zmr.bmi.gv.at/pages/mdurchf.htm [15. Juni 2007]
[513] http://zmr.bmi.gv.at/pages/allgemein.htm [16. Juni 2007]

die gemeinsame Verarbeitung mit den von der Sozialversicherung zugeordneten Versicherungsnummern möglich. Die Statistik Österreich hat die personenbezogenen Daten zu anonymisieren und den Ländern und Gemeinden („Wanderungsstatistik“) zur Verfügung zu stellen. Die im ZMR gespeicherten Daten dürfen weiters für statistische Zwecke übermittelt werden und zwar zumindest in für den Empfänger indirekt personenbezogener Form, sofern der Personenbezug für die Durchführung der Untersuchung nicht unerlässlich ist (laut *§16 b MeldeG*). In Österreich sind daher gesetzlich personenbezogene Statistiken möglich. Anerkannte Religionsgesellschaften dürfen die Meldedaten ihrer zahlungspflichtigen Mitglieder weiterhin abfragen. Darüber hinaus wurden zur Überprüfung der Richtigkeit der in den Melderegistern enthaltenen Daten im Rahmen der Volkszählung 2001 diverse Daten gemeinsam mit der Volkszählung ermittelt. Diese Verschränkung wurde mehrfach kritisch diskutiert [Cas, Peissl, 2002, S 15f].

Die Grundaussage zur informationellen Selbstbestimmung lautet: „*So viel Freiheit wie möglich und so viel Bindung wie nötig. Die Freiheit der Bürger wird dabei grundsätzlich vorangestellt; zugleich wird den Anforderungen der Gemeinschaft Rechnung getragen*.“[514]

Bei Cas [Cas, Peissl, 2002, S 12] werden zusammenfassend zwei Dimensionen für das Recht auf informationelle Selbstbestimmung festgehalten:

- das Recht des Einzelnen, grundsätzlich selbst über die Verwendung und Preisgabe seiner Daten zu bestimmen und
- das notwendige aufgeklärte und freiwillige Einverständnis in Kenntnis des Verwendungszwecks.

Unumgängliche Einschränkungen dürfen nur im überwiegenden Interesse der Allgemeinheit erfolgen und müssen durch das Gesetz unter Beachtung der Verhältnismäßigkeit legitimiert sein. Flankierend dazu sind organisatorische und verfahrensrechtliche Schutzvorkehrungen vorzusehen.

2.3.2.2 Zusammenhang von Identitätsmanagement und Datenschutz

An dieser Stelle soll der Einfluss von Privatheitsansprüchen der Benutzer auf Identitätsmanagementsysteme erläutert werden. Es gilt Identitäten zu verwalten, das passiert mit sogenannten Identitätsmanagementsystemen (siehe *3Identitätsmanagement*). Diese befähigen den User, die Verwaltung seiner Daten und damit das Recht auf informationelle Selbstbestimmung selbst in der Hand zu haben.

Die Identität einer natürlichen Person ist rechtlich in zweierlei Hinsicht von Bedeutung [Hansen, 2003, S 3f]:

- zur Identifizierung für rechtlich relevante Zwecke und

[514] Vgl. http://www.datenschutz.de/recht/grundlagen/ [31. Mai 2007]

- um persönliche Freiheitsrechte (Name, Selbstbestimmung, Meinungsfreiheit usw.) in Zusammenhang mit einer natürlichen Person zu schützen.

Demnach besteht die Identität zum einen aus Elementen, die ihre Einzigartigkeit garantieren sollen (siehe *2.2.1 Digitale Identität*). Zum anderen umfasst die Identität Persönlichkeitsrechte, die in demokratischen Staaten in der Verfassung und weiteren Gesetzen festgehalten sind und den Menschen die Möglichkeit geben, ihre Persönlichkeit zu entfalten und dadurch die Identität zu entwickeln. Diese Persönlichkeitsrechte bilden gleichzeitig eine rechtliche Basis für das Identitätsmanagement. Außerdem haben die Menschen das Recht, in vielen Situationen anonym oder unter (selbst gewähltem) Pseudonym aufzutreten.

Identitätsmanagement ist an sich rechtskonform, solange es nicht in betrügerischer Absicht geschieht, in anderer Weise die Rechte von Dritten beeinträchtigt oder gegen die guten Sitten verstößt. Darüber hinaus sieht das Recht selbst Möglichkeiten für Identitätsmanagement vor: so akzeptiert das österreichische Recht Eigengeschäfte trotz Handelns unter fremden Namen[515]. Sofern Name und Identität des Vertragspartners für den Abschluss eines Vertrages und dessen Durchführung keine Rolle spielen, kann unter einem beliebigen Pseudonym agiert werden. Die Erlaubnis für die Verwendung von Pseudonymen wird etwa im Signaturgesetz[516] festgehalten. Bei Verwendung bestimmter Pseudonyme kann der Nutzer rechtsverbindlich agieren, datenschutzrechtliche Auskunftsansprüche können sich demnach auch auf Pseudonyme erstrecken. Hierfür muss allerdings der Nachweis geführt werden, dass es sich beim Anfrager auch tatsächlich um den Pseudonyminhaber handelt.

Grundsätzlich ist es nicht immer notwendig, dass sich die Betroffenen mit ihren meldeamtlich registrierten Daten identifizieren. Meist reicht es aus, bestimmte, für den Anwendungskontext definierte Eigenschaften zu garantieren. Der Personenbezug ist damit zur Erfüllung der Zweckbestimmung der Daten sehr oft nicht notwendig.

Die im Signaturgesetz vorgesehenen Pseudonyme, erweitert um Interpretationsanweisungen für die pro Anwendungskontext notwendigen Eigenschaften, können lediglich einen Teil der denkbaren und sinnvollen Pseudonymarten eines umfassenden Identitätsmanagements abdecken. Nicht erfasst sind beispielsweise selbstgenerierte Pseudonyme, die wegen geringerer Anforderungen an ihre Rechtsverbindlichkeit keiner weiteren Zertifizierung bedürfen (z. B.: für einen beschränkten Einsatz in einer geschlossenen Benutzergruppe) oder nicht von Zertifizierungsstellen nach dem Signaturgesetz zertifiziert werden müssen.

Zu den Persönlichkeitsrechten, die für Identitätsmanagement eine Rolle spielen, gehört im Besonderen das Recht auf informationelle Selbstbestimmung. Die Benutzer sollen befähigt werden, selbst verantwortungsvoll über die Herausgabe ihrer personenbezogenen Daten zu entscheiden.

[515] Vgl. http://www.internet4jurists.at/gesetze/bg_signatur01.htm [8. Juli 2007]

Untersuchungen [Hansen, 2003, S 4f] zeigen, dass viele auf dem Markt angebotenen Identitätsmanagementsysteme zumindest aus Datenschutzsicht Mängel aufweisen. Diesbezüglich Abhilfe schaffen kann eine entsprechende Vertragsgestaltung bei gleichzeitiger Einwilligung der Benutzer datenschutzgerecht organisiert zu werden. Wesentlicher Faktor ist jedoch das Vertrauen der Kunden zu den Systembetreibern. Eine wichtige Entscheidung bei der Auswahl der Produkte spielt daher die Frage, ob die Datenverwaltung und -haltung bei einer Fremdfirma oder auf eigenen Systemen erfolgen soll. Produkte wie *Microsoft Passport/LiveID*[517] erfordern vom User das Vertrauen in den IMS-Provider, dem die Daten in Obhut gegeben werden. Aus Sicht des Datenschutzes sind daher diejenigen Identitätsmanagementsysteme zu bevorzugen, bei denen der Nutzer die Hoheit über seine Daten behält. Auch aus Informationssicherheitsgründen ist eine zentrale Speicherung von Nutzerdaten bei einem externen Anbieter kritisch zu sehen, denn diese Datenbanken können begehrte Angriffsziele sein. Die Benutzer müssen sich darüber im Klaren sein, dass sie im Falle der Datenverwaltung auf dem eigenen Computer auch selbst die Verantwortung für ein angemessenes Sicherheitsniveau übernehmen. Es bleibt eine offene Frage, wie dies mit den heute verbreiteten unsicheren Systemen (siehe *1.3 Taxonomie von Angriffen auf den Wert Information*) vom Benutzer praktisch geleistet werden kann. In allen Fällen muss den Herstellern der Produkte das Vertrauen entgegengebracht werden, dass sie keine *Hintertüren* (siehe *1.4.3.2 Backdoor/Rootkit*) in ihre Produkte eingebaut haben, die ein Ausspionieren erlauben. *Open Source*[518] kann zur gesteigerten Vertrauenswürdigkeit der Produkte beitragen. Werden rechtlich bedeutsame Aktionen durchgeführt, liegt es am Benutzer, sich um die Beweissicherung zu kümmern.

Identitätsmanagementsysteme bedingen ein hohes Niveau an Grunddatenschutz für alle beteiligten Komponenten:

- Alle eingesetzten Systeme sollten vertrauenswürdig sein und transparent für den Benutzer arbeiten. Die zugrundeliegenden Kommunikationsnetze müssen grundsätzlich eine Anonymität der Benutzer gewährleisten, damit nicht auf dieser Ebene übertragene identifizierende Informationen das Identitätsmanagement aushebeln.
- Stärkung des Benutzers und seiner Selbstdatenschutzkompetenz: Die verwendeten Identitätsmanagementsysteme sollten sich im Bereich des Benutzers und unter seiner Kontrolle befinden (z. B. PDA, Chipkarte – gegebenenfalls durch Biometrie gegen unautorisierte Zugriffe abgesichert). Nutzungsfreundliche Bedienoberflächen sind notwendig, um die verschiedenen Pseudonyme und Rollen zu verwalten und eine unabsichtliche Aufdeckung zu vermeiden. Dem

[516] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Signaturgesetz §5 §8 [8. Juli 2007]
[517] https://accountservices.passport.net/ppnetworkhome.srf?lc=1031 [17. Juni 2007]
[518] Open Source ist Software, die unter einer von der Open Source Initiative (kurz: OSI) anerkannten Lizenz steht. Die OSI stützt sich bei der Bewertung auf die Kriterien der Open Source-Definition. Diese geht weit über die Verfügbarkeit des Quelltexts hinaus und ist fast deckungsgleich mit Freier Software, d. h. der Quelltext muss für Bearbeitung und Weiterverbreitung offen sein.

Benutzer soll leicht verständlich dargestellt werden, wem er wann welche seiner Daten offenbart hat. Aushandlungskomponenten (siehe *2.1 Problemstellung und Herausforderung: mehrseitige Sicherheit*) und Benutzerkontrollfunktionen können das System ergänzen.

- Repräsentation von Pseudonymen und Rollen mit verschiedenen Eigenschaften: Für die Realisierung von digitalen Pseudonymen können kryptographische Methoden wie die elektronische Signatur (siehe *1.7.2.1.7 Elektronische Signatur*) integriert in Public-Key-Infrastrukturen (siehe *1.7.2.1.5 Public Key Infrastructure*) benutzt werden. Die Pseudonyme (siehe *2.2.2 Pseudonymität*) können sich unterscheiden in Zurechenbarkeit, Verkettbarkeit, Aufdeckbarkeit der Identität oder Begrenzung der Gültigkeit (zeitlich, Anzahl der Nutzungen, sperrbar oder zurückziehbar). Verschiedene Arten von Treuhändern (engl. *Trust Center*) sind denkbar, sodass eine faire Abwicklung von Transaktionen möglich ist, ohne die Identität der Beteiligten offenzulegen.
- Identitätsmanagementsysteme können nur die Datenflüsse der digitalen Welt abbilden, soweit diese bekannt und transparent sind. Grenzen bestehen beispielsweise bei (biometrischen) Überwachungen und bei unbemerkter Übertragung von *Globally Unique Identifier* (kurz: *GUID*)[519]. Zudem kann der Einsatz solcher Systeme neue Probleme aufwerfen, etwa durch eine große Abhängigkeit der Benutzer von ihrem Identitätsmanager oder durch die Verarbeitung personenbezogener Daten Dritter in dem System.

2.3.2.3 Definition von Daten nach dem TKG 2003 bzw. Kommunikationsgeheimnis und Datenschutz

Für die weiteren Ausführungen sind eine klare Differenzierung von Daten und ein Verständnis über deren Schutz aus rechtlicher Sicht notwendig. Im *§92 TKG 2003*[520] sind im 12. Abschnitt (Kommunikationsgeheimnis, Datenschutz) folgende Begriffserklärungen angeführt:

1. *Anbieter*: Betreiber von öffentlichen Kommunikationsdiensten.
2. *Benutzer*: eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben.
3. *Stammdaten*: alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind:
   a. Familien- und Vorname,
   b. akademischer Grad,
   c. Wohnadresse,
   d. Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,

[519] Ein GUID ist eine global eindeutige Zahl, die in verteilten Computersystemen zum Einsatz kommt (z. B.: Mac-Adresse). GUID stellt eine Implementierung des Universally-Unique-Identifier-Standards dar.

e. Information über Art und Inhalt des Vertragsverhältnisses,

f. Bonität.

4. *Verkehrsdaten*: Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

4a. *Zugangsdaten*: jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.

5. *Inhaltsdaten*: die Inhalte übertragener Nachrichten (siehe Z 7).

6. *Standortdaten*: Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.

7. *Nachricht*: jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können.

8. *Anruf*: eine über einen öffentlich zugänglichen Telefondienst aufgebaute Verbindung, die eine zweiseitige Echtzeit-Kommunikation ermöglicht.

9. *Dienst mit Zusatznutzen*: jeder Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht.

10. *Elektronische Post*: jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.

Ausführungen zum Kommunikationsgeheimnis ist im *§93 TKG 2003*[521] festgehalten:

1. Dem Kommunikationsgeheimnis unterliegen die Inhalts-, die Verkehrs- und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

2. Jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, sind zur Wahrung des Kommunikationsgeheimnisses verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach Ende der Tätigkeit fort, durch die sie begründet worden ist.

[520] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: TKG §92 [19. Juni 2007]
[521] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: TKG §93 [19. Juni 2007]

3. Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.
4. Werden mittels einer Funkanlage, einer Telekommunikationsendeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Telekommunikationsendeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten.

Allgemeines zum Datenschutz ist in *§96 TKG 2003*[522] zu finden. Detailliertere Ausführungen enthalten *§97* Stammdaten, *§99* Verkehrsdaten oder *§101* Inhaltsdaten.

1. Stamm-, Verkehrs-, Standort- und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden.
2. Die Übermittlung von im Abs. 1 genannten Daten darf nur erfolgen, soweit das für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber erforderlich ist. Die Verwendung der Daten zum Zweck der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen sowie sonstige Übermittlungen dürfen nur auf Grund einer jederzeit widerrufbaren Zustimmung der Betroffenen erfolgen. Diese Verwendung ist auf das erforderliche Maß und den zur Vermarktung erforderlichen Zeitraum zu beschränken. Die Anbieter dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen.
3. Der Anbieter ist verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten ermittelt, verarbeitet und übermittelt werden, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Diese Information hat auch auf das Recht hinzuweisen, die Verarbeitung zu verweigern. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, soweit unbedingt erforderlich, um einen vom Teilnehmer oder Benutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen. Der Teilnehmer ist auch über die Nutzungsmöglichkeiten auf Grund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Diese Information hat in geeigneter Form,

insbesondere im Rahmen Allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen. Das Auskunftsrecht nach dem Datenschutzgesetz (siehe *1.7.3.1 Datenschutz*) bleibt unberührt.

2.3.3 TECHNOLOGIEN UND ENTWICKLUNGEN MIT EINFLUSS AUF PRIVACY

Im Folgenden werden die wesentlichen Technologien und Entwicklungen mit Fokus auf internetbezogene Aktivitäten und Datenspeicherung vorgestellt, die Einfluss auf Privacy haben. Auf Basis einer Untersuchung der EU hinsichtlich Privacy [EPTA, 2006, S 16f] werden drei entscheidende Einflussfaktoren aufgezeigt:

- *„The digitalisation of telecommunications, allowing the generation of communications profiles,*
- *the rapid diffusion of mobile communications, enriching these profiles by location data and*
- *the extension of Internet into the daily life of many people, revealing information about personal interests and predilections through the use of its services.“*

Wie aus einer Gegenüberstellung von persönlichen Daten und verschiedenen Institutionen deutlich wird, zählen folgende „*Landschaften der Problemfelder*“ zu jenen Bereichen, in denen am meisten Daten generiert werden [Cas, Peissl, 2000, S 12]:

- Öffentliche Institutionen (Verwaltung, Meldewesen, Grundbuch, Polizei/Gericht, Bundesheer/Zivildienst, Finanzbehörden, Bildungssystem, Statistik Österreich),
- Arbeitgeber,
- Telekommunikation (Festnetzbetreiber, Mobiltelefonie, Internetprovider, Gesamtanbieter etc.),
- Finanzdienstleister (Gehaltskonto, Pensionskonto, Studentenkonto, Bankomat, Kredite, Kreditvermittler, Kreditkartenanbieter, Bausparkassen, diverse Fondsverwaltungen, Abrechnungszentralen, Finanzberater etc.),
- Gesundheitswesen (Sozialversicherung, Ärzte, private Krankenversicherungen, Spitalserhalter (private, Bund, Länder, Gemeinden), Apotheken etc.),
- Versicherungen (KFZ, Gebäude/Haushalts- und Lebensversicherungen, Makler etc.),
- Händler und Dienstleister verschiedener Branchen (Kundenkarten, Konsumprofile etc.),
- Kirchen und Vereine.

Jede der Privacy-gefährdenden Technologien bzw. Entwicklungen wird in Übersichtsform erläutert, die entsprechenden Schutzmaßnahmen in einem späteren Kapitel abgehandelt (siehe *2.4 Maßnahmen zum Schutz der Privacy*).

[522] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: TKG §96 [19. Juni 2007]

2.3.3.1 Digitalisierung und Datenspeicherung

Die Entwicklung hin zur Digitalisierung eröffnet nicht nur Unternehmen und dem Einzelnen Erleichterungen und ungeahnte Möglichkeiten im täglichen Ablauf, sondern bringt auch eine Bedrohung der Privatsphäre mit sich. Ein Bericht des Instituts für Technikfolgenabschätzung zeigt, dass über jeden Österreicher Daten in einer Vielzahl von Datensammlungen gespeichert sind. Die Annahmen reichen von etwa 100 bis zu mehreren hundert Datenbanken.

Durch die zunehmende Vernetzung und vor allem durch verbessertes Data Mining (siehe *2.2.5 Data Mining*) können auf rein statistischer Ebene bessere Aussagen über Kleingruppen und mit hoher Prognosewahrscheinlichkeit auch über Einzelpersonen gemacht werden, als sich aus den gesammelten Daten allein ergeben würden.

Ganz allgemein lässt sich eine Dynamisierung feststellen: nicht mehr nur statische Daten in Datensammlungen bilden die Grundlage für eine Bedrohung der Privatsphäre, vielmehr entstehen bei der Nutzung neuer Medien zusätzliche, sich bei jeder Mediennutzung verändernde Daten wie Verkehrs- und Inhaltsdaten, die eine umfassende Überwachung bzw. Verhaltensanalyse ermöglichen [Cas, Peissl, 2000, S 4].

Die öffentliche Hand verfügt inzwischen über alle relevanten Bürgerdaten. Der Beweis dafür ist die ab 2011 eingesetzte Registerzählung anstelle der bisher üblichen Volkszählung. Erstmalig werden die Informationen nicht von den Bürgern eingeholt, sondern den vorliegenden Verwaltungsregistern entnommen. Die Basis dafür wurde mit dem *Registerzählungsgesetz*[523] vom 16. März 2006 geschaffen. Rund um das Zentrale Melderegister werden Basisregister wie das Gebäude- und Wohnungsregister, das Unternehmensregister und das Bildungsstandregister der Bundesanstalt *Statistik Österreich*[524] sowie das Register des *Hauptverbandes der österreichischen Sozialversicherungsträger*[525], die Daten des *Arbeitsmarktservice*[526] und die Stammdaten der Abgabenbehörden des Bundes herangezogen[527].

Zwei Bereiche der fortschreitenden Digitalisierung sollen nun exemplarisch betrachtet werden: E-Government und Vorratsdatenspeicherung.

2.3.3.1.1 E-Government

E-Government ist zum Schlagwort der Modernisierung des Staates geworden. Viele Behörden suchen über das Internet den Weg zur bürgernahen, effizienten Verwaltung. Die Präsenz umfasst

[523] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Registerzählungsgesetz [19. Juni 2007]
[524] http://www.statistik.at/ [28. Juni 2007]
[525] http://www.sozialversicherung.at/ [28. Juni 2007]
[526] http://www.ams.or.at/neu/ [28. Juni 2007]
[527] Vgl. http://www.sozialversicherung.at/esvapps/page/page.jsp?p_pageid=110&p_menuid=65846&p_id=5 [28. Juni 2007];
www.statistik.at/registerzaehlung/start.shtml+registerz%C3%A4hlung&hl=de&ct=clnk&cd=1&gl=at [28. Juni 2007]

Informationsangebote, verschiedene Kommunikationsmöglichkeiten und Transaktionen zwischen Bürgern und Verwaltung. Neuere Ansätze sehen Verfahren zur Abwicklung komplexer Verwaltungsdienstleistungen einschließlich Signatur und Bezahlfunktion vor. Die Verfahren umfassen den gesamten Workflow: Antragstellung, Vorlage von Unterlagen, Aktenführung, Verwaltungsentscheidung, Zustellung und die behördeninterne Dokumentation und Archivierung[528].

Der Umgang des öffentlichen Sektors mit seinen umfangreichen Informationssammlungen und oft sensiblen Daten ist entscheidend für die moderne Verwaltung und rechtsstaatliche Demokratie. E-Government bedeutet Verknüpfung von Daten, Austausch von Informationen und – im Stadium der E-Partizipation – auch politischer Überzeugungen. Vernetzte Register und Informationsverbundsysteme etablieren sich heute in allen staatlichen Bereichen und stellen hohe Anforderungen an den Datenschutz. Es existieren zwar – komplexe – Regelungen wie etwa das *bereichsspezifische Personenkennzeichen* (kurz: *bPK*) (siehe *2.4.7 Bereichsspezifisches Personenkennzeichen und Bürgerkarte im E-Government*), dennoch sind noch viele Maßnahmen notwendig, damit diese mit kundenfreundlichem *One-Stop-Government* vereinbar ist. Hier sind laufende Kontrollen durch unabhängige Einrichtungen, effektiver Rechtsschutz und Nachvollziehbarkeit essentiell. E-Government soll dem Individuum Zugang zu seinen eigenen Daten eröffnen, der Staat muss den Rahmen setzen, damit die Bürger ihr informationelles Selbstbestimmungsrecht (siehe *2.3.2.1 Informationelle Selbstbestimmung*) wahrnehmen können. Ein verfassungsrechtlich gewährleisteter Informationszugang kann zugleich das Vertrauen in den Staat fördern und die Zivilgesellschaft stärken. Ein elektronisches Transparenzgebot sowohl in der öffentlichen Verwaltung als auch in der Gesetzgebung stärkt die demokratische Kontrolle, Meinungsbildung und mündige Bürgerbeteiligung, festigt die Legitimität und letztlich auch die Akzeptanz von Entscheidungen. Wiewohl Transparenz durch IT im behördlichen Bereich gewünscht ist, muss angemerkt werden, dass „[…] *increased transparency could infringe privacy right. To be transparent governments will have to register more data about citiziens, which could make the position of citizens more vulnerable* […]“ [Frissen et al., 2007, S 78]. Dieser aktivierende E-Staat erfordert ein Zusammenspiel von Recht, Technik und Bewusstseinsbildung von Bevölkerung, öffentlichen Bediensteten und Verantwortlichen [Parycek, 2007, S 3].

2.3.3.1.2 Vorratsdatenspeicherung

Am 15. März 2006 wurde von der Europäischen Union die *Richtlinie zur Vorratsdatenspeicherung* (engl. *Data Retention*) beschlossen. Die Richtlinie *2006/24/EG*[529] hat zum Ziel, die unterschiedlichen nationalen Vorschriften der EU-Mitgliedsstaaten zur Speicherung von Telekommunikationsdaten auf

[528] Vgl. http://www.lfd.niedersachsen.de/master/C27872_N13151_L20_D0_I560.html+e-government+datenschutz&hl=de&ct=clnk&cd=2&gl=at [28. Juni 2007]
[529] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 32006L0024 [26. Juni 2007]

Vorrat zu vereinheitlichen. Durch die Harmonisierung soll sichergestellt werden, dass die Daten für mindestens ein halbes Jahr zum Zweck der Ermittlung und Verfolgung von schweren Straftaten aufbewahrt werden. Die Umsetzung in nationales Recht wurde mit 15. September 2007 für Telekomdaten bzw. mit 15. März 2009 für Internetdaten festgesetzt[530].

Telekomunternehmen müssen die Verbindungsdaten (siehe *2.3.2.3 Definition von Daten nach dem TKG 2003 bzw. Kommunikationsgeheimnis und* Datenschutz) von SMS, Festnetz- und Mobilfunkgesprächen speichern, beim Internet werden Daten zum Zugang sowie zur E-Mail-Kommunikation und Internet-Telefonie erfasst. Inhalte sollen hingegen nicht gespeichert werden.

Die Richtlinie ist politisch und rechtlich umstritten. Während ihre Befürworter die Vorratsdatenspeicherung als unverzichtbares Instrument zur Terrorismusbekämpfung und Strafverfolgung bezeichnen, verweisen ihre Kritiker auf die damit verbundenen Eingriffe in die Privatsphäre der Bürger, die sie als weiteren Schritt hin zum Überwachungsstaat ansehen[531].

In Österreich wurde die Richtlinie in Form einer Novelle[532] zum TKG 2003 bis zur Fertigstellung der vorliegenden Arbeit noch nicht umgesetzt.

2.3.3.2 Gefährdungen durch Internet und E-Mail

Millionen von Menschen bewegen sich durch das Internet und die meisten unterliegen dabei dem Irrtum zu glauben, sie bleiben anonym, solange sie nicht bewusst Daten von sich herausgeben. Wenngleich diverse Möglichkeiten bestehen, durch einen bewussten Umgang mit diesem Medium die Preisgabe der Privatsphäre zu beeinflussen und zu minimieren (siehe *2.4 Maßnahmen zum Schutz der Privacy*), so muss dennoch betont werden, dass eine absolute Anonymität nur in sehr eingeschränktem Maße erreichbar ist [Cas, Peissl, 2000, S 21f].

Sobald der Rechner mit dem Internet verbunden ist, ist er identifizierbar, jeder Besuch einer Webseite, jedes E-Mail hinterlässt Spuren. Die in diesem Abschnitt dargestellten Techniken zeigen, dass es kaum mehr möglich ist, sich unbeobachtet im Internet zu bewegen.

Sicherheit und Anonymität von Benutzern ist vor allem im Hinblick auf zukünftige Entwicklungen des Internets wichtig. Web 2.0 steht für Partizipation, sieht sich als Plattform für Endnutzer (siehe *1.1 Problemstellung und Herausforderung*). Dies birgt die Gefahr, dass die Nutzung ohne Wissen des Benutzers protokolliert und ausgewertet werden kann.

2.3.3.2.1 IP-Adresse/Internet Service Provider

Jeder Benutzer bekommt von einem Internet Service Provider entweder eine statische oder dynamische IP-Adresse zugewiesen. Dynamische IP-Adressen sind ausschließlich Verkehrsdaten,

[530] Vgl. http://www.internet4jurists.at/provider/speicherung1a.htm [26. Juni 2007]
[531] Vgl. http://www.e-center.co.at/html/index.php [26. Juni 2007]

statische IP-Adressen sind sowohl Verkehrsdaten als auch Stammdaten. Zur Erfüllung des Auskunftsbegehrens müssen Verkehrsdaten verarbeitet werden, da IP-Adressen Zugangsdaten im Sinne des *§92 Abs. 3 Z 4a TKG 2003* sind. Die Verwendung der Verkehrsdaten unterliegt der Vertraulichkeit gem. *Art. 5* der *RL 2002/58/EG*[533] bzw. dem Kommunikationsgeheimnis gem. *§93 Abs. 1 TKG 2003* und besonderen Verwendungsbeschränkungen gem. *Art. 6 und Art 15 Abs. 1* der *RL 2002/58/EG* bzw. *§92 Abs. 2* und *§99 TKG 2003*. Diese Daten dürfen daher nur gespeichert werden, soweit dies für Verrechnungszwecke notwendig ist oder soweit die ausdrückliche Einwilligung des Betroffenen vorliegt[534].

Die IP-Adresse beinhaltet per se keine geographischen Informationen. Es ist jedoch möglich, aufgrund der IP-Adresse Schlüsse auf den Aufenthaltsort des Rechners zu ziehen (siehe *1.4.1.5.1 WhoIs, 1.4.1.5.2 DNS, 1.4.2.2 Network Mapping*). Durch Hinzunahme weiterer Informationen können Datenbanken aufgebaut werden, die zu gegebener IP-Adresse die geographische Position des Benutzers sowie seinen Provider liefern (*Geolokation* einer IP-Adresse, z. B.: http://visualroute.visualware.com/ [19. Juni 2007]). Es ist zu beachten, dass Geolokation nicht immer zuverlässige Informationen liefert, da vielfach Techniken wie *Network Address Translation* (kurz: *NAT*)[535] oder Proxys (siehe *1.7.2.4.3 Proxy*) im Einsatz sind [Stamer, 2005, S 5].

Um im Internet surfen zu können, wird ein Zugang bei einem Internet Service Provider benötigt. Die dafür benötigten Daten zur Anmeldung (Name, Anschrift, Rechnungsadresse, Kontaktdaten) werden als Stammdaten (siehe *2.3.2.3 Definition von Daten nach dem TKG 2003 bzw. Kommunikationsgeheimnis und* Datenschutz) bezeichnet und beim ISP gespeichert.

Der ISP speichert Namen und Adresse, er zeichnet auf, wann der Internetbesuch erfolgt ist, samt der jeweiligen individuellen IP-Adresse.

2.3.3.2.2 HTTP-Header

Bei jeder HTTP-Anfrage werden neben den verpflichtenden einige optionale Header mitgeschickt. Alle Anfrageparameter, die vom Client geschickt werden, können vom Server gespeichert werden (siehe *2.3.3.2.5 Server Logfiles*). Um Daten über Clients zu erheben, sind insbesondere folgende Header interessant [Stamer, 2005, S 6f]:

- *Accept-Header*: Dieser gibt an, welche MIME[536]-Type der Client akzeptiert. Dies ermöglicht dem Server, die angeforderte Ressource in der vom Client gewünschten Form auszuliefern. Damit geht

[532] http://www.parlament.gv.at/portal/page?_pageid=908,4662640&_dad=portal&_schema=PORTAL [17. März 2008]
[533] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 32002L0058 [8. Juli 2007]
[534] Vgl. http://www.internet4jurists.at/provider/auskunft1a.htm [19. Juni 2007]
[535] NAT ist der Überbegriff für Verfahren, um automatisiert und transparent Adressinformationen in Datenpaketen durch andere zu ersetzen. Diese kommen typischerweise auf Routern und Firewalls zum Einsatz.
[536] MIME (steht für: Multi Purpose Internet Mail Extension) ist ein Standard, nach dem beliebige Daten (Dateien, Bilder etc.) in das Textformat von E-Mail konvertiert und so per E-Mail übertragen werden können.

einher, dass der Server gewisse Dokumenttypen vorziehen kann, die mehr Informationen über den Client offenbaren.

- Der *Accept-Language-Header* gibt an, welche Sprachen der Client akzeptiert. Die Sprache kann dazu beitragen, mehr über Aufenthaltsort oder Herkunft des Users zu erfahren.
- *User-Agent-Header:* Dieser enthält Informationen über die Anwendung, mit der die Ressource angefordert wurde. Dabei handelt es sich beispielsweise um Informationen über die Version des Browsers sowie des Betriebssystems.
- Der *Referer-Header* liefert wichtige Informationen über das User-Verhalten. Seine Funktion ist wie folgt beschrieben: „*The Referer request-header allows a server to generate lists of back-links to resources for interest, logging, optimized caching etc. It also allows obsolete or mistyped links to be traced for maintenance.*“ Wird eine Ressource angefordert, so enthält der Referer-Header die URL der Ressource, die den Link zur angeforderten Ressource enthält. Im Folgenden wird mit Referer der Referer-Header inklusive Referer-URL bezeichnet. Wurde die angeforderte Ressource nicht über einen Link besucht, so ist der Referer leer. Durch Auswertung des Referers lässt sich verfolgen, über welche Links Besucher auf eine Webseite gelangt sind oder über welche Suchbegriffe sie die Seite gefunden haben. Auch für Advertising-Netzwerke ist der Referer nützlich, da der Anbieter eines Banners mit Hilfe des Referers feststellen kann, über welche Webseite sein Banner angefordert wurde. Der Referer kann ein Risiko für die Sicherheit bzw. Anonymität darstellen. Bei GET-Anfragen kann der Query-String Werte enthalten (z. B.: GET / order […].cg i?name=Tom&c r e d i t+card=234876923234&PIN=1234 HTTP/1.1). Diese Daten werden im Referer-Header übermittelt, falls ein eingebettetes Objekt (z.B. Banner, Webbug) angefordert wird oder die Seite über einen Link verlassen wird. Es besteht also die Gefahr, dass die Daten ohne Wissen des Nutzers an Dritte übermittelt werden könnten.

2.3.3.2.3 Cookies

Ein Cookie ist eine Datei, die ein Webserver an einen Client sendet, der diese speichert und bei späteren Anfragen zurückschickt. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf eine Internetseite erkennbar. Cookies stellen keine direkte Gefahr dar, eröffnen aber Einblick in das Verhalten von Anwendern [Atzinger et al., 2002, S 14].

Eine Unterscheidung erfolgt in *First-party-Cookie* und *Third-party-Cookie*. Ersteres ist ein Cookie aus der angeforderten Domain, zweiteres ein Element aus einer anderen Domain (z. B. eines eingebetteten Banners oder Bildes). Zudem wird zwischen *Session-Cookies*, deren Gültigkeit mit der Session abläuft, und persistenten Cookies, die mit dem Gültigkeitsdatum ablaufen, unterschieden.

Cookies (*RFC 2109*[537]) wurden eingeführt, um das HTTP-Protokoll um eine Zustandsverwaltung[538] (Übergabe von Sitzungssdaten) zu erweitern. Die Verwaltung eines Zustandes ist die Voraussetzung, um Sitzungen[539] mit Clients zu unterstützen. Im Internet ist eine Sitzung eine logisch zusammenhängende Folge von Formularen, wobei jedes Formular von allen vorigen abhängen kann (z. B.: Einkaufswagen eines Online-Shops). Die Unterstützung von Sitzungen und somit von Zustandsverwaltung ist für viele Webanwendungen notwendig.

Die Verwendung von Cookies ist die verbreiteteste Art der Zustandsverwaltung. Andere Möglichkeiten der Implementierung einer Zustandsverwaltung sind *URL-Rewriting* oder versteckte Formularfelder. Der Client muss also nicht notwendigerweise Cookies akzeptieren, um Sitzungen mit einem Server zu unterstützen. Die Erweiterung des http-Protokolls durch Cookies ist optional und kann vom Client deaktiviert werden:

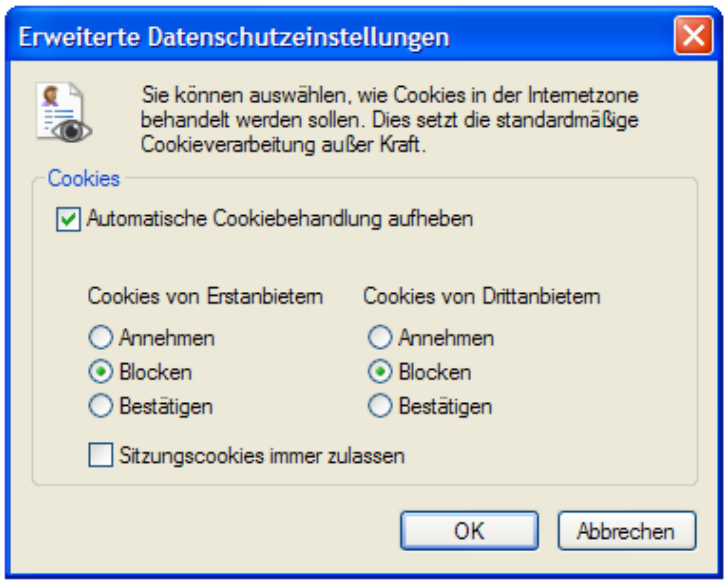


Abbildung 38: De-Aktivieren von Cookies im Internet Explorer 7

Durch die Überwindung der Zustandslosigkeit stellen Cookies ein effektives Mittel dar, um das Verhalten von Usern im Internet über einen längeren Zeitraum hinweg aufzuzeichnen. Dabei wird typischerweise eine eindeutige ID für einen User in einem Cookie abgelegt. Anhand dieser ID können alle Anfragen einem bestimmten Nutzer zugeordnet werden [Stamer, 2005, S 9].

[537] http://www.ietf.org/rfc/rfc2109.txt [20. Juni 2007]

[538] Zustandslosigkeit wird als die Eigenschaft eines Protokolls oder Systems bezeichnet, mehrere Anfragen (auch desselben Auftraggebers) grundsätzlich als voneinander unabhängige Transaktionen zu behandeln. Die Verbindung wird auch nach erfolgreicher Datenübertragung nicht aufrechterhalten.
Insbesondere werden Anfragen ohne Bezug zu früheren Anfragen behandelt und keine Sitzungsinformationen ausgetauscht und/oder verwaltet. Das Mitführen von Sitzungsdaten wird erst auf Anwendungsebene implementiert, beispielsweise durch die explizite Übermittlung einer Session-ID in jeder Anfrage in einem Cookie.

[539] Eine Sitzung bezeichnet die (zeitweise) bestehende Verbindung eines Clients mit einem Server.

Besonderes Augenmerk auf Kundenanalyse legen beispielsweise Amazon und Microsoft. Nach dem Vorbild von Amazon hat Microsoft im Mai 2006 ein sogenanntes „*Super-Cookie*“[540] patentiert. Damit wird durch die Registrierung aller Online-Bewegungen eine detailgenaue Kundenbeobachtung möglich. Die Ergebnisse der Datensammlung helfen dem Anbieter, seine Produkte personalisiert für jeden einzelnen Kunden zielgruppengerecht anzubieten (siehe *2.2.4 Personalisierung*). Ähnlich wie bei Amazon ist es dadurch möglich, Werbeangebote zu platzieren, jedoch ohne dass hierfür ein Login notwendig wäre. Microsoft verspricht sich von dem zugesprochenen Patent deutliche Zuwächse im Bereich der Kundenbindung und eine damit verbundene Erhöhung der elektronischen Einkäufe.
Die Entwicklung der Cookies hat einen weiteren Schub erfahren. Das Magazin für Computertechnik *c't* [c't, 2007, S 224] berichtet von drei neuen Methoden:

- *Flash-Cookie*: Flash (steht für: Adobe-Flash, ehemals Macromedia-Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte, die vielfach im Einsatz ist (u.a. Google, Yahoo). Der Flash Player kann kleine Textdateien, sogenannte *Local Shared Objects* (kurz: *LSO*s), auf dem Rechner des Anwenders abspeichern, die den gleichen Zwecke wie HTTP-Cookies erfüllen. Problematisch ist dabei der Umstand, dass diese LSOs nicht von der Cookieverwaltung des Browsers administriert werden und bei Bedarf manuell gelöscht werden müssen.
- *DOM-Storage-Object* (Firefox): Basiert auf der Spezifikation für *Web Applications 1.0* der *WHAT WG*[541]. Das noch in Entwicklung begriffene Web Applications 1.0 gilt als Vorstudie zum künftigen X(HTML)5 und enthält Abschnitte, welche sich unabhängig von der übrigen Spezifikation implementieren lassen, wie etwa „*client-side session and persistent storage*“. Ähnlich den Flash-Cookies bietet DOM-Storage erheblich mehr Platz als Cookies. Anders als die http-Cookies kommuniziert der Datenspeicher nicht direkt mit dem Webseiten-Skript auf dem Client.
- *userData* (Internet Explorer): Microsoft arbeitet hier nach einem Konzept namens „*Behaviors*“. Zu den Behaviors zählt „*persistence*“, um skriptgesteuerte History, Lesezeichen, Webseiten und beliebige Daten (userData) zu speichern. Größenbeschränkung wie Zugriff gelten unabhängig von Protokoll und Verzeichnis. Immerhin ist es möglich, userData gemeinsam mit den Cookies zu löschen.

Kein einziger Browser bietet die Möglichkeit, Flash-Cookies, DOM-Storage-Objects oder userData einzusehen. Der Anwender erfährt nicht, wo die Daten liegen, was sie enthalten, wer darauf zugreifen kann.

[540] Vgl. http://www.pressetext.de/pte.mc?pte=060508040 [22. Juni 2007]
[541] http://www.whatwg.org/ [22. Juni 2007]

2.3.3.2.4 Webbug

Als Webbugs (auch: Webspion) werden kleine, unsichtbare Grafiken (1x1-Pixel, transparent) bezeichnet, die in HTML-Mails (siehe *2.3.3.2.8 E-Mail*) bzw. auf Webseiten platziert werden, um Useraktivitäten zu protokollieren [c't, 2006-3, S 205].

Ein entsprechender HTML-Tag könnte folgendes Aussehen haben: <*img src="http://www.bigbadcompany.com/cgi-bin/screw-your-privacy.cgi"*>. Auffällig dabei ist, dass als Quelle für das Bild keine gewöhnliche Grafikdatei (z. B. *.gif, *.jpg) angegeben ist, sondern ein CGI-Skript aufgerufen wird, das ein solches Bild zurückliefert. Durch den Aufruf eines Skripts werden Informationen wie beispielsweise IP-Adresse, verwendetes Betriebssystem oder Referer-Information (siehe *2.3.3.2.2 HTTP-Header*) mitgeliefert.

Webbugs sind insbesondere in Kombination mit JavaScripts (siehe *1.4.3.5.1 Cross Site-Scripting*) und Cookies wirksam. Wird beim Aufruf des Webbugs ein Cookie mitgeschickt, so kann darin beispielsweise die ID eines Benutzers übermittelt werden. Mit JavaScript können Informationen an die URL des Bildes angehängt und so dem Server des Webbugs mitgeteilt werden [Stamer, 2005, S 10].

Das Verhalten des Users lässt sich dann sowohl über eine einzelne als auch über mehrere Sessions hinweg verfolgen.

2.3.3.2.5 Server Logfiles

Die beim Besuch einer Webseite getätigten Zugriffe werden auf dem Webserver protokolliert. Gespeichert werden – abhängig vom Logfile-Format – üblicherweise: Client-IP-Adresse, Zeit/Datum der Anfrage, Anzahl übertragender Bytes, HTTP-Status-Code, Referer etc. [Stamer, 2005, S 10]. Darüber hinausgehend werden häufig noch weitere Daten gespeichert: Browserversion des Clients, Angaben zum verwendeten Betriebssystem oder Angaben zur Konfiguration des Rechners.

Es gibt eine große Anzahl von Tools, welche Logfiles auswerten und die Daten in graphischer Form darstellen. Mit den aufgezeichneten Daten lassen sich beispielsweise Statistiken erstellen oder Benutzeraktivitäten verfolgen (siehe *2.3.3.2.6 Google Analytics*).

Für die Analyse der Daten sind unter anderem folgende Begriffe von Bedeutung [Atzinger et al., 2002, S 11] (detailliertere Informationen zur Webanalyse zu finden unter: http://www.analyticstools.com/ [8. Juli 2007]):

- *Visit*: Jeder Besucher erzeugt unabhängig von der Aufenthaltsdauer einen Visit.
- *Page View*: Jeder Aufruf einer HTML-Seite erzeugt einen Page View (oder *Page Impression*). Dabei spielt es keine Rolle wie viele Graphiken die HTML-Seite beinhaltet.
- *Hit:* Das Aufrufen einer HTML-Seite, einer Graphik oder eines Scripts erzeugt jeweils einen Hit. Die Anzeige einer kompletten Website im Browser erzeugt also mehrere Hits: z. B. eine HTML-Seite mit 5 Graphiken erzeugt 6 Hits. Jeder Hit erzeugt im Logfile einen Zeileneintrag.
- *Request*: Jede erfolgreiche Anforderung einer Seite, Grafik etc. erzeugt einen Hit.

- *Ad Click*: Die Anzahl der Klicks auf ein Werbe-Banner wird mit Ad Click bezeichnet.

Eine Erweiterung des Server Logging, die mehr Informationen über das Verhalten von Benutzern offenbart, ist die *Clickstream-Analyse*. Um ein genaues Benutzerprofil zu generieren, werden bei der Clickstream-Analyse möglichst alle Aktivitäten des Benutzers aufgezeichnet. Häufig werden zur Analyse von Clickstreams auch Formulareingaben hinzugezogen. So können beispielsweise Suchbegriffe oder betrachtete Artikel einem Benutzer zugeordnet werden. Dies ermöglicht insbesondere bei Webseiten, die eine Authentifizierung des Nutzers verlangen, detaillierte Nutzerprofile zu erstellen (siehe *2.3.3.2.7 Portale*).
Ein Beispiel für einen Anbieter, der Clickstreams von Kunden speichert, ist Amazon. In der Datenschutzerklärung[542] (siehe *2.4.2.1 Platform for Privacy Preferences*) wird gesagt, dass Amazon jeden Schritt eines Kunden speichert: „*Wir erfassen und speichern alle Informationen, die Sie auf unserer Website eingeben oder uns in anderer Weise übermitteln*." Diese Praxis von Amazon stößt auf Kritik, da sie eine Gefahr für die Privatsphäre der Kunden darstellt [Stamer, 2005, S 13].

2.3.3.2.6 Google Analytics

Google Analytics[543] ist ein kostenloser, frei verfügbarer Dienst, welcher zur Analyse von Zugriffen auf Webseiten genutzt werden kann.
Neben der von anderen Analyseprogrammen bekannten Funktionen wie Herkunft der Besucher, Verweildauer und Suchbegriffe in Suchmaschinen bietet Google Analytics den Vergleich von Suchbegriff-Kampagnen, kurze Zusammenfassungen und Trendberichte, die Visualisierung von Ausstiegspunkten und Landkarten mit Besucherstatistiken. Das Programm kann auch die Klickraten auf alle Links, graphisch über die Seite eingeblendet, anzeigen. E-Mail-Berichte und benutzerdefinierbare Übersichtskonsolen sollen es den Webseitenbetreibern leichter machen, die richtigen Informationen aus den Daten herauszuarbeiten[544].
Eine konkrete Gegenmaßnahme ist beispielsweise die Verwendung der Firefox-Browsereigenschaft „NoScript". Damit werden die IP-Adresse und der Zeitstempel für ein Auslesen unterdrückt.

2.3.3.2.7 Portale

Als Webportal wird eine Anwendung bezeichnet, die über einen zentralen, personalisierten Zugang verschiedene Services bereitstellt. Diese können beispielsweise E-Mail, Nachrichten (engl. *News*), Einkaufsmöglichkeit und Suchdienst sein. Webportale sind für den Benutzer meist kostenlos und

[542] Vgl. http://www.amazon.de/gp/help/customer/display.html/028-5455695-4361333?ie=UTF8&nodeId=3312401 [8. Juli 2007]
[543] http://www.google.ch/analytics/de-DE/ [22. Juni 2007]
[544] Vgl. http://www.heise.de/newsticker/meldung/89509/from/rss09 [22. Juni 2007]; http://www.golem.de/0608/47201.html [22. Juni 2007]

finanzieren sich in der Regel über Werbung. Beispiele für Portale sind *Yahoo*[545] oder *MSN*[546]. Bei Webportalen neuerer Generation (Google, Microsofts *Live*[547]) steht den Usern offen, diese zu personalisieren und nach eigenen Vorstellungen zu gestalten. Dazu stehen *RSS-Feeds*[548], diverse *Gadgets* (Wettervorhersage, Horoskop, Aktienkurse, Uhr etc.), Funktionen wie stufenlos variierbare Darstellung von Bildern oder konfigurierbare Makrosuche in selbst definierten Webseiten zur Verfügung.

Die Negativseite von RSS-Feeds haben Mitglieder der Studenten-Community *Facebook*[549] kennen gelernt[550]. Der News-Feed hat automatisiert Informationen über sämtliche Aktivitäten (Hinzufügen von neuen Freunden, Änderung des Beziehungsstatus etc.) auf den Seiten befreundeter User gesendet. „*Obwohl es scheinbar der MySpace-Generation nicht viel auszumachen scheint, persönliche Details im Internet zu publizieren, sorgte diese Anwendung, die den Usern die Spionagearbeit abnimmt, für weitreichende Proteste*“, hat die *New York Times*[551] den Vorfall kommentiert.

Da sich ein Benutzer bei einem Portal anmeldet, können sämtliche Aktionen des Benutzers verfolgt und ausgewertet werden. Dies ermöglicht dem Portalbetreiber ein detailliertes Nutzerprofil zu erstellen, um sein Angebot möglichst genau auf die Benutzer zuzuschneiden (siehe *2.2.4 Personalisierung*). Genau darin liegt die Gefahr der Privatrechtsverletzung, da nicht immer transparent ist, welche Daten gespeichert werden und was mit ihnen passiert (siehe *1.9 Exkurs: Google*) [Stamer, 2005, S 20f].

2.3.3.2.8 E-Mail

E-Mails können sowohl im *Plain Text-Format* als auch im *HTML-Format* verschickt und empfangen werden. Während E-Mails im Plain Text-Format keine Risiken bergen, bestehen bei HTML-Mails Gefahren für die Anonymität der Benutzer. Auf sicherheitstechnische Bedenken wird nicht weiter eingegangen, da diese bereits in vorigen Kapiteln (siehe *1.3.4 Computer Anomalien/Malicious Code, 1.4.1.2 Exkurs: Phishing, 1.4.1.2.1 Pharming, 1.6 Exkurs: E-Mail/Spam*) erörtert wurden. HTML-Mails sind den in vorigen Abschnitten beschriebenen Gefährdungen durch Cookies, Webbugs oder Referer ausgesetzt. Bei E-Mails ist das primäre Ziel der Datenerhebung nicht die Benutzerprofilerstellung, sondern die Feststellung, ob eine E-Mail-Adresse gültig ist bzw. ob und

[545] http://www.yahoo.com/ [20. Juni 2007]
[546] http://at.msn.com/ [20. Juni 2007]
[547] http://www.live.com/ [20. Juni 2007]
[548] Really Simple Syndication (kurz: RSS) ist ein elektronisches Nachrichtenformat, das dem Benutzer ermöglicht, die Inhalte einer Webseite (oder Teile davon) als sogenannte RSS-Feeds zu abonnieren oder in andere Webseiten zu integrieren. Die Abgrenzung zum normalen Webbrowser besteht darin, dass aktuelle Nachrichten automatisch geladen werden, wenn ein Kanal (engl. Feed) einmal abonniert ist. Im Unterschied zu E-Mail geht die Initiative von dem Empfänger aus, der den Feed anwählte, sprich, der Anbieter kann die Leser nicht auswählen.
[549] http://www.facebook.com/ [22. Juni 2007]
[550] Vgl. http://www.pressetext.at/pte.mc?pte=060911002 [22. Juni 2007]

wann eine E-Mail gelesen wurde. Dies kann dadurch erreicht werden, indem ein Bild mit HTML-Code in eine E-Mail eingefügt wird (siehe *2.3.3.2.4 Webbug*). Je nach Mail-Client können bei der Anfrage nach einer Ressource (z. B.: einem Bild, Flash-Objekt) Informationen über den eingesetzten Mail-Client übertragen werden. Diese Informationen könnten genutzt werden, um Mail-Client-spezifische Sicherheitslücken auszunutzen [Stamer, 2005, S 13].

Viele Free-E-Mail-Provider blenden in der Fußzeile von verschickten E-Mails Werbung ein. Dabei handelt es sich vielfach um zufällig eingefügte Banner. In der letzten Zeit zeichnet sich jedoch ein Trend hin zu kontextsensitiver Werbung ab. Um kontextabhängige Werbung einblenden zu können, muss jede E-Mail gelesen werden. Dies tangiert zum einen die Privatsphäre der Benutzer, zum anderen sind die rechtlichen Auswirkungen strittig. Ein bekannter Free-E-Mail-Provider, der kontextsensitive Werbung einsetzt, ist Gmail, weiterführende Erläuterungen dazu siehe unter *1.9.1.1.2 Datenschutz bei Google*.

2.3.3.2.9 Angriff auf Informationssicherheit und die Verwendung von Malicious Code-Tools

An dieser Stelle ist auf das erste Kapitel zu verweisen, wo viele – nicht nur technische – Möglichkeiten (siehe *1.3 Taxonomie von Angriffen auf den Wert Information* und *1.4 Unberechtigte Informationsbeschaffung und unberechtigter Zugriff*) aufgezeigt wurden, die Sicherheit von Systemen zu kompromittieren und damit die Privatsphäre der Benutzer zu gefährden.

Erwähnung finden soll jedoch die Zunutzemachung einiger dieser Werkzeuge und Techniken. In vielen Ländern gibt es Diskussionen und Überlegungen über die Schaffung von Grundlagen für den Einsatz von Trojanern und Keyloggern zur Überwachung von Verdächtigten durch behördliche Institutionen. Als Online-Durchsuchung wird der technische Zugriff einer Behörde auf Daten ohne Wissen des Betroffenen bezeichnet. Sie ist keine Durchsuchung im eigentlichen Rechtssinne, dient jedoch ebenso wie diese dazu, Informationen zu beschaffen und Beweismittel zu erlangen. Beiden Durchsuchungsarten ist gemein, dass sie erheblich in die Privatsphäre des Betroffenen eingreifen. Der Unterschied liegt darin, dass die Online-Durchsuchung geheim durchgeführt wird.

Die USA hat als Reaktion auf Anschläge vom 11. September 2001 mit dem *USA Patriot Act* (steht für: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*)[552] ein Bundesgesetz verabschiedet, das sich verstärkt dem Krieg gegen den Terrorismus widmet. Es bringt eine Einschränkung der amerikanischen Bürgerrechte in größerem Maße mit sich, aber auch Auswirkungen für USA-Reisende, da die Anforderungen an Pässe erhöht wurden. Konkret sind etwa folgende Inhalte hinsichtlich Privacy enthalten [Fleissner, 2005, S 82]:

- minimiert richterliche Kontrolle bei Überwachungen und Abhöraktionen,

[551] http://www.nytimes.com/ [22. Juni 2007]
[552] http://www.whitehouse.gov/infocus/patriotact/ [21. Juni 2007]

- erlaubt Durchsuchungen auch in Abwesenheit der Bewohner ohne Durchsuchungsbefehl,
- ermöglicht FBI-Zugang zu sensiblen Daten ohne Gerichtsbeschluss und konkrete Hinweise (Universitäten, Psychiater, Kreditinstitute),
- erlaubt dem Auslandsgeheimdienst CIA auch im Inland zu spionieren,
- erleichtert Informationsaustausch zwischen Polizei und Geheimdiensten,
- verschärft Strafen für Computerkriminalität drastisch, kann als „*terrorist offense*“ eingestuft werden.

Bekannt ist der vom FBI eingesetzte Trojaner „*Magic Latern*“[553], der einen Teil des Spywareprogramms „*Carnivore*“[554] darstellt. Zudem wird vom FBI „*CIPAV*“ (steht für: *Computer and Internet Protocol Address Verifier*) verwendet, mit dem es möglich ist, trotz Viren- und Firewallschutz in einen PC einzudringen. In diesem Zusammenhang kommen etablierte Antiviren-Hersteller zunehmend unter Verdacht, mit den Behörden hinsichtlich solcher Geheimmissionen zu kooperieren. Werden die Signatur-Datenbanken für derartige Spyware-Programme vorbereitet, bleibt die Spyware auf dem Computer unentdeckt. Bisher haben alle etablierten Security-Anbieter stets offiziell versichert, dass auch für Behörden keine Ausnahmen gemacht werden[555].
Ein anderes bekanntes, wenn auch geheimes, weltweites Spionagesystem ist „Echelon“[556] [Janowicz, 2006, S 201].
In Deutschland gibt es anhaltende Diskussionen um die Ausweitung der Anti-Terrorgesetze[557] und den sogenannten „Bundestrojaner“[558]. Eine Grundsatzentscheidung hat der Bundesgerichtshof im Februar 2007 getroffen, indem er die heimliche Online-Durchsuchung von Computern für unzulässig erklärt hat[559]: „*Die Grundsätze des Rechtsstaates verlangen, dass der Staat die Privatsphäre seiner Bürger unbedingt respektiert, auch dann, wenn sie eines Verbrechens verdächtigt werden. So sollen bei einer Hausdurchsuchung möglichst der Beschuldigte selbst oder unabhängige Zeugen anwesend sein. Das Verbot verdeckter Ermittlungen gelte auch für das Internet.*“

[553] Vgl. http://www.heise.de/tp/r4/artikel/11/11333/1.html [21. Juni 2007]
[554] Vgl. http://www.heise.de/tp/r4/artikel/4/4288/1.html [21. Juni 2007]; http://www.epic.org/privacy/carnivore/ [21. Juni 2007]
[555] http://www.heise.de/newsticker/meldung/92914 [23. Juli 2007]
[556] An Echelon sind neben den USA die englischsprachigen Staaten United Kingdom, Kanada, Australien und Neuseeland beteiligt. Zunächst wurde Echelon für das Abhören der militärischen und diplomatischen Kommunikation der ehemaligen Sowjetunion und ihrer Verbündeten eingesetzt. Heute findet das System – höchstwahrscheinlich – in der Überwachung des Drogenhandels, von terroristischen Aktivitäten und in der Wirtschaftsspionage Verwendung. Vgl. http://www.heise.de/tp/r4/special/ech.html [21. Juni 2007]; http://www.echelonwatch.org/ [28. Juni 2007]
[557] Vgl. http://www.heise.de/newsticker/meldung/75193 [21. Juni 2007]; http://www.heise.de/newsticker/meldung/75621 [21. Juni 2007]
[558] Vgl. http://www.heise.de/security/artikel/86415/0 [21. Juni 2007]; http://www.sueddeutsche.de/,Ple5Lrs/computer/artikel/65/93971/ [21. Juni 2007]; http://www.bundestrojaner.de/ [21. Juni 2007]

Weiters wird argumentiert: „*Bei den verdeckten Online-Durchsuchungen muss, wie seit dem 11. September 2001 üblich, die Terrorgefahr, und neuerdings nun auch die Kinderpornographie zur Begründung herhalten. Keine Frage, der Staat trägt eine hohe Verantwortung, seine Bürger zu schützen. Aber er darf sie nicht schützen, indem er das Recht beugt*."

In Österreich steht *Lauschangriff* für die optische und akustische Überwachung von Personen unter Verwendung technischer Mittel. Diese Form der Beweisgewinnung ist in Österreich – wie auch die *Rasterfahndung* – seit 1997 in *§149d StPO* geregelt. Überwacht werden nicht-öffentliches Verhalten bzw. Äußerungen von Personen in Form von Bild/Tonübertragung und -aufzeichnung. Kontrolliert und geprüft wird die Anordnung und Durchführung des Lauschangriffes durch unabhängige Rechtsschutzbeauftragte. Anfangs wurde der Lauschangriff nur unter Probe eingeführt, da es erhebliche Bedenken gegen Eingriffe in die Privatsphäre gab. Doch mittlerweile ist diese Form der Überwachung zur Verbrechensbekämpfung in Österreich unumstritten[560].

Im Sommer 2007 hat die Diskussion[561] darüber begonnen, in Österreich den Einsatz von technischen Spionagetools zu legalisieren. In Überlegung ist, einen Trojaner, ähnlich dem in Deutschland eingesetzten, mit dem Argument „[…] *wir müssen im tagtäglichen Wettlauf mit den Kriminellen ständig auf dem Laufenden sein* […]" zu verwirklichen[562].

2.3.3.2.10 ICANN

ICANN[563] (steht für: *Internet Corporation for Assigned Names and Numbers*) ist eine privatrechtliche Non-Profit-Organisation amerikanischen Rechts mit Sitz in Kalifornien. Aufgabe ist es, die Stabilität und Sicherheit des Internets – konkret: des Domain Name Systems mit seinen 13 zentralen Root-Servern – zu gewährleisten. Die Organisation entscheidet über die Grundlagen der Verwaltung von Namen und Adressen im Internet und beschließt technische Verfahrensstandards. Auf diese Weise koordiniert ICANN technische Aspekte des Internet, ohne jedoch verbindliches Recht zu setzen. ICANN untersteht der amerikanischen Regierung und wird als eine Art „Weltregierung des Internets" bezeichnet[564]. Die Regierungen der Welt haben bei ICANN lediglich Beraterstatus, sie sind im Regierungsbeirat *Governmental Advisory Committee* vertreten, der auch einen eigenständigen Sitz bei der EU-Kommission in Brüssel hat. Dieser Status der Staaten wird mit Blick auf die Vormachtstellung der US-Regierung und deren staatliche Aufsicht vielfach kritisiert und ist Gegenstand von Diskussionen über die künftige Struktur, zumal in den USA der Datenschutz nicht jene Rolle wie in

[559] Vgl. http://www.bundesgerichtshof.de/ [21. Juni 2007]; http://www.stern.de/computer-technik/internet/587865.html?nv=ct_mt [21. Juni 2007]
[560] Vgl. http://www.bmi.gv.at/oeffentlsicherheit/2001/11_12/artikel_4.asp [21. Juni 2007]
[561] Vgl. http://futurezone.orf.at/it/stories/201047/ [21. Juni 2007]; http://www.wirtschaftsblatt.at/home/schwerpunkt/itnews/317142/index.do [17. März 2008]
[562] Vgl. http://www.kurier.at/interaktiv/meinungen/83066.php [21. Juni 2007]
[563] http://www.icann.org/ [21. Juni 2007]
[564] Vgl. http://www.heise.de/ct/icann/ [25. Juni 2007]

Europa genießt (siehe *2.3.2 Rechtliche Belange*). Im Dezember 2006 verlängerten die US-Regierung und ICANN ihr bisheriges „*Memorandum of Understanding*“ durch ein sogenanntes „*Joint Project Agreement*“ um weitere drei Jahre[565]. Die US-Regierung machte dadurch deutlich, dass sie nicht gewillt ist, ihren Einfluss aufzugeben, Zugeständnisse an die anderen Länder gibt es nur bedingt[566].
Bestätigt werden diese Entwicklungen aus österreichischer Sicht in einem Interview (Juni 2007)[567] mit *Richard Wein*, dem Geschäftsführer der österreichischen Registrierungsstelle *nic.at*[568]:
„[…] *Wer soll künftig „Herr des Internets“ sein?*
Wein: Das ist schwer zu sagen. Die Diskussion darüber, wie stark Regierungen in das Internetgefüge eingebunden sind, wird die Community in den nächsten Jahren stark beschäftigen. In Österreich haben wir damit kein Problem, die Zusammenarbeit mit dem Bundesministerium für Verkehr, Innovation und Technologie und der Rundfunk und Telekom Regulierungs-GmbH läuft sehr gut. International gibt es zum Beispiel von Seiten Brasiliens oder Syriens starke Regulierungsbedürfnisse gegenüber dem doch US-lastigen System Internet. Das wird in den kommenden Jahren zu heftigen Diskussionen führen.
Welche Lösungsansätze gibt es hierfür?
Wein: Es wird die Einführung neuer Gremien diskutiert, die ähnlich der UNO nach dem Prinzip "one seat, one voice" organisiert sind. Daneben gibt es Bestrebungen, die oberste Internetverwaltungsstelle ICANN stärker zu internationalisieren. Wichtig ist dabei, dass ein Gremium geschaffen wird, das dann auch mit genug Macht ausgestattet ist, gewisse Dinge umzusetzen […]“.

2.3.3.3 RFID

RFID (steht für: *Radio Frequency Identification*) ist ein Verfahren zur automatischen Identifizierung von Gegenständen (Produkten, Bargeld, Ausweisdokumenten, Fahrkarten etc.) und Lebewesen. Neben der berührungslosen Identifizierung und der Lokalisierung von Objekten ohne Sichtkontakt steht RFID für die automatische Erfassung und Speicherung von Daten. Eine RFID-Systeminfrastruktur umfasst einen Transponder (oder: *Tag*), ein Sende-Empfangs-Gerät sowie ein im Hintergrund wirkendes IT-System. Herzstück der Technologie bildet der Transponder – ein winziger Computerchip mit Antenne. Der Chip ist in ein Trägerobjekt (Klebeetikett, Plastikkarte etc.) integriert und mit einem Nummerncode versehen. Dieser verschlüsselt Informationen, die in einer Datenbank hinterlegt werden. Dadurch erhält jeder Gegenstand mit RFID-Transponder eine unverwechselbare Identität.
Um die gespeicherten Informationen zu erfassen, sind spezielle Lesegeräte erforderlich. Die Sende-Empfangs-Einheit erzeugt ein elektromagnetisches Feld, das von der Antenne des RFID-Transponders empfangen wird. Der Transponder sendet daraufhin den Nummerncode an das Lesegerät. Je nach

[565] Vgl. http://www.icann.org/announcements/announcement-29sep06.htm [25. Juni 2007]
[566] Vgl. http://www.heise.de/newsticker/meldung/61294 [25. Juni 2007]
[567] Vgl. http://www.pressetext.at/pte.mc?pte=070623005 [25. Juni 2007]

Frequenzbereich, Sendestärke und ortsabhängigen Umwelteinflüssen können Daten aus einer Distanz von wenigen Zentimetern bis zu mehreren Metern gelesen werden. Ähnlich wie sich im Internet Auskünfte zu Personen oder Unternehmen auf deren Homepage finden lassen, ist dies auch für Objekte möglich. Hierzu leitet das Lesegerät die Zahlenkombination an eine Datenbank weiter. Das IT-System entschlüsselt den Code und verknüpft ihn mit Informationen, die in der Datenbank oder auch im Internet hinterlegt sind. Das Wissen des Systems liegt dabei nicht im Transponder, sondern in den Datenbanken.

Bereits heute setzen Industrie und Handel auf RFID, weil sie damit ihre Geschäftsprozesse optimieren, Prozesskosten senken und Produktsicherheit erhöhen können. Es existieren die unterschiedlichsten Einsatzmöglichkeiten, vor allem können RFID-Systeme den Alltag vieler Privatpersonen erleichtern und die Abläufe in der Arbeitswelt vereinfachen. Zurzeit stehen einer flächendeckenden Nutzung von RFID allerdings noch die hohen Stückkosten der Transponder entgegen[569].

Auf der anderen Seite kommen mit den positiven Eigenschaften datenschutzrechtliche Fragen auf. Ein Verstoß gegen die Datenschutzbestimmungen liegt dann vor, wenn Personen mit Transpondern ausgestattet werden und diese dann heimlich gelesen werden. Ein RFID-Transponder ist ein Speicher, in dem persönliche Daten hinterlegt werden können. Es stellt sich die Frage, wie sich diese Daten schützen lassen.

Zudem können mittels RFID durch die Zuordnung von Aufenthaltsorten und Zeitpunkten zu einer Person personenbezogene Daten[570] erzeugt werden, die einen Eingriff in die Privatsphäre bedeuten können. Dies kann zum Beispiel in Unternehmen der Fall sein, die ihren Mitarbeiter mit Transpondern versehene Firmenausweise aushändigen, um dann deren Gewohnheiten am Arbeitsplatz auszulesen.

Selbst wenn lediglich Objekte mit Transpondern ausgestattet werden, kann dies zu datenschutzrechtlichen Problemen führen, wenn Kunden Produkte kaufen, die ohne deren Wissen mit Transpondern versehen sind. Wird beispielsweise ein Transponder in einem Auto angebracht, dann könnte mit diesen Transpondern (theoretisch) nachverfolgt werden, wohin der Käufer im Laufe der Zeit fährt, in der das Auto in seinem Besitz ist. Zusammen mit anderen Informationen, die andere Transponder beziehungsweise Lesegeräte liefern, könnte dann ein fast vollständiges Bild von einer Person erstellt werden, ohne dass diese Person überhaupt ahnt, dass sie ausspioniert wird.

American Express[571] hat ein Modell (März 2007) zum Tracken der Kundenbewegungen über RFID-Chips in ihren Kreditkarten entwickelt[572]. Ein anderes Beispiel gibt es von der *Washington University*[573] zu berichten. Die Firmen *Apple*[574] und *Nike*[575] bieten das Produkt *Nike+iPod-Kit* an.

[568] http://www.nic.at/ [25. Juni 2007]
[569] Vgl. http://www.info-rfid.de/technologie/25.html [26. Juni 2007]; http://www.rfid-journal.de/ [26. Juni 2007]
[570] Vgl. http://sicherheitskultur.at/RFID_privacy.htm [26. Juni 2007]
[571] http://www.americanexpress.com/ [26. Juni 2007]
[572] Vgl. http://www.spychips.com/press-releases/american-express-conference.html [26. Juni 2007]
[573] http://www.washington.edu/ [26. Juni 2007]

Dabei sendet der RFID-Chip im Schuh an einen Empfänger im iPod die Schritte des Besitzers und der iPod berechnet daraus die zurückgelegte Entfernung, die Geschwindigkeit und den Kalorienverbrauch. Die Wissenschaftler haben ein Gerät gebaut, mit dem auf bis zu 20 Meter Entfernung die Geräte (an Hand ihrer internen ChipID) identifiziert und in Google Earth angezeigt werden können. Die Organisation *CASPIAN* (steht für: *Consumers Against Supermarket Privacy Invasion and Numbering*) setzt sich seit 1999 gegen Überwachungskonzepte ein und dokumentiert auf ihrer Webseite[576] Vorfälle solcher Art.

Aus Privacy-Sicht liegt die Gefahr der RFID-Technik im Verlust der informationellen Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung*). Die einzelne Person hat durch die versteckten Sender keinen Einfluss mehr darauf, welche Informationen preisgegeben werden.

2.3.3.4 Pervasive Computing/Internet der Dinge

Der Begriff *Pervasive Computing* (auch: Ubiquitäres Computing (siehe *1.5.2 Ubiquitäres Computing*)) oder *Internet der Dinge* (engl. *Internet of Things*) steht für die elektronische Vernetzung des Alltags durch den Einsatz *intelligenter* Gegenstände. Die Idee ist, dass Dinge (Objekte), die mit einer eigenen Intelligenz ausgestattet sind, selbstständig Informationen austauschen[577]. Computerprozessoren und Sensoren werden laufend kleiner und billiger, drahtlose Kommunikation ist nahezu überall verfügbar (siehe *1.5.3 Personal Area Network, 1.5.4 Local Area Network, 1.5.5 Wide Area Networks*). Durch automatisiertes Sammeln (z. B.: durch RFID – siehe *2.3.3.3 RFID*) und Auswerten (z. B.: durch Data Mining – siehe *2.2.5 Data Mining*) von Daten können Persönlichkeitsprofile generiert werden.

Ein Trend, der sich in diesem Bereich abzeichnet, ist der des *Wearable Computing*. Wearables sind elektronische Geräte, die am Körper getragen werden oder in die Kleidung integriert sind. Das Funktionsspektrum der Wearables umfasst die Erfassung und Verarbeitung von Körper- und Umgebungsdaten sowie die Kommunikation über das Internet oder lokale Netze [TA-Swiss, 2003, S 96].

Mit Pervasive Computing sind weitreichende Folgen für die Gesellschaft verbunden. Ein wesentliches Thema dabei ist der Einfluss von Pervasive Computing auf Privacy [TA-Swiss, 2003, S 267f].

2.3.3.5 Digital Rights Management

Digitale Rechteverwaltung (engl. *Digital Rights Management* (kurz: *DRM*)) ist ein Verfahren, mit dem die Verbreitung digitaler Inhalte kontrolliert werden kann. Die Rechteverwaltung findet bei digitalen Film- und Tonaufnahmen, bei Software und elektronischen Dokumenten (Bücher, E-Mails, Geschäftsmodelle etc.) Verwendung und ermöglicht den Rechteinhabern Abrechnungsmöglichkeiten

[574] http://www.apple.com/ [26. Juni 2007]
[575] http://www.nike.com/index.jhtml [26. Juni 2007]
[576] http://www.spychips.com/ [26. Juni 2007]

für Lizenzen und Rechte sowie Kontrollmechanismen über die Nutzung der Daten. DRM ist darauf ausgerichtet, digitales geistiges Eigentum zu schützen.

DRM-Systeme verwirklichen die Idee der Zugriffskontrolle digitaler Inhalte mit Hilfe kryptografischer Verfahren (siehe *1.7.2.1 Kryptologie*). Realisiert wird dies, indem ein beliebiger digitaler Inhalt durch Verschlüsselung eindeutig an eine Lizenz gebunden wird. Ohne die zum digitalen Inhalt gehörige gültige Lizenz kann der Benutzer zwar das Gerät oder den Datenträger erwerben, nicht jedoch auf den Inhalt zugreifen[578].

In Zukunft können Techniken des Trusted Computing (siehe *1.7.2.8 Trusted Computing*) verwendet werden, um die Einhaltung der Rechte zu gewährleisten[579].

Anwendung kann DRM im Bereich des Identity Managements (siehe *3.4.2 Access-Management und Technologien zur Autorisierung und Authentifizierung*) finden, da es granulierte Sicherheitsmechanismen mit sich bringt (z. B.: darf lesen, darf kopieren, darf ändern) [Hansen-2, 2006, S 14].

Aus rechtlicher Sicht gibt es zur Regelung in den USA den *Digital Millennium Copyright Act* (kurz: *DMCA*)[580]. Dieses Gesetz verbietet die Umgehung von DRM-Verfahren unter Androhung von Geldstrafen und/oder Freiheitsentzug.

Für Europa sind die Richtlinien *93/98/EWG*[581] vom 29. Oktober 1993 zur Harmonisierung der Schutzdauer des Urheberrechts und bestimmter verwandter Schutzrechte und *2001/29/EG*[582] des Europäischen Parlaments vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft relevant [Proksch, 2006, UrhRe, S 3].

In Österreich ist das *Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte* (kurz: UrhG) neben dem Datenschutzgesetz ausschlaggebend. Laut *§10 UrhG* ist der Urheber eines Werkes „der es geschaffen hat“ („Schöpferprinzip“). Das UrhG gilt ab Vollendung des Werkes, ein Copyrightvermerk ist für Österreich nicht nötig. Durch die EU-weite Harmonisierung gemäß RL 93/98/EG ist die Dauer des Urheberrechts einheitlich ab Tod des Urhebers auf 70 Jahre beschränkt, nachher erlischt jeder Rechtsanspruch [Proksch, 2006, UrhRe, S 5].

Die mit DRM-Techniken verbundene personenbezogene Datenverarbeitung kann als Vertragsbestandteil (Durchsetzung der Lizenzrechte) legitim sein, soweit sie sich auf die dafür erforderlichen Daten beschränkt, sich der Kunde der Verarbeitung als Teil des Vertrages bewusst ist und eine strikte Zweckbindung der verarbeiteten personenbezogenen Daten sichergestellt wird.

---

[577] Vgl. http://www.computer.org/portal/site/pervasive/ [26. Juni 2007]
[578] Vgl. http://www.digital-rights-management.de/ [27. Juni 2007]; http://netzpolitik.org/2006/digital-rights-management/ [27. Juni 2007]
[579] Vgl. http://www.ccc.de/digital-rights/?language=en [27. Juni 2007]
[580] http://www.copyright.gov/title17/ [27. Juni 2007]
[581] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 31993L0098 [26. Juni 2007]

Die Informationspolitik über die personenbezogene Datenverarbeitung zur Lizenzverwaltung ist sehr dürftig, es entsteht teilweise der Eindruck, dass Verarbeitungen zu diesem Zweck nicht bekannt werden sollen. Die Nutzung solcher Daten zu anderen Zwecken, beispielsweise zum Marketing und zur Kundenbindung, dürfte von besonderem Interesse für die Unternehmen sein. Sie stellt gleichzeitig ein beträchtliches Risiko für die informationelle Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung*) der Kunden dar. Der Umfang der für DRM-Techniken erhobenen und genutzten personenbezogenen Daten ist maßgeblich von der technischen Gestaltung der Systeme abhängig. Deren Hersteller berücksichtigen das datenschutzrechtlich geforderte Prinzip datensparsamer Technikgestaltung (siehe *2.4.2.2 Datensparsamkeit*) und die europarechtliche Vorgabe zur Implementierung technisch-organisatorischer Maßnahmen des Datenschutzes bereits im Designprozess von Technik (z. B.: durch die Einbindung von Anonymisierungs- und Pseudonymisierungskonzepten) (siehe *2.4.2.4 Integration von Datenschutzmechanismen in IT-Komponenten*) bisher jedoch nicht. Hier besteht erheblicher Nachholbedarf, wenn ein datenschutzgerechter Einsatz von DRM-Techniken in Zukunft möglich sein soll [ULD, 2005, S 7].

2.3.4 EXKURS: PRIVACYASPEKTE FÜR DEN BETRIEBLICHEN USER

Der technische Fortschritt ermöglicht es, jeden Schritt eines Mitarbeiters am PC zu überwachen. In der betrieblichen Praxis wird die private Nutzung von Internet und E-Mail unterschiedlich gehandhabt (siehe *1.7.3.2 Arbeitsrechtliche Grundlagen der Informationssicherheit in Unternehmen*). Während einige Unternehmen über keinerlei Regelungen verfügen, verhängen andere Verbote oder kontrollieren durch spezielle Software das Online-Verhalten der Beschäftigten. Als Mitarbeiter in einem restriktiv aufgebauten Unternehmensnetzwerk hat man in der Regel kaum Möglichkeiten, sich vor neugierigen Vorgesetzten zu schützen. Nur eine bewusste, verantwortungsvolle Nutzung von Technologie (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz*) und organisatorische Regelungen (z. B.: Betriebsvereinbarung) können der totalen Überwachung *einen Riegel vorschieben* oder sie zumindest erschweren [GPA, 2006, S 4].

Jede automationsunterstütze Verarbeitung personenbezogener Daten des Arbeitnehmers bedarf gemäß *§96 Abs 1 Z 3 Arbeitsverfassungsgesetz* grundsätzlich der Zustimmung des Betriebsrates (siehe *1.7.3.2.1 Mitwirkung des Betriebsrates*). Führt ein Unternehmen Aufzeichnungen über nicht-personenbezogene Daten (z. B.: Durchschnittskrankenstände), sind diese nicht zustimmungspflichtig. Wird allerdings eine Verknüpfung zu einem Arbeitnehmer hergestellt, kann diese Maßnahme zustimmungspflichtig werden, es sei denn, sie dient zur Erfüllung gesetzlicher Anforderungen an den Arbeitgeber (z. B.: Zahlung von Krankenentgelt, Meldung an die Sozialversicherung) (siehe *1.7.3.2.2 Personalinformationssysteme*). Möchte ein Arbeitgeber das „Surf-Verhalten“ und den E-Mail-Verkehr

[582] http://www.ris.bka.gv.at/celex/ Suche nach (Abgeleitetes Recht): 32001L0029 [26. Juni 2007]

seiner Mitarbeiter aufgrund gespeicherter Logfiles überprüfen, hat er wegen der damit nach dem Arbeitsverfassungsgesetz verbundenen Berührung der Menschenwürde eine Zustimmungspflicht, die entweder in Form einer Betriebs- oder einer Individualvereinbarung einzuholen ist. Bei Log-Files und E-Mails handelt es sich um potentiell sensible Daten, welche demgemäß nur bei Vorliegen eines Ausnahmetatbestandes laut *§9 DSG 2000 Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten*[583] protokolliert werden dürfen [Streitberger, 2003, S 33]. Werden die Log-Files auf Servern des Unternehmens gespeichert, so ist der Arbeitgeber Auftraggeber im Sinne des *DSG 2000* (siehe *1.7.3.1 Datenschutz*). Daten dürfen gemäß *§7 Abs 1 DSG 2000*[584] nur dann verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder den rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzt sind. Betroffener ist in diesem Fall der jeweilige Arbeitnehmer, dessen Daten protokolliert werden. Dem Mitarbeiter stehen daher das Auskunftsrecht lt. *§26 Abs 1 DSG 2000*[585], das Recht auf Richtigstellung oder Löschung *§27 Abs 1 DSG 2000*[586] und das Widerspruchsrecht *§28 Abs 1 DSG 2000*[587] zu [Streitberger, 2003, S 16f, S 31ff]. Fachliche Voraussetzungen gehören nicht zu den personenbezogenen Daten im Sinne des §96 Abs. Z 1 ArbVG und können demnach ohne Zustimmung des Betriebsrates erfasst werden. Der Arbeitgeber darf daher alle bisherigen beruflichen Tätigkeiten, Qualifikationen und Kenntnisse des Arbeitsnehmers registrieren, soweit eine Zweckmäßigkeit vorliegt.

Das Beratungsunternehmen *American Management Association* (kurz: *AMA*)[588] hat bereits 2001 erstaunliche Werte bezüglich Arbeitsplatzüberwachung (engl. *Workplace Monitoring and Surveillance*) in amerikanischen Unternehmen erhoben [AMA, 2001, S 1]:

Monitoring Internet connections	62,8 Prozent
Storage & review of e-mail messages	46,5 Prozent
Storage & review of computer files	36,1 Prozent
Video recording of employee job performance	15,2 Prozent
Recording & review of telephone conversations	11,9 Prozent
Storage & review of voice mail messages	7,8 Prozent
Total, active monitoring of communications & performance:	77,7 Prozent

Die Gründe, warum Unternehmen ihre Mitarbeiter bei deren Online-Aktivitäten überwachen, sind vielfältig. Zunächst muss sich ein Unternehmen vor Malicious Code und gegen Ausspionieren

583 http://www.ris.bka.gv.at/bundesrecht/ Suche nach: DSG §9 [9. Juli 2007]
584 http://www.ris.bka.gv.at/bundesrecht/ Suche nach: DSG §7 [9. Juli 2007]
585 http://www.ris.bka.gv.at/bundesrecht/ Suche nach: DSG §26 [9. Juli 2007]
586 http://www.ris.bka.gv.at/bundesrecht/ Suche nach: DSG §27 [9. Juli 2007]
587 http://www.ris.bka.gv.at/bundesrecht/ Suche nach: DSG §28 [9. Juli 2007]
588 http://www.amanet.org/ [29. Juni 2007]

schützen. Es ist im Interesse des Unternehmens, Betriebsgeheimnisse, interne Finanzdaten und geistiges Eigentum zu schützen. Wenn Mitarbeiter über das Firmennetzwerk (exzessiv) privat surfen, private E-Mails schreiben, Filme herunterladen oder illegal kopierte Musik tauschen, könnten personelle wie systemtechnische Ressourcen des Unternehmens vergeudet werden bzw. könnte es eventuell zu Urheberrechtsklagen an die Firma kommen. Manchmal geht es auch darum, über bestimmte Mitarbeiter Informationen zu sammeln, um sie zurechtzuweisen oder eine Entlassung argumentieren zu können[589]. Im Wesentlichen erwarten sich Unternehmen durch die Mitarbeiterüberwachung eine gesteigerte Effizienz [GPA, 2006, S 8].

Um eine Strukturierung zu bekommen, welche Daten über einen Arbeitnehmer anfallen respektive gesammelt werden können, wird eine Unterscheidung im Sinne von *§93 TKG 2003* in Stammdaten, Verkehrsdaten und Inhaltsdaten vorgenommen.

1. Stammdaten sind personenbezogene Daten eines Arbeitnehmers, die von seinem Arbeitgeber im Rahmen des Arbeitsverhältnisses gespeichert und verwendet werden. Dazu gehören zunächst alle Informationen, die der Arbeitgeber zur Erfüllung seiner gesetzlichen und arbeitsvertraglichen Pflichten benötigt, also beispielsweise Name und Adresse des Arbeitnehmers, Höhe des Gehalts und Steuerklasse. Darüber hinaus werden im Regelfall auch weitergehende Informationen gespeichert, die für das Arbeitsverhältnis von Bedeutung sein können, beispielsweise Angaben über die Ausbildung und Qualifikation des Arbeitnehmers oder seinen beruflichen Werdegang. Die Daten ergeben sich direkt aus den Angaben des Arbeitnehmers respektive aus indirekten Informationen an den Arbeitsgeber (z. B.: Kreditkartennummer durch Reiseabrechnung), von Behörden (z. B.: Gehaltspfändungen vom Finanzamt, Mündelgeldzahlungen von Jugendamt, Amtsstundenfreistellung für Bürgermeister von Stadt/Gemeinde) und Institutionen/Organisationen (z. B.: Freistellung bei Einsatzfall von der Feuerwehr, freier Tag bei Feiertagen der (evangelischen) Kirche, Inanspruchnahme von durch Dienstreisen erlangten Bonusmeilen für private Ferienreisen) sowie aus Sozialleistungen des Unternehmens (z. B.: Krankheitsdaten[590] durch Zusatzkrankenversicherung, betrieblicher Gesundenuntersuchung und Betriebsarzt, Autokennzeichen durch Parkplatz):

   Name, Adresse(n), Titel, Sozialversicherungsnummer, Steuernummer, Geschlecht, Religionsbekenntnis, Krankheit(en), Geburtsdatum, Geburtsort, Bankverbindung(en), bisherige(s) Arbeitsverhältnis(se), weitere(s) Dienstverhältnis(se), Beteiligungen bei Unternehmen, Ausbildung, Qualifikation, Lebenslauf, Zeugnisdaten, Familienverhältnisse (Partner, Kinder,

[589] Vgl. http://oe1.orf.at/highlights/55675.html [29. Juni 2007]; http://www.stern.de/wirtschaft/arbeit-karriere/:%DCberwachung-Big-Brother-Arbeitsplatz/541928.html?eid=541941 [30. Juni 2007]

[590] Bei Krankheitsdaten wird sehr restriktiv vorgegangen, aber zumindest die Art der Krankheit wird an den Arbeitgeber – mit dem Einverständnis des Mitarbeiters – kommuniziert. Der Arbeitnehmer ist in der Regel selbst daran interessiert, damit zum einen im Notfall richtig geholfen werden kann, zum anderen längere Krankenstandszeiten begründet werden können.

Eltern, Familienstand etc.), Notfalldaten, private Telefonnummer(n), private E-Mail-Adresse(n), Strafregisterauszug, Reisepassnummer, Führerscheinnummer und -klassen, privates Autokennzeichen, Pfändung(en), Gewerkschaftsmitgliedschaft, Mitgliedschaft bei Feuerwehr bzw. Rettung, Hobbies etc.

Personalnummer, Abteilung, Stellenbeschreibung, Kostenstelle, Firmenkarten-, Gleitzeitkartennummer, Vorgesetzter (direkt, indirekt), Mentor, Dienstvertrag, Jobhistory, Gehaltsentwicklung (Vorrückungen, Prämien, Aktienoptionen), Ranking, Daten (objektive und subjektive Wünsche und Ziele) Mitarbeitergespräch, Dienstverfehlungen, Schulungshistory (intern, extern), Standort (Gebäude, Zimmernummer), Telefonnummer(n), Dienstauto, zur Verfügung gestellte Hardware (Mobiltelefon, PDA, PC, Drucker etc.)

2. Verkehrs- und Inhaltsdaten: An- und Abwesenheitszeiten, Krankenstandsdaten, Reisezeiten, Onlinezeiten im Büro, Zugriffe von außerhalb des Büros, besuchte Webseiten, Einträge in Intranetforen, bekommene/verfasste E-Mails, gelesene/erstellte Dateien, empfangene/getätigte Telefongespräche etc.

In der Personaldatenverwaltung ersetzen elektronische Verfahren zunehmend manuelle Abläufe (z. B.: Personalakt). Die Daten werden mithilfe mächtiger Personalinformationssysteme (engl. *Human Ressource Systems*) (z. B. *SAP ERP HCM*[591]) gepflegt. Diese digitale Personaldatenverarbeitung ermöglicht dem Arbeitgeber weitreichende Auswertungs- und Kontrollmöglichkeiten. Mitarbeitern aus der Administration (Personal, Lohnverrechnung, IT) sowie Vorgesetzten steht damit – zumindest theoretisch – eine einheitliche Quelle über die Daten jedes einzelnen Arbeitnehmers zur Verfügung. Obwohl sich die Zugriffsrechte in solchen Systemen beschränken lassen, stehen dem Verwaltungsmitarbeiter bzw. dem Vorgesetzten teilweise weit mehr Daten zur Verfügung als er zur Ausführung seiner Tätigkeit benötigt.

Im nächsten Kapitel (siehe *3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*) werden Ansätze erarbeitet, wie zum einen dem Mitarbeiter mehr Einfluss auf die Bereitstellung seiner Daten gegeben werden kann, zum anderen, wie den Verwaltungsmitarbeitern und Vorgesetzten nur jene Daten zur Verfügung stehen, die tatsächlich zur Erledigung ihrer Arbeit notwendig sind.

Status quo ist, dass die Geschäftsführung bzw. der Vorgesetzte Einsicht in Stammdaten nehmen kann[592]. Dazu kommen alle Angelegenheiten, bei denen Genehmigungen erforderlich sind, wie beispielsweise Bestellungen für den internen Bedarf, Urlaubsanträge oder Reiseabrechungen. Da der Vorgesetzte nicht nur fachlich (Projekte, Verkaufszahlen der Mitarbeiter) zur Kontrolle verpflichtet

[591] http://www.sap.com/germany/solutions/business-suite/erp/hcm/index.epx [30. Jun i 2007]
[592] Vgl. http://www.dialogdata.com/software/personal/mibs/personalinformation/service/chefinformation.html [30. Juni 2007]

ist, sondern auch kostenseitig, werden ihm periodisch die Bewegungen auf der Kostenstelle (engl. *cost location*) des Mitarbeiters zur Kenntnis gebracht.
Mitarbeitern in der Personalabteilung stehen im Wesentlichen alle Stammdaten zur Verfügung.
Die IT-Abteilung hat theoretisch Zugriff auf alle elektronisch gespeicherten Inhalte (Dokumente, Kalendereinträge, E-Mails, Bürgerdaten etc.), solange diese nicht verschlüsselt oder explizit geschützt sind. Zudem kann nachvollzogen werden, von welchem PC aus wann welche Webseiten aufgerufen wurden bzw. wann und an wen der Mitarbeiter E-Mails geschickt hat. Bekommt der Administrator von seinem Vorgesetzten den Auftrag, diese Verkehrsdaten personenbezogen auszuwerten, würde das vom betroffenen Benutzer nicht bemerkt werden. Neben der Auswertung existierender Daten gibt es technische Möglichkeiten, die Mitarbeiter online zu überwachen[593] (siehe *2.3.3.2 Gefährdungen durch Internet und E-Mail*).

2.4 MAßNAHMEN ZUM SCHUTZ DER PRIVACY

Die drei wesentlichen Säulen, auf denen das Grundrecht auf Privatsphäre ruht, sind durch den Staat vorgegebene gesetzliche Vorschriften (siehe *1.7.3.1 Datenschutz*), Bewusstseinsbildung/freiwillige Selbstbeschränkungen und technische Vorkehrungen zur Datensparsamkeit bzw. gegen missbräuchliche Datensammlung (siehe *2.2.5 Data Mining*) bei Anbietern und Benutzern von Informationstechnologien. Jede dieser drei Säulen ist essentiell, keine für sich allein ausreichend, um das Grundrecht auf Privatsphäre absichern zu können. Was für verantwortungsvolle, der Risiken bewusste Konsumenten gilt, ist für sorglose Benutzer umso wichtiger. Es kann niemand gezwungen werden, aus seinem Privatleben ein Geheimnis zu machen, ebenso wenig darf Unkenntnis oder Sorglosigkeit mit einem Verlust von Grundrechten verbunden sein. Unwissenheit schützt nicht vor Strafe, darf aber auch nicht dazu führen, dass Rechtsverletzungen ungehindert und ungestraft möglich werden [Cas, Peissl, 2002, S 6].
Da die Wege von Daten intransparent sind, ist die beste Strategie sicher jene der Datenvermeidung (siehe *2.4.2.2 Datensparsamkeit*). Dazu ist es notwendig, die Benutzer zu informieren, sie in die Lage zu versetzen, die Mechanismen zu erkennen, um dann bewusst die Nutzungsentscheidung treffen zu können. Oft wird dies allerdings eine Entscheidung zwischen Preisgabe der Privatsphäre und höherer Bequemlichkeit sein. Verschlüsselung (siehe *1.7.2.1 Kryptologie*), Pseudo-/Anonymität (siehe *2.2.2 Pseudonymität, 2.2.3 Anonymität*) und Technologienutzung (siehe *2.4.3 Säule 3: Datenschutz durch Technik*) sind mögliche Wege zur Aufrechterhaltung/Wiederherstellung von Privatsphäre. Absolut notwendig ist es, die informationelle Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung*) im Bewusstsein der Benutzer zu verankern. Dazu gehören Ausbildung, Verankerung von Grundbegriffen der Informationssicherheit als Basiswissen aller Benutzer,

[593] http://www.spionagecheck.de/ [1. August 2007]

Aufklärung, Information, breite Diskussion (siehe *1.8.2.5.2 Sensibilisierung und Schulung*) – nicht nur im Kreis der Wissenden [Cas, Peissl, 2000, S 29].

In diesem Zusammenhang findet in der Literatur[594] der Begriff *Systemdatenschutz* Erwähnung. Dieser umfasst all diejenigen technischen und organisatorischen Vorkehrungen, die für den Schutz des Rechts auf informationelle Selbstbestimmung förderlich und rechtlich geboten sind. Er beschränkt sich nicht auf einen Datenschutz durch Technik, sondern schließt auch organisatorische Regelungen ein und geht durch neue Ansätze wie Datensparsamkeit, Anonymisierung oder Pseudonymisierung und Datenschutz-Gütesiegel über die klassischen technischen und organisatorischen Maßnahmen hinaus.

Die *Deutsche Gesellschaft für Informatik* formulierte in einem Memorandum an Politik und Unternehmen Forderungen [GI, 2007, S 1] zur Identifizierung und Überwachung von Bürgern (verkürzt):

1. Information und Sensibilisierung der breiten Öffentlichkeit zu den technischen Überwachungsmöglichkeiten von Kommunikation und Nutzerverhalten verbunden mit Hinweisen, unter welchen Voraussetzungen Bürger sich der Überwachung entziehen können.
2. Für jedermann leicht erkennbare Kennzeichnung der Überwachung im öffentlichen und privaten Raum.
3. Weitgehende Vermeidung der Speicherung und Verarbeitung personenbezogener Daten, mindestens aber Beschränkung auf konkrete, eng eingegrenzte Zwecke. Dadurch lässt sich ein Missbrauch datenschutzrelevanter Informationen wirkungsvoll verhindern.
4. Erstellung eines öffentlichen, entgeltfrei einsehbaren (Internet-) Registers aller zur Überwachung nutzbaren (unternehmenseigenen und behördlichen) Datensammlungen mit den Datenfeldern und einer Beschreibung der Inhalte sowie den vorgesehenen und möglichen Verwendungen durch die zuständigen Unternehmensleitungen, damit sich Betroffene an sie wenden können.
5. Abwägung des spezifischen Nutzens jedes einzelnen Überwachungsverfahrens sowohl mit den Beschränkungen der Persönlichkeitsrechte der Betroffenen als auch mit den entstehenden Kosten. Dies gilt für die Datensammlung und Zusammenführung bis hin zur Auswertung.
6. Analyse, inwieweit die Rechte der Datenschutzbehörden zur effizienten Verhinderung von Missbräuchen verstärkt werden sollten.
7. Einbau wirksamer und einfach nutzbarer Sicherheitsmechanismen gegen Identifizierung und Überwachung in alle zur Kommunikation nutzbaren Geräte; das Sicherheitsniveau ist von unabhängigen Stellen zu bewerten und diese Bewertung zu veröffentlichen.

[594] Vgl. https://www.datenschutzzentrum.de/systemdatenschutz/index.htm [1. Juli 2007]

2.4.1 SÄULE 1: GESETZLICHE RAHMENBEDINGUNGEN

An dieser Stelle ist auf die diversen Ausführungen in vorigen Kapiteln und Abschnitten zu verweisen, wo die Grundlagen bzw. speziellen Ergänzungen zum Thema Datenschutz behandelt wurden: *1.7.3 Gesetzeslage, 1.7.3.1 Datenschutz, 1.7.3.2.4 Umgang mit personenbezogenen Daten, 1.9.1.1.2 Datenschutz bei Google, 2.2.5 Data Mining, 2.3.2.1 Informationelle Selbstbestimmung, 2.3.2 Rechtliche Belange, 2.3.3.2.1 IP-Adresse/Internet Service Provider und 2.3.3.1.2 Vorratsdatenspeicherung*.

Die bestehenden regulativen Rahmenbedingungen sind den Bestrebungen von Ermittlungsbehörden ausgesetzt, die sich durch den erleichterten Zugang zu Telekommunikationsdaten bessere Aufklärungs- und Präventionsmöglichkeiten erhoffen. Diese Bestrebungen haben durch die Terroranschläge vom 11. September 2001 wesentlich an Gewicht und politischer Durchsetzbarkeit gewonnen und sind in eine Reihe von internationalen und nationalen Gesetzesnovellierungen gemündet, die erweiterte Überwachungsbefugnisse und die Speicherung von Verkehrs- und Inhaltsdaten beinhalten.

Die größten Defizite bestehen bei der Transformation des durch die EU-Richtlinien angestrebten Schutzniveaus und dessen Durchsetzung durch nationale Gesetze. Maßnahmen, die diese Diskrepanz verringern sollen, betreffen gesetzliche Änderungen zur Stärkung und Erweiterung der Kompetenzen der Datenschutzbehörden (z. B.: Datenschutzkommission – siehe *1.7.3.1 Datenschutz*), zur Erleichterung des Zugangs zum Recht für die Konsumenten (z. B. Recht auf Beauskunftung, auf Richtigstellung und Löschung seiner Daten – siehe *1.7.3.1 Datenschutz, 2.3.4 Exkurs: Privacyaspekte für den betrieblichen User*) sowie die Rücknahme oder Verhinderung von Reformen, die das Grundrecht beeinträchtigt haben bzw. schmälern würden (z. B.: Vorratsdatenspeicherung – siehe *2.3.3.1.2 Vorratsdatenspeicherung*) [Cas, Peissl, 2002, S 6].

2.4.2 SÄULE 2: BEWUSSTSEINSSCHAFFUNG UND SELBSTBESCHRÄNKUNG

Klassische Formen der Aufklärung und Bewusstseinsschaffung sind eine Einbindung der Datenschutzproblematik in allen Formen des Unterrichts, zielgruppenspezifisches Informationsmaterial mit Broschüren und multimedialen Datenträgern sowie die Bereitstellung eines thematisch konzentrierten Webportals (Anm.: bei der im Jahr 2007 gelaunchten E-Government-Seite *Digitales Österreich*[595] des Bundeskanzleramts verkommt der Datenschutz zum Randthema).

Im Bereich der Selbstregulierung zielen die Vorschläge darauf ab, vorhandene Ansätze wie das E-Commerce[596]- bzw. E-Government[597]-Gütesiegel oder maschinenlesbare Datenschutzpolitiken gemäß

[595] http://www.digitales.oesterreich.gv.at/ [1. Juli 2007]
[596] http://guetezeichen.at/ [1. Juli 2007]
[597] http://www.cio.gv.at/e-Gov-Guetesiegel/ [1. Juli 2007]

Platform for Privacy Preferences (kurz: *P3P*)[598] zu forcieren [Cas, Peissl, 2002, S 7]. Dazu kommen Aspekte und Prinzipien wie Datensparsamkeit, Selbstdatenschutz und Integration von Datenschutzmechanismen in IT-Komponenten.

2.4.2.1 Platform for Privacy Preferences

P3P soll dem Benutzer im Internet helfen, mittels standardisierter Technik einen Überblick zu erhalten, was mit seinen Daten geschieht, die beim Besuch einer Website anfallen. Durch die Standardisierung ist es möglich, auch Datenschutzerklärungen von fremdsprachigen Internetseiten zu interpretieren. Gewährleistet wird die Durchsetzung der Benutzerrechte nur vom Rechtssystem eines Staates und nicht durch die bloße Existenz einer P3P-Datenschutzerklärung [Rickert, 2004, S 31].

Technisch wird das durch die Verwendung eines sogenannten P3P-Agenten gelöst, welcher kostenlos im Internet erhältlich ist. In vielen Webbrowsern ist dieser Agent bereits integriert (z. B.: Microsoft Internet Explorer ab Version 6.0).

Am Beispiel des Internet Explorers 7.0 (kurz: IE) soll P3P veranschaulicht werden:

Zunächst ist folgende Information zum Thema Datenschutzbericht in der Hilfe des Browsers zu finden: „*Die Datenschutzrichtlinie einer Website informiert Sie, welche Art von Informationen die Website sammelt, an wen sie diese Informationen weitergibt und wie diese Informationen verwendet werden.*

Viele Websites stellen Datenschutzerklärungen als schriftliche Dokumente bereit, die Sie im Internet anzeigen können. Websites enthalten ggf. auch eine P3P-Datenschutzrichtlinie (Platform for Privacy Preferences). Wenn eine Website über eine P3P-Datenschutzrichtlinie verfügt, kann der Internet Explorer diese anzeigen. Internet Explorer kann in einigen Fällen auch Ihre Datenschutzeinstellungen mit einer Darstellung der P3P-Datenschutzrichtlinie vergleichen, um zu bestimmen, ob die Website Informationen auf Ihrem Computer speichern darf (in Form von kleinen Dateien, die als Cookies bezeichnet werden).“ (siehe *2.3.3.2.3 Cookie*).

Die P3P-Datenschutzrichtlinie (engl. *Privacy Policy*) einer Website wird angezeigt, indem im IE auf die Schaltfläche „Seite“ und dann auf „Datenschutzrichtlinie der Webseite“ geklickt wird:

[598] http://www.w3.org/P3P/ [1. Juli 2007]

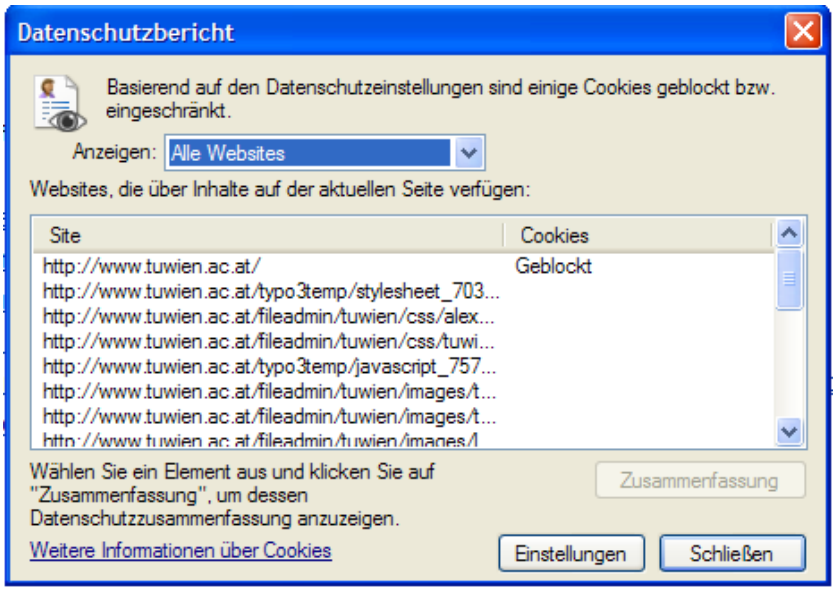


Abbildung 39: Anzeige P3P-Datenschutzrichtlinie im Internet Explorer

2.4.2.2 Datensparsamkeit

Der beste Datenschutz besteht darin, dass keine oder möglichst wenig personenbezogene Daten anfallen. Datenvermeidung und Datensparsamkeit sind Grundprinzipien eines zeitgemäßen Datenschutzes. Verfahren müssen demnach so ausgestaltet werden, dass nur so viele personenbezogene Daten gesammelt werden, wie für die jeweilige Anwendung unbedingt notwendig sind. Gerade das unnötige Sammeln von sensitiven Daten durch öffentliche und nicht-öffentliche Stellen widerspricht dem Grundrecht auf informationelle Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung*). Dieser Grundsatz muss bereits bei der Gestaltung der Technik und ihrer Einsatzbedingungen berücksichtigt werden (siehe *2.4.2.4 Integration von Datenschutzmechanismen in IT*). Dies gilt vor allem für Verkehrsdaten (siehe *2.3.2.3 Definition von Daten nach dem TKG 2003 bzw. Kommunikationsgeheimnis und* Datenschutz), die beim Betrieb von IT-Systemen anfallen und denen beim Übergang zum Ubiquitous Computing (siehe *1.5.2 Ubiquitäres Computing* und *2.3.3.4 Pervasive Computing/Internet der Dinge*) zunehmende Bedeutung zukommt. Bei elektronischen Diensten können anonyme Nutzungsmöglichkeiten (siehe *2.2.3 Anonymität, 2.4.4 Anonym Surfen*) einen wichtigen Beitrag leisten. Soweit eine Individualisierung von Dienstleistungen, Statistiken und wissenschaftlichen Forschungsvorhaben erforderlich ist, sollten – wo möglich – Pseudonyme (siehe *2.2.2 Pseudonymität, 2.4.6 Pseudonym Surfen und Mailen*) verwendet werden [BSI-2, 2006, S 2].

Das Datensparsamkeitsprinzip umfasst neben der Einschränkung auf die erforderlichen Daten die Gewährleistung ihrer Zweckbindung (siehe *2.3.2 Rechtliche Belange*). Viele dieser Anforderungen lassen sich durch technischen Datenschutz realisieren oder zumindest weitgehend unterstützen.

2.4.2.3 Selbstdatenschutz

Unter Selbstdatenschutz wird verstanden, dass die Benutzer die Gefahren hinsichtlich Datenschutz und Datensicherheit kennenlernen und selbst aktiv Gegenmaßnahmen ergreifen. Problematisch an der Internettechnologie ist der inzwischen hohe Komplexitätsgrad. Die meisten User kennen die damit verbundenen Gefahren nicht, persönliche Daten herauszugeben, zumal sie der fälschlichen Annahme sind, das Internet wäre anonym.

In der Informationsgesellschaft bedarf es daher entsprechender Aufklärung, die den Benutzern bewusst macht, sich beim Surfen und vor allem bei finanziellen Transaktionen im Internet zu schützen. Nur unter den Bedingungen, dass das Wissen der Benutzer und die Lösungen der Komplexität der Technik gerecht werden, können die Risiken wirksam minimiert werden.

Neben einigen Verhaltensregeln reicht die Palette der zu beachtenden technischen Faktoren von informationssicherheitstechnischen Maßnahmen (Virenschutz, Firewall – siehe *1.3.4 Computer Anomalien/Malicious Code, 1.7.2.4.1Firewall, 1.7.2.6 Neue und alternative Ansätze des Schutzes vor Malicious Code*) über das Absichern des PCs mit Zugangsschutz (Passwort – siehe *1.7.2.5 Graphisches Passwort*) bis hin zur Verschlüsselung (siehe *1.7.2.1 Kryptologie*)[599].

Cas und Peissl [Cas, Peissl, 2000, S 32] erarbeiteten folgende Empfehlungen und Vermeidungsstrategien für die Internetnutzung:

- mehrere Provider nutzen,
- Zurückhaltung bei Preisgabe von Daten,
- andere Identitäten und anonyme E-Mail-Adressen verwenden; insbesondere bei Chats und Newsgroup-Beiträgen gegebenenfalls eigene Beiträge aus Newsgroup-Archiv entfernen und Archivierung blockieren,
- Verschlüsselungssoftware nutzen,
- Anonyme Mail- und Webdienste nutzen,
- spezialisierte Softwarepakete zum Schutz der Privatsphäre und des eigenen Rechners einsetzen.

2.4.2.3.1 Privacyschutz für die Suche mit Webbrowsern

Eine unterschätzte Gefahr hinsichtlich Privacy bilden Suchmaschinen. Diese speichern die Suchbegriffe, die aufgrund der Ergebnisse besuchten Seiten, Zeitprotokolle und die IP-Adresse. Das ermöglicht, die Identität, die Vorlieben, die Onlinezeiten eines Users herauszufinden. Einige Möglichkeiten, dagegen aktiv zu werden[600]:

- *Don't log into search engines or their tools: If you log into a search engine, you make it easy for that search engine to build a comprehensive profile about you, because they know your identity as*

[599] Vgl. https://www.datenschutzzentrum.de/selbstdatenschutz/index.htm [1. Juli 2007]
[600] Vgl. http://www.cio.com/article/121315/Seven_Tips_to_Keep_Your_Search_History_Private [1. Juli 2007]

you search. Long gone are the days when a search engine was only a search engine. Today, they're entire ecosystems of sites and services. Google, for example, offers dozens of services, including Gmail, online office software, blogging services and more. For privacy's sake, never do searches when you're logged into any of a search engine's services, such as its mail service. Another option is to use one browser such as Firefox for a service like Gmail, and another such as Internet Explorer for doing Google searches. That way, it will be much harder for the search engine to correlate your identity with your searches. For maximum safety, use an anonymizing service for the browser that you use to search with.

- *Keep yourself safe from Google* (siehe *1.9 Exkurs: Google*)*: If you're like most people, you do all or most of your searching from one search engine – Google. This means you're particularly vulnerable, because Google will have a record of all your searches. Even if you don't log into Google, it can track your searches because it uses cookies to track you from session to session. You could, of course, delete all your cookies before you visit Google. But that's problematic, because cookies can be quite useful. A simpler solution is to block only Google from placing cookies on your PC. The more Google services like this that you sign up for, the more information Google knows about you. This makes it that much easier for the search giant to create a profile about you. So either don't sign up for those services or else create separate Google accounts for each of them, so that the search engine can't correlate all your interests. When you use Search History, Google stores a record of all your searches on its servers. If you're worried that that search history may fall into the wrong hands, or be subpoenaed by the government, simply don't use the service.*
- *Regularly change your IP-address: Search engines can correlate all your searches by tracking the IP address you're using and then using that to link together all the searches you perform on their sites. There's a simple way to get around this; regularly change your IP-address.*
- *Use alternative browser (i.e. ixquick*[601] *or browzar*[602]*): Use a search engine that doesn't retain a history of your searches* (Anm.: Beim nur 200 KB-grossen Gratisprodukt Browzar werden die besuchten Seiten, Formulardaten und Cookies nicht im Cache gespeichert und die sonst obligatorischen History-Verläufe fallen weg. Ein Informationsfenster zeigt beim Schließen des Browsers zudem die Erledigung der Löschprozesse übersichtlich an.). *It says it deletes all information about your searches within 48 hours, so the information simply isn't around for anyone to use. If the government subpoenas the data, there's nothing for them to get.*
- *Don't include personal information in your searches: We've all "Googled" ourselves at times, just to see what's out there on the Web about us. But every time you use personal information in a search, such as your name, address and so on, you make it easy for a search engine to know who*

[601] http://us.ixquick.com/deu/ [1. Juli 2007]

you are and then correlate searches with your name. Worse, it can lead to identity theft if you search for information such as your Social Security number and someone gets hold of your search records. So try to avoid including personal information about yourself in your searches.

- *Do sensitive searches from a public hot spot: If you absolutely must do a search about personal information or do a search that is sensitive for some other reason, don't do it at home or at work.*
- *Avoid using your Internet service provider's search engine: Your service provider knows your IP-address, which means that it can track all the Web sites you visit. That's bad enough for your privacy, but if you also use its search engine, it will be able to correlate your IP address to your searches and build an even more comprehensive profile about you. That profile may be available to anyone with a subpoena*.

2.4.2.3.2 Löschen von Userdaten

Immer mehr Menschen verfassen im Internet Weblogs, diskutieren in Foren oder haben Profilseiten in Social Networks. Dabei wird unterschätzt, wie viele persönliche Informationen preisgegeben werden. Im Juli 2007 wurden einem leitenden Angestellten eines US-amerikanischen Unternehmens acht Jahre alte Postings bei Yahoo zum Verhängnis, er verlor durch die anonyme (Anm.: Anonymität wurde aufgedeckt) Bekanntgabe von Finanzdaten seinen Job[603]. Vor allem junge Leute unterschätzen vielfach die Öffentlichkeit des Internets und prahlen etwa auf MySpace-Seiten mit ausgelassenen Urlaubsfotos. Das kann einem beispielsweise bei Bewerbungen zum Nachteil gereichen. Laut einer Umfrage (Herbst 2006) des *Bundesverbandes Deutscher Unternehmensberater*[604] recherchieren bereits 28 Prozent der deutschen Personalchefs im Internet nach Informationen über Jobanwärter.

Welche Einträge jemand in Diskussionsforen, Newsgroups etc. hinterlassen hat, kann mittels Tools wie *Google Group Search*[605] durch die Eingabe eines Namens im Feld „Autor“ überprüft werden. Im Allgemeinen ist es für den Einzelnen schwierig, eingetragene Daten und registrierte Accounts zu löschen. Der User hat lediglich die Möglichkeit, sich an den Webseitenbetreiber mit dem Ansuchen zu wenden, seine Daten zu beseitigen, ohne jedoch die Gewissheit zu haben, dass das entsprechend bzw. sauber erledigt wird. Google beispielsweise regelt das Entfernen von Inhalten durch folgende Vorgehensweisen: *http://www.google.ch/intl/de/remove.html* [*1*. Juli 2007]. Im Konkreten werden folgende Entfernungsoptionen angeboten:

- ändern der URL einer Website,
- entfernen einer Website,

---

[602] http://www.browzar.com/ [1. Juli 2007]

[603] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9026999&source=NLT_PM&nlid=8 [26. Juli 2007]

[604] http://www.bdu.de/ [1. Juli 2007]

[605] http://groups.google.de/advanced_group_search [1. Juli 2007]

- entfernen individueller Seiten,
- entfernen von Snippets,
- entfernen von Seiten aus dem Cache,
- entfernen eines veralteten oder inaktiven Links,
- entfernen eines Bildes aus Googles Bildsuche.

Professionelle Hilfe im Löschen von Benutzerdaten bietet das amerikanische Unternehmen *ReputationDefender*[606]. Dieses überwacht den *Ruf* des Benutzers und bereinigt die unerwünschten Daten (kompromittierende Fotos, Einträge in Foren etc.) gegen Bezahlung.

2.4.2.3.3 DRM bei E-Mails

Der amerikanische E-Mail-Dienst *BigString*[607] bietet die Möglichkeit, Kontrolle über die selbst versendeten Daten zu behalten. Dies wird durch einen E-Mail-*Selbstzerstörungsmechanismus* sichergestellt, den der Absender nach Belieben konfigurieren kann. Damit wird beispielsweise eine Nachricht automatisch gelöscht, nachdem sie der Empfänger gelesen hat. Die Selbstzerstörungsfunktion ermöglicht dem Absender, die Kontrolle über sein geistiges Eigentum zu behalten. Der Boom des Social Networking ermöglicht, dass Bilder ins Web gelangen, die den abgebildeten Personen nicht zum Vorteil gereichen. Der User kann mit dem Dienst unterbinden, dass private Videos weitergeleitet oder ins Web gestellt werden und ihn auf diesem Weg im ungünstigsten Fall bloßstellen könnten. Unternehmen oder Künstler aus der Unterhaltungsbranche können Videos verschicken, die nur einmal angesehen werden dürfen. BigString bietet somit ein DRM für E-Mail-Attachements. Der Versender legt fest, wie oft der Mailanhang angesehen werden darf, oder ob der Empfänger es weiterleiten kann. Zudem kann darüber bestimmt werden, ob eine Datei auf die Festplatte des Empfängers gespeichert oder gedruckt werden darf.
(Anm.: Der Autor hat diesen Dienst im Juli 2007 getestet und dabei festgestellt, dass alle Features bei einfacher Bedienbarkeit vorhanden sind, aber – noch – nicht in vollem Umfang funktionieren.)

2.4.2.4 Integration von Datenschutzmechanismen in IT-Komponenten

Datenschutz soll nicht allein durch gesetzliche Regelungen normiert, sondern auch durch das Design der IT-Komponenten realisiert werden [Cas, Peissl, 2002].
Das *World Wide Web Consortium* (kurz: *W3C*) spielt dabei eine wesentliche Rolle. Es versucht, einheitliche Technologien (Spezifikationen, Richtlinien, Software und Tools) zu entwickeln, die den Fortschritt des Webs fördern und seine Interoperabilität sicherstellen. Die Zukunft des Webs sieht das W3C „*für jedermann (unabhängig von Kultur, Fähigkeiten etc.), auf allem (auf Endgeräten vom*

[606] http://www.reputationdefender.com/ [1. Juli 2007]

leistungsfähigen Computer mit hochauflösenden Bildschirm bis hin zu mobilen Endgeräten), von überall (mit Bandbreiten von niedrig bis hoch) in diversen Interaktionsmodi (Berührung, Stift, Mouse, Stimme, Hilfstechnologien, Computer mit Computer).“[608]

Das W3C hat die Wichtigkeit der Entwicklung von Technologien erkannt, die Vertrauen und Sicherheit fördern und dadurch zunehmend komplexere Interaktionen zwischen Beteiligten rund um den Globus ermöglichen. Basierend auf der Erfahrung mit P3P fährt W3C fort, Überlegungen anzustellen, wie Sicherheitsmechanismen in Dienste implementiert werden können. Deshalb erforscht W3C, wie private Metadaten[609] genutzt werden können, damit Userdaten auf vertrauenswürdige Art auf Serverseite verwaltet werden können. *Semantic Web*[610]-Technologien ermöglichen es der Software, relevante Informationen zu finden und zu analysieren. Die traditionelle Public-Key-Infrastruktur (siehe *1.7.2.1.5 Public Key Infrastructure*) muss erweitert werden, um die Vielfalt der verschiedenen Lebensformen im Web widerzuspiegeln[611].

Nach anhaltender Kritik präsentierte Microsoft im Oktober 2006 ein Dokument namens „*Microsofts Privacy Guidelines for Developing Software Products and Services*“[612]. Darin wird für das Softwaredesign bzw. die Entwicklung festgehalten, wie die Privatsphäre der Kunden besser geschützt werden kann: „*The document outlines recommendations for software developers that will help them protect customer privacy when building applications that deal with sensitive information, such as Web sites or Web-based features that send personal information over the Internet. [...] For example, Microsoft implemented a way to erase personal information in the new phishing filter it has built for its Internet Explorer browser. The filter, designed to protect users when they surf to online sites that could use phishing to steal personal information, compares sites that users visit to known phishing sites. However, before going to any site to do this verification, the filter erases any personal information that would identify which user visited.*“

---

[607] http://www.bigstring.com/ [3. Juli 2007]

[608] Vgl. http://www.w3c.de/about/future.html [1. Juli 2007]

[609] Die Enterprise Privacy Authorization Language (kurz: EPAL) ist eine formalisierte Sprache, um den Schutz personenbezogener Daten innerhalb eines Unternehmens und unternehmensübergreifend darstellen und durchsetzen zu können. Vereinfacht dargestellt werden dabei jedem von dem Unternehmen gesammelten personenbezogenen Datum Informationen beigefügt, anhand derer entschieden werden kann, wie die Daten benutzt werden dürfen. EPAL-Datenschutzinformationen dienen ausschließlich der Festlegung, wer personenbezogene Datenkategorien zu welchem Zweck wie verarbeiten darf und zwar unabhängig davon, welche Datenmodelle eine Software verwendet oder welche Zugriffsrechte dem Nutzer eines EDV-Systems allgemein zustehen. http://www.w3.org/Submission/2003/07/ [1. Juli 2007]

[610] Das Semantic Web bietet ein Rahmenwerk, das es erlaubt, Daten über Applikations-, Unternehmens- und Community-Grenzen hinweg zu teilen und wiederzuverwenden. Das Semantic Web ist eine Erweiterung des gegenwärtigen Webs, in der Information eine definierte Bedeutung zugewiesen wird, was Mensch und Computer erlaubt, besser zu kooperieren. Informationen sollen zusätzlich zu der für Menschen lesbaren Form auch formal, in einer für Maschinen verarbeitbaren Form repräsentiert werden, damit Programme darauf operieren können, so dass Anfragen aufgrund ihres Bedeutungsinhalts anstelle ihrer Schreibweise bearbeitet werden können.

[611] Vgl. http://www.w3c.de/about/future.html [1. Juli 2007]

[612] http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en [1. Juli 2007]

2.4.3 SÄULE 3: DATENSCHUTZ DURCH TECHNIK

Ein bewusster Umgang mit dem Medium Internet trägt massiv dazu bei, die eigene Privatsphäre zu schützen und dem Missbrauch persönlicher Daten vorzubeugen. Diese Strategie stößt oft auf Grenzen, weil etwa keine oder ungenügende Informationen über das virtuelle Gegenüber und dessen Umgang mit persönlichen Daten vorhanden sind, weil bestimmte Dienste nur unter Bekanntgabe personenbezogener Daten in Anspruch genommen werden können oder weil Datenspuren ohne Kenntnis und Einverständnis der Benutzer gesammelt und ausgewertet werden. Es liegt daher nahe, diese Probleme durch technische Maßnahmen zu entschärfen oder zu beseitigen, die unter *Privacy Enhancing Technologies* (kurz: *PETs*) zusammengefasst werden. PETs umfassen eine Reihe von Technologien, die gemeinsam mit organisatorischen Maßnahmen das Prinzip der Datensparsamkeit in Informationstechnologien transformieren, eine anonyme oder pseudonyme Nutzung von Diensten ermöglichen oder den Benutzer direkt bei der Wahrung seiner Privatsphäre unterstützen [Cas, Peissl, 2002, S 27].

PETs sind Anwendungen, die die Privatheit von Benutzern und deren Daten im Internet verbessern sollen. Üblicherweise werden diese Systeme in folgende Gruppen aufgeteilt [Wörndl, 2003, S 41]:

- Verschlüsselungs- und Filtersysteme (siehe *1.7.2.1 Kryptologie, 1.7.2.4 Perimetersicherheit*),
- Verfahren zur Anonymisierung und Pseudonymisierung (siehe *2.4.4 Anonym Surfen, 2.4.5 Anonym Mailen, 2.4.6 Pseudonym Surfen und Mailen*),
- Policy-Tools: Anwendungen, die es Dienstanbietern und Benutzern erlauben, Praktiken im Bezug auf Privatheit von Diensten offen zu legen und auszuwerten. Diese sollen Benutzer informieren, welche personenbezogenen Daten über sie gesammelt und wie diese Informationen verwendet werden (siehe *2.4.2.1 Platform for Privacy Preferences*).

Da Verschlüsselungs- und Filtersysteme und mit P3P das wesentlichste Policy-Tool bereits betrachtet wurden, werden im Folgenden einige Anwendungen zur Anonymisierung und Pseudonymisierung vorgestellt. Generell kann mit Hilfe von Anonymisierungs- und Pseudonymisierungs-Tools das Identitätsziel (siehe *2.1 Problemstellung und Herausforderung*) einer anonymen und pseudonymen Kommunikation und eine Verbesserung der Vertraulichkeit erreicht werden [Wörndl, 2003, S 45].

2.4.4 ANONYM SURFEN

Es gibt eine Reihe von Möglichkeiten, um Anonymität beim Surfen im Internet zu erreichen. Exemplarisch sollen einige Verfahren dargestellt werden, es gibt aber noch andere (z. B.: Freenet[613]), auf die nicht näher eingegangen wird.

[613] http://freenetproject.org/ [3. Juli 2007]

Im September 2006 beschlagnahmte die Polizei in Deutschland in einer bundesweiten Aktion ein Dutzend Server, die dem anonymen Surfen dienten. Laut Angaben der Strafverfolger sollte ein Kinderpornoring ausgehoben werden. Beobachter der Szene vermuten eher eine Aktion gegen Anonymisierungsserver-Betreiber. Diese sollten *die Macht der Behörden* zu spüren bekommen, um sie zur Kooperation zu bewegen. Die Politik fordert seit Jahren im Kampf gegen den Terrorismus Einschränkungen bei der Anonymisierung [c't, 2006-4, S 208].

2.4.4.1 Anonymisierungs-Proxys

Um beim Surfen die IP-Adresse zu verschleiern, werden sogenannte *Anonymizer*[614] (z. B.: *http://www.anonymizer.com/* [3. Juli 2007], *http://www.nutzwerk.de/safersurf/* [3. Juli 2007]) benutzt. Die häufigste und einfachste Variante sind anonymisierende Proxyserver. Der Benutzer gibt in ein Webformular oder einen Client die gewünschte Webadresse ein, die an den Anonymisierungsdienst weitergeleitet wird. Der besuchte Server erhält dadurch beim Verbindungsaufbau nicht die IP-Adresse des Clients, sondern jene des Proxys (Anm.: mit Seite *http://www.leader.ru/secure/who.html* kann die Funktionalität eines Anonymizers überprüft werden). Zudem entfernen die Anonymizer-Dienste alle Daten des Requests (z. B.: Cookies, Referer), die den User identifizieren könnten [Atzinger et al., 2002, S 8].
Das Problem dabei ist, dass der Proxybetreiber die Identität des Benutzers kennt und diese auf Anfrage herausgeben kann.

2.4.4.2 Crowds

Bei der Anonymisierung durch *Crowds* werden die Webanfragen einzelner Benutzer in einer Menge von Crowds-Mitgliedern *versteckt*. Eine Webanfrage wird nicht an den betreffenden Webserver direkt, sondern an einen zufällig ausgewählten, anderen Crowds-Benutzer – bzw. dessen Crowds-Client – geschickt. Die Anfrage durchläuft damit zunächst mehrere dieser Crowds-Clients, damit kann ein Diensteanbieter Anfragen nicht mehr einem bestimmten Benutzer zuordnen [Reiter, Rubin, 1997, S 8].

[614] http://www.anonymitaet.com/anonymisierer/index.html [3. Juli 2007]

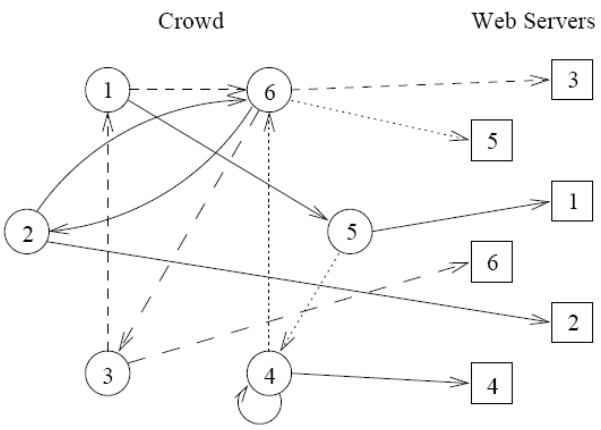


Abbildung 40: Crowds

Crowds besitzen den Vorteil, dass keine zentrale Komponente wie ein Anonymisierungs-Proxy erforderlich ist. Allerdings kann ein Angreifer, der den Kommunikationsverkehr abhört, durch eine zeitliche Verkettung von Nachrichten deren Verfolgung erreichen. Zudem lässt sich durch Crowds nur eine Sender- und keine Empfängeranonymität erzielen. Beschränkend ist auch die Tatsache, dass eine genügend große Menge von Benutzern vorhanden sein muss, um eine Anonymität zu gewährleisten [Wörndl, 2003, S 45].

2.4.4.3 Mix-Konzepte

Bei Mix-Konzepten wird die Kommunikationsbeziehung zwischen Sender und Empfänger einer Nachricht durch Knoten im Netzwerk, sogenannte *Mixe*, verborgen, die eine Verkettung von Nachrichten verhindern. Das Ziel ist die Anonymisierung der Kommunikationsbeziehung:

- der Empfänger bleibt vor dem Sender anonym,
- der Sender bleibt vor dem Empfänger anonym,
- Sender und Empfänger bleiben voreinander anonym.

Ein Mix spielt dabei – ähnlich einem Proxy – die Rolle eines Nachrichtenvermittlers. Er nimmt Nachrichten an und sorgt dafür, dass die von ihm weitergereichten Nachrichten nicht zu den von ihm angenommenen in Beziehung gesetzt werden können (durch Änderung der Reihenfolge der ausgehenden Nachrichten, durch Umkodieren via asymmetrischer Verschlüsselung, durch Erzeugung von *Dummy*-Nachrichten etc.).
Als Nachteil erweist sich die aufwändig durchzuführende asymmetrische Verschlüsselung jeder Nachricht. Neben der schlechten Performance stellt sich das Problem, dass einzelne Nachrichten in den Mix-Stationen verzögert werden, was bei synchroner Kommunikation behindernd ist [Wörndl, 2003, S 45f].

Beispielhaft für Mix-Konzepte werden im Folgenden *Onion-Routing*, dessen Weiterentwicklung *Tor* und *Java Anon Proxy* (kurz: *JAP*) vorgestellt.

2.4.4.3.1 Onion-Routing und Tor

Beim Onion-Routing[615] werden die Webinhalte über ständig wechselnde Routen von mehreren Mixen geleitet. Diese stellen verschlüsselnde Proxyserver dar. Dadurch bleibt die Identität dessen, der die Daten angefordert hat, für den Webserver auf der anderen Seite anonym. Selbst die Betreiber der Nodes sind aufgrund des Verschlüsselungsschemas nicht in der Lage, eine Zuordnung zwischen dem Benutzer und seinen angeforderten Webinhalten herzustellen, es sei denn, alle Nodes der jeweiligen Route arbeiten zusammen. Ziel ist es, nicht nur die Daten zu verbergen, sondern auch die Tatsache, dass überhaupt kommuniziert wird. Ein Onion-Routing bedarf einer ständigen Verbindung zwischen den einzelnen Onion-Routern, da die Daten beidseitig geschickt werden müssen. Der Vorteil ist, dass ein einziger vertrauenswürdiger Onion-Router ausreicht, um die volle Anonymität der Verbindung zu garantieren [Atzinger et al., 2002, S 8].

Eine Zurechenbarkeit von Nachrichten zu Sender oder Empfänger ist nicht möglich, da sehr viele Nachrichten die Menge der Onion-Router passieren und damit keine Zuordnung von eingehenden zu ausgehenden Nachrichten vorgenommen werden kann [Wörndl, 2003, S 46f].

Ein verbreitetes Programm zur Nutzung von Onion-Routing ist Tor, das vielfach als Weiterentwicklung von Onion-Routing angesehen wird. Im September 2006 wurde von der Gruppe *Hacktivismo*[616] der Webbrowser *Torpark*[617], der die IP-Adresse des Benutzers mittels Onion-Routing verschleiert, veröffentlicht[618]. Torpark ist eine einzelne installierbare Datei, die von einem USB-Stick aus gestartet werden kann und von jedem Windows-Rechner aus anonymes Surfen ermöglichen soll. Torpark ist so konfiguriert, dass er zunächst zum Tor-Proxy Kontakt aufnimmt und die Anfragen des Users dann über das Tor-Netzwerk ins Internet weiterleitet. Die Abfragen des Nutzers werden innerhalb des Tor-Netzwerks mehrfach verschlüsselt und so verschickt, dass sie nicht von Rechner zu Rechner zurückverfolgt werden können.

2.4.4.3.2 JAP

Mit JAP (Anm.: der kommerzielle Dienst heißt *JonDo*[619]) wird eine Anonymisierung der Internetzugriffe erreicht, indem sich die Computer nicht direkt zum Webserver verbinden, sondern ihre Kommunikationsverbindungen verschlüsselt über den Umweg von mehreren Zwischenstationen,

[615] http://www.onion-router.net/[3. Juli 2007]
[616] http://www.hacktivismo.com/ [3. Juli 2007]
[617] http://www.xerobank.com/download.html [3. Juli 2007]
[618] Vgl. http://futurezone.orf.at/hardcore/stories/137959/ [3. Juli 2007]
[619] http://www.jondos.de/ [4. Juli 2007]

sprich Mixe, laufen[620]. Bei JAP ist vorgegeben, in welcher Reihenfolge die Mixe verwendet werden können. Eine Folge zusammengeschalteter Mixe nennt man *Mixkaskade*. Die Nutzer können zwischen verschiedenen Mixkaskaden auswählen.

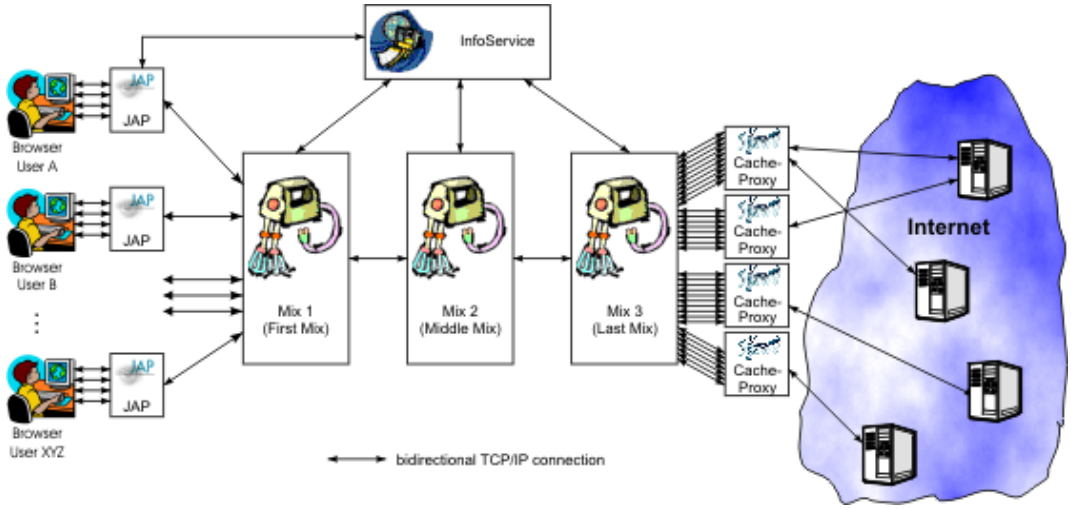


Abbildung 41: Anonymisierung mit JAP

Da viele Benutzer gleichzeitig diese Zwischenstationen des Anonymitätsdienstes nutzen, werden die Internetverbindungen jedes Benutzers unter denen aller anderen Benutzer versteckt. Kein Außenstehender, kein anderer Benutzer, nicht einmal der Betreiber des Anonymitätsdienstes kann herausbekommen, welche Verbindungen zu einem bestimmten Benutzer gehören. Im Regelfall werden die Mixe von unabhängigen Institutionen betrieben, die in einer Selbstverpflichtung erklären, dass sie weder Log-Files über die geschalteten Verbindungen speichern, noch derartige Daten mit den anderen Mix-Betreibern austauschen. JAP versetzt seine Benutzer in die Lage, die ihnen vertrauenswürdig erscheinenden Mixkaskaden aufgrund dieser Informationen gezielt auszuwählen.

2.4.4.4 CookieCooker

CookieCooker ermöglicht es dem Benutzer möglich, einerseits die durch Cookies und Anmeldung mit Benutzername und Passwort entstehenden Vorteile auf ausgewählten Webseiten zu nutzen und andererseits das Datensammeln zu erschweren, somit das *Profiling* zu verhindern.
Die wichtigsten Funktionen von CookieCooker[621]:

- Blockieren von Werbung,
- Verwendung unterschiedlicher Identitäten gegenüber einem Webserver,
- zufällige Auswahl der verwendeten Identität,
- Beschränkung der Speicherung von Cookies auf eine Session,
- Austausch von Cookies mit anderen Benutzern,

[620] Vgl. http://anon.inf.tu-dresden.de/ [3. Juli 2007]

- Unterstützung bei der Anmeldung bei Webdiensten,
- maximaler Datenschutz.

2.4.5 ANONYM MAILEN

Um anonyme E-Mails zu versenden, werden sogenannte *Remailer* benutzt. Diese entpersonalisieren Nachrichten, indem sie die Headerinformationen aus den E-Mails entfernen, damit Rückschlüsse auf den Absender nicht möglich sind. Durch die Einbeziehung asymmetrischer Verschlüsselung (siehe *1.7.2.1.1 Verschlüsselungsverfahren*) erhöht sich die Sicherheit des Verfahrens. Unterschieden werden die Remailer-Typen *Cypherpunkt*[622], *Mixmaster*[623] und *Mixminion*[624]. Die Remailer-Software kann auf einem PC, einem Client im LAN oder auf einem Rechner im Internet installiert sein[625].
Da viele Remailer immer wieder Ziel von Angriffen sind, haben viele Betreiber, die aus Idealismus solche Dienste angeboten haben, aufgegeben. Remailer-Diensteanbieter definieren, um Missverständnissen hinsichtlich ihrer Motive vorzubeugen, als Selbstschutzmaßnahme Regeln. Ein Beispiel von Anti-Missbrauchs-Regeln eines Remailers[626]: „*Ich betrachte Folgendes als unzulässige Verwendung dieses anonymen Remailers und werde Schritte unternehmen, jedermann davon abzuhalten, folgendermaßen vorzugehen:*

- *Versendung von Nachrichten, die in erster Linie stören oder ärgern sollen.*
- *Benutzung des Remailers zu irgendwelchen illegalen Zwecken. Aufgrund der globalen Natur des Internet, liegt es in der alleinigen Verantwortung des ursprünglichen Senders, herauszufinden, was gesetzlich vertretbar ist.*
- *Unerwünschte, kommerzielle Werbebotschaften (Spam).*
- *Beschwerden an die Versender unerwünschter Werbemails.*"

Ebenso wenig wie die Post können auch Remailer verhindern, dass durch sie unerwünschte Nachrichten gesendet werden. Remailer-Betreiber haben aber die Möglichkeit, gewisse E-Mail-Adressen zu sperren. Eine Liste von Remailern befindet sich auf der Homepage des *Datenschutzzentrums für Schleswig-Holstein*[627].

[621] Vgl. http://www.cookiecooker.de/ [3. Juli 2007]
[622] http://www.bsi.de/literat/anonym/anwmix.htm#6.1 [5. Juli 2007]
[623] http://mixmaster.sourceforge.net/ [4. Juli 2007]
[624] http://www.mixminion.net/ [5. Juli 2007]
[625] Vgl. http://www.emailprivacy.info/remailers/ [5. Juli 2007]
[626] Vgl. http://www.anon.gildemax.de/ [5. Juli 2007]
[627] https://www.datenschutzzentrum.de/projekte/anon/links.htm#remail [5. Juli 2007]

2.4.6 PSEUDONYM SURFEN UND MAILEN

Oftmals ist eine vollständige Anonymität nicht möglich bzw. wünschenswert, da es beispielsweise für Personalisierungsdienste erforderlich sein kann, dass sich Benutzer gegenüber einem Dienst identifizieren, damit einzelne Aktionen (z. B.: Auswertung von Benutzerinteressen) einem Benutzer zugeordnet werden können, ohne jedoch dessen wahre Identität zu kennen. Um diese Funktionalität zu ermöglichen, werden Pseudonyme verwendet (siehe *2.2.2 Pseudonymität*). Eine diesbezügliche Anwendung bietet das Produkt Anonymizer (siehe *2.4.4.1 Anonymisierungs-Proxys*). Benutzer laden von der Webseite eine Client-Software und installieren diese am PC. Eine Funktion ist die Erstellung und die Verwaltung von Pseudonymen (hier: *Nyms*):

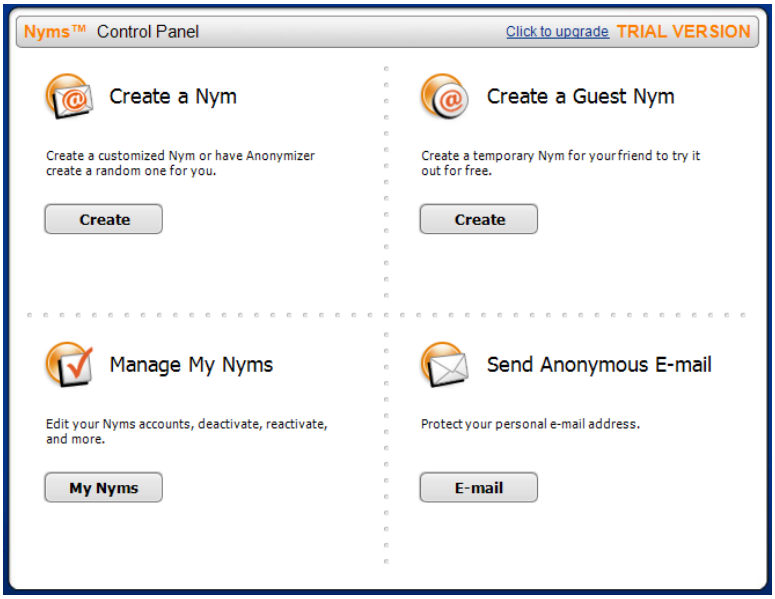


Abbildung 42: Pseudonym-Funktion von Anonymizer

Das ermöglicht, Pseudonyme selbst zu wählen oder per Zufallsgenerator erzeugen zu lassen. Die Nyms können in Kategorien eingeteilt (z. B.: Diskussion, Einkauf, Informationsmaterial etc.) und beschrieben (bei welcher URL verwendet, bis wann gültig) werden, damit bei einer Vielzahl an Pseudonymen auch zu einem späteren Zeitpunkt die Verwendung noch erkennbar bleibt. Pseudonymisierungs-Dienste können Beschränkungen von Anonymisierungstools aufheben, ohne eine Preisgabe der Identität des Benutzers nötig zu machen. Als weitere Besonderheit kann durch Erzeugen einer Pseudo-E-Mail-Adresse die Herausgabe einer echten E-Mail-Adresse vermieden werden. Eine E-Mail-Adresse ist oft für Dienste erforderlich, erlaubt aber meist auch Rückschlüsse auf die Identität des Benutzers bzw. birgt die Gefahr unerwünschter Werbe-E-Mails (siehe *1.6 Exkurs: E-Mail/Spam*) [Wörndl, 2003, S 46].

2.4.7 BEREICHSSPEZIFISCHES PERSONENKENNZEICHEN UND BÜRGERKARTE IM E-GOVERNMENT

Informationsverbundsysteme etablieren sich in allen behördlichen Bereichen und stellen hohe Anforderungen an den Datenschutz. E-Government soll dem Individuum Zugang zu seinen eigenen Daten eröffnen, der Staat muss den Rahmen setzen, damit die Bürger ihr informationelles Selbstbestimmungsrecht ausüben können (siehe *2.3.3.1.1 E-Government*). Eine Regelung hinsichtlich Datenverwaltung stellt das sogenannte bereichsspezifische Personenkennzeichen dar.

Von staatlicher Seite gibt es den Wunsch, ein eindeutiges Personenkennzeichen einzuführen, mit dem jeder einzelne Bürger eindeutig identifiziert werden kann. Ein offizielles Personenkennzeichen wie in anderen Ländern gibt es in Österreich nicht, es existieren jedoch einige solcher eindeutiger Nummernsysteme, die einem solchen Personenkennzeichen (Sozialversicherungsnummer, ZMR-Zahl etc.) entsprechen. Aus datenschutzrechtlicher Sicht liegt die Problematik eindeutiger Personenkennzeichen jedoch darin, dass sie eine eindeutige Verknüpfung unterschiedlicher Datenbestände ermöglichen. So ermöglicht die Verwendung der Sozialversicherungsnummer in den verschiedensten Bereichen (z. B.: als eindeutiger Schlüssel in der Bildungsevidenz, Leistungen des Arbeitsmarktservices, beim Abschluss eines Bausparvertrages, beim Antrag auf Studienbeihilfe, in der Verwaltung von Präsenz- und Zivildienern) eine Verknüpfung von Daten aus diesen Bereichen. Auch wenn eine solche direkte Verknüpfung gegenwärtig in vielen Fällen rechtlich unzulässig ist, wird dennoch die technische Grundlage für den gläsernen Menschen geschaffen[628].

Mit der Einführung des österreichischen E-Government-Gesetzes am 1. März 2004 bzw. dessen Novelle[629] am 1. Jänner 2008 wurde versucht, eine neue, datenschutzkonforme Lösung der Personenkennzeichenproblematik herbeizuführen. Die in diesem Zusammenhang wesentlichen Begriffe werden wie folgt definiert[630]:

- *Stammzahl* (§2 Z 8): eine zur Identifikation von natürlichen und juristischen Personen und sonstigen Betroffenen herangezogene Zahl, die demjenigen, der identifiziert werden soll, eindeutig zugeordnet ist und hinsichtlich natürlicher Personen auch als Ausgangspunkt für die Ableitung von (wirtschafts-) bereichsspezifischen Personenkennzeichen (§8, §14) benutzt wird. Laut §6 (2) wird für natürliche Personen, die im Zentralen Melderegister einzutragen sind, die Stammzahl durch eine mit starker Verschlüsselung gesicherten Ableitung aus ihrer ZMR-Zahl (§16 Abs. 1 des Meldegesetzes 1991, BGBl. Nr. 9/1992) gebildet. Für alle anderen natürlichen Personen ist ihre Ordnungsnummer im *Ergänzungsregister* (Abs. 4) (kurz: *ERnP*)[631] für die Ableitung der

[628] Vgl. http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=50350pcj [5. Juli 2007]
[629] http://www.a-sit.at/pdfs/E-GovG%20Novelle%202007%20BGBl%207_2008.pdf [11. März 2008]
[630] Vgl. http://www.digitales.oesterreich.gv.at/site/5581/default.aspx [5. Juli 2007]
[631] http://portal.bmi.gv.at/ref/portref/ernp.html [9. Juli 2007]

Stammzahl heranzuziehen. Die Stammzahl von natürlichen Personen darf bei elektronischen Behördenverfahren aus Datenschutzgründen nicht direkt in Applikationen gespeichert werden.

- Das *bereichsspezifische Personenkennzeichen* (§9 (1)) (kurz: *bPK*) wird durch eine Ableitung aus der Stammzahl der betroffenen natürlichen Person gebildet. Die Identifikationsfunktion dieser Ableitung ist auf jenen staatlichen Tätigkeitsbereich (im Detail siehe *Bereichsabgrenzungsverordnung*[632]) beschränkt, dem die Datenanwendung zuzurechnen ist, in der das Personenkennzeichen verwendet werden soll. Die zur Bildung des bPK eingesetzten mathematischen Verfahren (Hash-Verfahren über die Stammzahl und die Bereichskennung) werden von der Stammzahlenregisterbehörde festgelegt (§9 (3)). Die bPK identifiziert den Bürger im Verfahren (ähnlich der Steuernummer in Finanzverfahren), wodurch dem Bürger seine Daten immer wieder eindeutig zugeordnet werden können. Durch den Einsatz der mathematischen Einwegfunktion wird die Möglichkeit der Rückrechnung von der bPK auf die Stammzahl ausgeschlossen. Das heißt, dass alle Einträge eines Bürgers in unterschiedlichen Verwaltungsbereichen auch verschiedene Zahlen haben und die Daten somit nicht verknüpfbar sind.

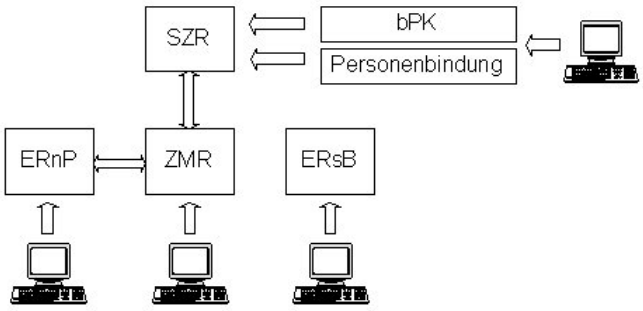


Abbildung 43: Zusammenhänge der verschiedenen Register sowie die grundlegenden Zugangsmöglichkeiten für Behörden und/oder Privatpersonen

Zur Wahrung des Datenschutzes wird daher im österreichischen E-Government auf ein einheitliches Personenkennzeichen in Verfahren verzichtet. Benötigt eine Behörde zur Identifikation einer Person ein bereichsspezifisches Personenkennzeichen aus einem anderen Verfahrensbereich (Fremd-bPK), darf dieses von der Stammzahlenregisterbehörde beauskunftet und verspeichert werden. Die Stammzahlregisterbehörde übermittelt das Fremd-bPK ausschließlich verschlüsselt an die anfragende Behörde [Bundeskanzleramt, 2006, S 125f].

Ein zentrales Element der IT-Sicherheitsmaßnahmen im Bereich von E-Government bildet das Konzept „Bürgerkarte“. Die Funktion Bürgerkarte ist im E-Government-Gesetz verankert. Sie umfasst

[632] http://www.ris.bka.gv.at/bundesrecht/ Suche nach: Bereichsabgrenzungsverordnung [1. August 2007]

die elektronische Signatur (siehe *1.7.2.1.7 Elektronische Signatur*) und die eindeutige Identifikation auf Basis der Stammzahl, welche auf der Karte gespeichert ist. Dabei wird der Begriff der Bürgerkarte dadurch erweitert, dass jede technische Einrichtung (Sozialversicherungskarte, Bankomatkarte, Mobiltelefone etc.), die diese Eigenschaften erfüllt, als Bürgerkarte infrage kommt. Sie haben die geeignete Identifikation und den Schutz vor Missbrauch zu gewährleisten.

Mit der Personenbindung[633] und den elektronischen Vollmachten wird eine eindeutige Identifikation des Antragstellers ermöglicht, mittels elektronischer Signatur wird die Authentizität des Anbringens bei elektronischen Behördenverfahren ermöglicht. Unsichere Passwortsysteme und eine Einzelregistrierung für jedes Verfahren werden damit und durch die elektronische Signatur ersetzt.

Das E-Government-Gesetz stellt fest, dass eine Identifikation nur zulässig ist, wenn diese auch inhaltlich geboten ist. Situationen, wo prinzipiell zum Einstieg in ein Web-Angebot die Identifikation von der Person verlangt wird – etwa um das Nutzerverhalten zu ermitteln – werden damit explizit verhindert. Beim Ausfüllen von konventionellen Formularen wird oft eine Fülle von Daten (Name, Wohnort, Sozialversicherungsnummer etc.) eingefordert. Diese Angaben sind notwendig, um eine eindeutige Identifikation des Antragstellers zu erleichtern (Anm.: beim Ausfüllen eines Formulars können aufgrund unterschiedlicher Schreibweisen oder Oberflächlichkeit Fehler unterlaufen, die eine eindeutige Identifikation erschweren bzw. unmöglich machen). Mittels Bürgerkarte wird die eindeutige Identifikation hingegen automatisiert durchgeführt. Beim Musterverfahren „Elektronische Strafregisterbescheinigung“ sind die Benutzereingaben auf ein Minimum beschränkt, Name und Geburtsdatum werden direkt von der Karte eingelesen. Die Identifikation ist eindeutig, es sind nur noch verfahrensspezifische Informationen notwendig. Bei hinreichender Verbreitung neuer E-Government Verfahren und Technologien könnte in einzelnen Verfahren sogar darauf verzichtet werden, zusätzliche Informationen zu den Identifikationsdaten im Rahmen der bereichsspezifischen Personenkennung zu speichern. So könnte beispielsweise im Bereich der Statistik eine gänzliche Anonymisierung stattfinden. Mit dieser Technologie wäre etwa eine zukünftige Führerscheinentzugsanwendung so realisierbar, dass eine Person erst dann identifiziert werden kann, wenn weitere Verfehlungen mit gesetzlichen Folgen eintreten, ansonsten aber die Identität der Person nicht preisgegeben wird. Mit der elektronischen Abwicklung von Verfahren wächst daher nicht automatisch die Gefahr der *Vergläserung des Menschen*. Die eindeutige Identifikation von Personen

[633] Bei der elektronischen Antragstellung an die Behörde muss die Person, die den Antrag stellt, eindeutig identifiziert und authentifiziert werden. Bei der Personenbindung wird dem Signaturzertifikat einer Person ein eindeutiges Identitätsmerkmal – die Stammzahl – zugeordnet. Diese Verknüpfung zwischen Zertifikat und Person wird elektronisch von der Behörde signiert. Damit ist eine kryptographisch gesicherte Bindung zwischen der elektronischen Signatur einer Person und eines für diese Person eindeutigen Identifikationsmerkmals gegeben. Die Personenbindung ermöglicht die eindeutige, automatisierbare Identifikation einer Person bei der elektronischen Kommunikation mit der Behörde über bereichsspezifische Personenkennzeichen.

wurde bisher immer auch bei Papierverfahren verwendet. Vielmehr kann eine elektronische Abwicklung auch dazu genutzt werden, die Tätigkeit der Behörde kontrollierbarer zu machen[634].

An dieser Stelle muss angemerkt werden, dass es den Konzepten an Praxisnähe mangelt und sie daher in Umsetzung und Verbreitung deutlich weniger Fortschritte machen als erwartet. Das bPK ist ein komplexes Verfahren, dass erst vereinzelt implementiert wurde, da sich die Integration in die diversen Applikationen aufwendig gestaltet.

Gegen den Einsatz der Bürgerkarte sprechen technische wie organisatorische Hürden, das Fehlen der Einbindung der Wirtschaft und einer sogenannten *Killer-Applikation*. Der Betrieb erfordert einen kostenpflichtigen externen Kartenleser, die Installationsroutine erweist sich als fehleranfällig und kompliziert[635]. Mit Jahresende 2007 läuft die Verwaltungssignatur (bietet gegenüber der sicheren Signatur eine Vereinfachung und wurde geschaffen, um im E-Government den Einsatz elektronischer Signaturen voranzutreiben) aus, eine Verlängerung ist nicht vorgesehen, das heißt, danach ist die Freischaltung der Bürgerkartenfunktion auf der E-Card nicht mehr möglich. Die Versuche, die Banken davon zu überzeugen, die Bürgerkarte für das Onlinebanking zu verwenden, sind bis dato nicht von Erfolg gekrönt. Des Weiteren hat einer Statistik[636] des Österreichischen Bundeskanzleramts zufolge ein Bürger lediglich 1,7 Behördenkontakte pro Jahr, zugleich genügen für viele Verfahren Credentials in Form von Benutzername und Passwort.

Chancen für den vermehrten Einsatz der Bürgerkarte könnten zum einen durch die Generierung eines Nutzens für den Benutzer und zum anderen durch die Vereinfachung des Betriebs (z. B.: Verwendung von Mobiltelefonen) erreicht werden[637].

Ansonsten gibt es bereits Bestrebungen und Vorschläge, überall dort, wo keine elektronische Signatur notwendig ist, auf die Bürgerkarte zu verzichten und eine einfache Identifikation mit in den zentralen Registern ZMR und ERnP gespeicherten Usernamen samt Passwort zu forcieren.

2.5 FAZIT

Die Vielfalt der Datenverarbeitung führt zu einer sprunghaften Zunahme von personenbezogenen Daten mit hoher Aussagekraft. Sie erlauben, individuelles Verhalten ebenso detailliert nachzuvollziehen wie kollektive Lebensstrukturen [Roßnagel, 2007, S 204]. Treibende Faktoren sind vor allem der steigende Einsatz von Internettechnologien in allen Lebensbereichen und die allgegenwärtige Datenverarbeitung. Pervasive Computing verändert die Interaktion des Menschen mit Informationstechnik und schafft dadurch Verhältnisse, in denen viele Beteiligte in wechselnden Rollen mitwirken. Zudem werden vielfältige Zwecke gleichzeitig verfolgt und die Datenverarbeitung von den

[634] Vgl. http://www.cio.gv.at/faq/AllgemeineAspekte/ [5. Juli 2007]
[635] Vgl. http://oe1.orf.at/highlights/73241.html [5. Juli 2007]
[636] Persönliche Mitschrift aus einer Diskussionsrunde im Rahmen der E-Government-Konferenz 2007 (http://e-government.adv.at/2007/ [5. Juli 2007])
[637] Vgl. http://derstandard.at/?url=/?id=2844671 [5. Juli 2007]

Techniksystemen – für den Betroffenen unbemerkt und in ihren Wirkungen undurchschaubar – selbst organisiert. Wenn allgegenwärtige Datenverarbeitung so funktioniert, wie sie soll, funktioniert sie immer auch als Überwachungstechnologie. Zu einem großen Teil sind es die Benutzer selbst, die den Systemen ihre Daten über Lebensumstände, Bedürfnisse und Präferenzen anvertrauen. Informationen, die in einem anderen Kontext auch gegen sie verwendet werden könnten. Die staatlichen und kommerziellen Interessen am Data Mining und an der Gewinnung von Profilen sind jedenfalls groß.

Angesichts des enormen Überwachungspotentials sind gesetzliche, organisatorische und technische Vorkehrungen zum Schutz der Privatsphäre unvermeidlich.

Auf die neuen Verhältnisse sind die Grundsätze des Datenschutzes nicht ausgelegt bzw. kaum anwendbar. Sie entstanden zu einer Zeit, als die Datenverarbeitung mit überschaubaren Zuständigkeiten und Verantwortlichkeiten noch auf zentralen Großrechnern erfolgte. Die seinerzeit geprägten Grundsätze der Transparenz, Zweckbindung, Erforderlichkeit oder Mitwirkung des Betroffenen widersprechen teilweise den Zielen, die mit der allgegenwärtigen Datenverarbeitung verfolgt werden. Daher ist eine Modernisierung des Datenschutzrechts, die den künftigen Bedingungen allgegenwärtiger Datenverarbeitung gerecht wird, notwendig. Zum anderen ist eine der Ursachen für die faktisch geringe Wirkung der den Datenschutz betreffenden Gesetze in den mangelnden Kompetenzen und Möglichkeiten der dafür zuständigen Behörden zu sehen. Hier kann eine Stärkung der Datenschutzbehörden mit erweitertem Verantwortungs- und Prüfungsbereich Abhilfe schaffen.

Die beste Strategie, seine Privatsphäre zu schützen, ist jene der Datenvermeidung. Verfahren und Applikationen müssen so konzipiert werden, dass möglichst wenig personenbezogene Daten erfasst werden. Dieser Grundsatz muss bereits bei der Gestaltung von Technik und ihrer Einsatzbedingungen berücksichtigt werden. Für die Technikgestalter müssen Anreize geschaffen werden, Datenschutz in der Infrastrukturentwicklung zu integrieren. Besonders im Rahmen der E-Government-Aktivitäten sollte – aufgrund der Vorbildwirkung für die privatwirtschaftlichen Unternehmen – auf die Implementierung von datensparenden Technologien geachtet werden. Zudem ist es notwendig, die Benutzer entsprechend zu informieren, sie in die Lage zu versetzen, die Mechanismen zu erkennen, um dann bewusst eine Nutzungsentscheidung treffen zu können. Hinsichtlich Selbstregulierung gilt, dass einerseits bewusste Konsumenten und andererseits ein Staat, der bereit ist, Gesetzen Nachdruck zu verleihen und bei einer Missachtung von Grundrechten entsprechende Sanktionen zu setzen, Grundvoraussetzungen für freiwillige Maßnahmen und der Kooperation von Unternehmen sind. Als überwiegend unternehmensinterner Prozess mit wenig Sichtbarkeit nach außen und eingeschränkter Kontrollierbarkeit ist ein faires Verhalten von Unternehmen notwendig, um die Privatsphäre der Kunden (z. B.: bei Data Mining) schützen zu können.

Die technischen Konzepte sind entwickelt und es existieren eine Reihe von Services und Tools, die den Kunden eine anonyme bzw. pseudonyme Nutzung ermöglichen oder sie vor unbemerkten

Datensammlungen bewahren können. Die angebotenen Dienste und Programme sind von unterschiedlicher Wirksamkeit und Benutzerfreundlichkeit, zudem teilweise geprägt von Brüchen in der Verfügbarkeit. Verschlüsselung, Anonymität, Pseudonyme und bewusste Technologienutzung durch die Verwendung unterschiedlicher Medien zu unterschiedlichen Zwecken zeigen mögliche Wege zur Aufrechterhaltung bzw. Wiederherstellung von Privatsphäre. Unter der Voraussetzung eines bestmöglich geschützten Privatbereichs soll dem Benutzer die Hoheit über seine Daten gegeben werden. Dazu notwendig sind *freiheitsfördernde* Architekturen der Informationstechnik, die die Zusammenführung personalisierbarer Daten durch „informationelle Gewaltenteilung“ verhindern.

Identitätsmanagementsysteme, die im nächsten Kapitel dargestellt werden, stellen solche Architekturen dar. Es sollen Ansätze aufgezeigt werden, wie es Mitarbeitern in Betrieben damit ermöglicht werden kann, ihren Anspruch auf Privatheit zu wahren. Die Möglichkeit zur informationellen Selbstbestimmung muss in einer immer stärker durch Informationstechnologien geprägten Umwelt gewahrt und gestärkt werden.

3 IDENTITÄTSMANAGEMENT

3.1 PROBLEMSTELLUNG UND HERAUSFORDERUNG

Die rasche Entwicklung der technischen Möglichkeiten und die zunehmenden Korruptionsfälle sowie Daten- bzw. Identitätsdiebstähle (siehe *1.3.5 Computerkriminalität, 1.3.5.2 Datendiebstahl und Spionage, 1.3.5.3 Identitätsdiebstahl*) verleihen dem Thema „Mitarbeiterüberwachung“ neue Brisanz (siehe *2.3.4 Exkurs: Privacyaspekte für den betrieblichen User*). Dabei geht es nicht nur um den Missbrauch von Internet und E-Mail am Arbeitsplatz, sondern auch um ein erhöhtes Sicherheitsbedürfnis der Unternehmen angesichts der Risiken der Informationstechnologie (siehe *1.3 Taxonomie von Angriffen auf den Wert Information*). Die fortschreitende Vernetzung der Geschäftsprozesse bzw. Firmenübernahmen und Partnerschaften bringen eine steigende Komplexität der IT-Infrastruktur mit sich. Die Systeme müssen so konzipiert sein, um von der zunehmenden Digitalisierung und Interaktion mit Geschäftspartnern über das Internet profitieren zu können. Die Folge ist eine weitere Heterogenisierung der IT-Infrastruktur und ein Ansteigen der Zahl an Applikationen. Betriebssysteme, Datenbanken, Applikationen und Portale haben ihre jeweils eigenen Authentifikationsmechanismen und Credentials. Zudem führt die vermehrte Interaktion mit Kunden zu einem sprunghaften Anstieg von Benutzeridentitäten (siehe *2.2.1 Digitale Identität*). Dies belastet zum einen den Anwender mit einer größer werdenden Anzahl an Benutzernamen und Passwörtern, zum anderen bedeutet das für die IT-Abteilung einen steigenden administrativen Aufwand in der Benutzerverwaltung, weil nicht nur Benutzer und Berechtigungen für Mitarbeiter, sondern auch für Kunden bzw. Bürger, Partner und Lieferanten verwaltet werden müssen. Diese Heterogenität verursacht enorme Kosten für die Benutzer- und Berechtigungsverwaltung. Zudem gilt es, die Verschiedenartigkeit der Zugriffe technisch umzusetzen. Jedenfalls führt die Aufrüstung der unternehmensweiten IT in ein Dilemma: Wie können in einer solchen Umgebung gleichzeitig IT-Kosten kontrolliert, ein notwendiger Sicherheitsstandard gewahrt und der Zugang zur Information als wesentlicher Produktionsfaktor erweitert und kontrolliert werden?

Das Management digitaler Identitäten gewinnt zunehmend an Bedeutung. Zum einen erfordert das Denken in übergreifenden Geschäftsprozessen eine einheitliche und offene Infrastruktur. Zum anderen setzt der Trend zu verteilten Anwendungen und zur Ressourcenvirtualisierung – etwa in Form von Web Services oder Service-orientierten Architekturen (kurz: SOA) – digitale Identitäten sowie automatisierte Rechteprüfungen voraus. Mit der unternehmerischen Dynamik verstärkt durch Mitarbeiterfluktuation und Personalrochaden steigt der Bedarf an Rollen- und Rechtemanagement. Daneben verbietet ein gestiegenes Sicherheitsbewusstsein die „gut gemeinten“ *Workarounds* der Vergangenheit. Die durch E-Business bzw. E-Government verschwimmenden Unternehmensgrenzen erfordern eine neue, identitätsbasierende Sicherheitsarchitektur. Gesetze und Regulative wie Basel II (siehe *1.8.4.3.1 Basel II)* oder Sarbanes-Oxley (siehe *1.8.4.3.2 Sarbanes Oxley Act*) setzen die Unternehmen im Sinne der Nachhaltigkeit und Auditierbarkeit unter Druck. Die unter dem Stichwort

„Corporate Governance“ geführte Diskussion hat damit einen verbindlichen Rechtsrahmen erhalten, der für viele Unternehmen die Notwendigkeit mit sich bringt, die Sicherheit und Zuverlässigkeit rechnergestützter Prozesse neu zu bewerten. Diese Compliance-Ansprüche sind nur durch einen hohen Grad an Automatisierung erfüllbar[638]. Ergänzt werden diese Anforderungen durch verstärkte Diskussionen hinsichtlich des Schutzes privater Informationen von Mitarbeitern in Unternehmen (siehe *3.5.1 Anforderungen und Nutzen* aus Mitarbeitersicht).

Die Verwaltung digitaler Identitäten stellt die Voraussetzung zur Realisierung von Zugriffsschutz und personalisierten Anwendungen dar. Identitäten sind erforderlich, um entscheiden zu können, wer auf welche Informationen wie und wann zugreifen darf bzw. um Informationen für Benutzer individualisieren zu können. Identitätsmanagement (engl. *Identity Management*) wird damit zur Grundlage der Unternehmensanwendungen. Der Trend hin zur verteilten Verarbeitung hat die Effektivität einer zentralen Kontrolle geschwächt. Es bedarf daher einer durchdachten Identitätsmanagement-Infrastruktur, um für die verteilten Systeme unternehmensintern eine Basis zu schaffen.

Ein funktionierendes Identitätsmanagement-Rahmenwerk birgt betriebswirtschaftliches Potenzial. Die Benutzerverwaltung, die bislang ausschließlich vom EDV-Administrator erledigt wurde, kann aufgeteilt werden. Ein großer Teil kann vom Benutzer selbst durchgeführt werden, ein anderer von der Personalabteilung, der technische Part bleibt der IT-Abteilung vorbehalten. Damit werden Ressourcen in der Unternehmens-IT frei für andere notwendige Arbeiten, der Mitarbeiter kann sich seiner Daten sicher sein, hat aber eine Bringschuld und trägt auch mehr Verantwortung. Durch das Splitten der Benutzerverwaltung erhöht sich auf der einen Seite die Benutzer-Produktivität, auf der anderen Seite wird eine Reduktion der Administrationskosten auf IT-Seite erreicht. Durch ein standardisiertes IM-Rahmenwerk wird die Basis für neue Geschäftsanwendungen – ohne den typischen Entwicklungsoverhead – gelegt. „Karteileichen“ oder über Jahre angesammelte Rechte eines Users werden durch ein Identitätsmanagementsystem verhindert (siehe *3.5.2 Anforderungen, Nutzen und treibende Faktoren* aus Unternehmenssicht).

Entsprechend vielschichtig sind auch die Technologien, die benötigt werden (siehe *3.4 Komponenten und Funktionen eines Identitätsmanagementsystems*). Verzeichnisdienste für die Speicherung von Identitätsinformationen, Verfahren für die Authentifizierung, Provisioning-Lösungen, um Benutzerberechtigungen in einem koordinierten Prozess in vielen Systemen anlegen zu können, Webaccess-Management-Systeme für die Steuerung externer Zugriffe oder Lösungen für die Benutzer- und Kennwortsynchronisation sind nur einige der Bausteine. Neben der Informationssicherheit gewinnen andere Nutzungsformen von Identitäten an Bedeutung. Die Personalisierung von Informationen gehört dabei zu den wichtigsten (siehe *2.2.4 Personalisierung*).

[638] Vgl. http://www.computerwoche.de/knowledge_center/it_security/594015/index2.html [30. Juli 2007]

Unter Identitätsmanagement wird der gesamte Prozess des Umgangs mit digitalen Identitäten – von ihrer Speicherung in Verzeichnisdiensten bis hin zu Technologien wie Digital Rights Management (siehe *2.3.3.5 Digital Rights Management*) oder der Personalisierung von Informationen – verstanden. Eine wesentliche Rolle spielen dabei Autorisierung, Authentifizierung und Administration (siehe *2.2.1 Digitale Identität* und *2.2.6 Autorisierung, Authentifizierung und Authentizität*). Diese Themen werden von vielen Unternehmen oft nur oberflächlich behandelt. Ein zentrales Identitäts- und Zugriffsmanagement ist die Grundvoraussetzung für Anwendungen, die auf Integration und Interaktion ausgelegt sind. Die konsequente Pflege verteilter Benutzer- und Rechteverwaltungen erweist sich schon bei 100 Benutzern und wenigen Anwendungen als schwieriges Unterfangen. Mit zunehmender Benutzer- und Applikationszahl steigen die Kosten für die Administration und die Fehlerquote[639].

Identitätsmanagementsysteme (kurz: IMS) sollen im betrieblichen Umfeld dem Benutzer die größtmögliche Freiheit über seine Daten geben. Es gilt – wie oben erläutert – technische wie organisatorische Hürden zu überwinden. Die Benutzer brauchen einen Mechanismus, ein Werkzeug, um den Zugriff auf ihre Daten kontrollieren zu können. Die Möglichkeiten der EDV-Abteilung bzw. einer höheren Instanz (Vorgesetzte, Personalabteilung), Mitarbeiter zu überwachen respektive ein vollständiges Mitarbeiterbild zeichnen zu können, sollen zumindest eingeschränkt werden: Arbeitszeitkontrolle, Internetsurfverhalten, E-Mail-Kommunikation, Datei-Zugriff etc. Im Sinne der Datensparsamkeit sollen nur jene Daten zur Verfügung gestellt werden, die unbedingt (z. B.: gesetzlich) notwendig sind. Ein Identitätsmanagementsystem soll es dem Benutzer ermöglichen, verschiedene Identitäten – Pseudonyme – zu definieren und zu wählen, in welcher Rolle er gegenüber dem Kommunikationspartner auftritt und welche Informationen er ihm offenbart. Der Benutzer soll eine dienstliche und eine private Rolle annehmen können. In der dienstlichen Rolle werden die Rechte des Users im Netzwerk bzw. lokal auf dem PC geregelt: Netzwerklogin, Druckerzuordnung, Abteilungslaufwerk, Applikationsrechte. Mit der privaten Rolle wird dem Mitarbeiter die Möglichkeit eingeräumt, persönliche Tätigkeiten (Online-Banking, Besuch von Webseiten privaten Interesses, Blogs etc.) durchzuführen.

Konzepte für ein umfassendes Identitätsmanagement gibt es seit 1985, als *David Chaum* vorgeschlagen hat, jedem Menschen einen persönlichen Card-Computer zu geben, der alle Bezahlvorgänge und andere Transaktionen für ihn erledigt und dabei durch Verwendung geeigneter Pseudonyme Datensicherheit und Datenschutz gewährleisten soll [Hansen, 2003, S 2]. Hinsichtlich der Einführung eines IMS in einem Unternehmen gibt es unterschiedliche Standpunkte. Viele sehen die Lösung in der Erweiterung des in der Regel bereits bestehenden Personalinformationssystems (kurz: PIS), andere befürworten ein eigenständiges IMS-Produkt mit integraler Vernetzung in das PIS.

[639] Vgl. https://www.kuppingercole.de/sections/basics [3. August 2007]

Der Autor dieser Dissertation ist seit 2004 in einem Unternehmen mit weit mehr als 1000 Benutzern mitverantwortlich für die Planung und Umsetzung von Maßnahmen im Rahmen eines umfassenden Informationssicherheitsmangementsystems. Eine der zu bewältigenden Herausforderungen besteht in der unternehmensübergreifenden Zusammenarbeit via Webportal. Dabei soll den Benutzern eine immer größer werdende Anzahl an externen Anwendungen von verschiedenen Institutionen zur Verfügung gestellt werden. Da es sich dabei um personenbezogene Daten handelt, ist eine entsprechende Sicherheitsinfrastruktur erforderlich. Dazu gehört ein Berechtigungskonzept, welches den hausinternen und den externen Anforderungen entspricht. Es existieren verschiedene Berechtigungsparameter für Mitarbeiter mit unterschiedlichen Rollen. Deren Verwaltung hat mit höchster Sorgfalt zu erfolgen. Zudem ist es wichtig, dass alle vom Benutzer getätigten Aktivitäten in einer Applikation nachvollziehbar dokumentiert werden. Nicht zuletzt muss auf die Benutzerfreundlichkeit Bedacht genommen werden, da die Bedienung der Anwendungen verschieden ist. Die Projektumsetzung (Anm.: Die Ausführungen werden auf einem gewissen Abstrahierungslevel gehalten, da einerseits eine Detailtiefe nur bedingt notwendig ist, zum anderen, um vertrauliche Daten wie Konfigurationen oder Sicherheitseinstellungen des Arbeitgebers des Autors nicht preiszugeben.) erfolgt im Wesentlichen in zwei Schritten: Als Basis dient ein derzeit im Aufbau befindliches Portalverbundsystem, das den sicheren Austausch von Daten und Berechtigungen zwischen zwei oder mehreren Organisationen ermöglicht. Auf dieser Grundlage sollen Überlegungen angestellt werden, wie durch Funktionserweiterungen ein holistisches Identitätsmanagementsystem entstehen kann. Bestrebung ist, ein System zu skizzieren, dass neben dem Nutzen für Mitarbeiter und Unternehmen vor allem den Aspekt der informationellen Selbstbestimmung für den Anwender in den Vordergrund stellt. Sämtliche Ausführungen werden aus informationssicherheitstechnischer Sicht begleitet.

3.2 DEFINITION IDENTITÄTSMANAGEMENT

„*Identitätsmanagement ist etwas ganz Alltägliches in unserer Gesellschaft. Es bedeutet, dass jede Person sich in den ständig wechselnden Kontexten ihres Lebens im Großen und Ganzen bewusst ist und wählen kann, was sie jeweils ihren Kommunikationspartnern über sich offenbart und in welcher Rolle sie auftritt. Diese informationelle Selbstbestimmung wird im Privatleben ganz natürlich wahrgenommen. Dabei ist der echte Name eines Menschen oft gar nicht so wichtig. Beispielsweise kann eine Person unter ihren Sportfreunden lediglich unter einem Spitznamen bekannt sein. Verschiedene Leute haben also einen ganz unterschiedlichen Blick auf die jeweilige Identität einer Person, die ihrerseits intuitiv die Informationen über sich selbst im normalen Miteinander „verwaltet" und damit die Bilder, die sich andere von ihr machen, beeinflussen kann*." [Köhntopp, 2000]

Was die Menschen bei persönlichen Kontakten gewohnt sind, kann im digitalen Bereich anders sein. Das begründet sich dadurch, dass aufgrund des fehlenden *Face to Face*-Kontakts nicht sichergestellt ist, wer der Kommunikationspartner ist. Zudem ist der Kommunikationskanal zum Partner

grundsätzlich nicht abgesichert. Durch das Internet hat der bewusste Umgang mit der eigenen Identität eine nie zuvor gekannte Bedeutung erreicht.

Eine vereinheitlichte, allgemein akzeptierte Definition und ein genau definierter Funktionsumfang von Identitätsmanagement existieren nicht. In den folgenden Ausführungen sollen daher die wesentlichen Kriterien und Eckpunkte von Identitätsmanagement – vor allem für das unternehmerische Umfeld – wiedergegeben werden.

Als Identitätsmanagement wird der zielgerichtete und bewusste Umgang mit Identitäten (siehe *2.2.1 Digitale Identität*) bezeichnet. Zum Identitätsmanagement zählen die sichere Administration von Identitäten, der Identifikationsprozess eines Subjekts/Objekts (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*) und die Information, die mit der Identifikation eines Subjekts/Objekts innerhalb eines bestimmten Kontexts verbunden ist. Subjekte/Objekte können mehrere Identitäten haben, die in verschiedenen Kontexten verwendet werden können.

Eine Identity Management-Lösung besteht aus unterschiedlichen, webbasierenden, mandantenfähigen Modulen und Komponenten für verschiedene Funktionen. IMS zielen darauf ab, eine einheitliche, systemübergreifende Plattform für die Verwaltung von Benutzern und Berechtigungen zu schaffen[640]. Eine zentrale Rolle spielen Verzeichnisdienste (siehe *3.4.1.1 Verzeichnisdienst*). In diesen bzw. in einem Überverzeichnis, dem sogenannten Metadirectory (siehe *3.4.1.2 Metadirectory und Virtuelles Verzeichnis*), werden die personenbezogenen Daten von Mitarbeitern (Name, Mailadresse, Telefonnummer usw.) verwaltet. Das Verzeichnis bildet die zentrale Drehscheibe für die Verteilung und Synchronisation der Benutzerdaten und -rechte (siehe *3.4.2.4 Provisioning*). Föderiertes Identitätsmanagement (siehe *3.2.3 Identitätsföderation und -kontrolle*), Passwortsynchronisierung (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) und User Self Services (siehe *3.4.2.5 Self Service*) sind weitere elementare Funktionen.

In Folge der Entwicklung von Intranets, Extranets und unternehmensweiten Internetzugängen wird die Sicherheit des Zugriffes auf Daten ein immer wichtiger werdendes Anliegen. Zugang unterschiedlicher Benutzer von mehreren Orten, unter Verwendung unterschiedlichster Devices wird die Norm werden und muss technisch realisiert werden (siehe *1.5.1 Arbeitsplatz der Zukunft, 1.5.2 Ubiquitäres Computing*). Ein Identitätsmanagementsystem ermöglicht es Benutzern, Art und Umfang der Herausgabe personenbezogener Daten zu kontrollieren (siehe *2.3.2.1 Informationelle Selbstbestimmung*). Dadurch stellt es einen wichtigen Baustein zur Erfüllung von Datenschutzanforderungen und mehrseitiger Sicherheit (siehe *1.8 Unternehmenssicherheit, 2.1 Problemstellung und Herausforderung*) dar.

[640] Vgl. http://www.computacenter.de/technologien/web_technology/ims.shtm [8. November 2007]

3.2.1 ANFORDERUNGEN AN IDENTITÄTSMANAGEMENTSYSTEME UND DATENSCHUTZ

Die Basis für den Einsatz eines Identitätsmanagementsystems ist das Funktionieren von Informationssicherheit in einer Organisation (siehe *1.8 Unternehmenssicherheit*). Identitätsmanagementsysteme können – je nach Verwendung – unterschiedliche Funktionalitäten haben und viele Facetten aufweisen. Für den Einsatz eines IMS ist es daher wichtig, dass es in einem größeren Kontext betrachtet wird, um zum einen flexibel integrier- und verwendbar zu sein und zum anderen nicht in seiner Datenschutzfunktionalität umgangen werden zu können. Grundlegendes zum Datenschutz – insbesondere im Zusammenhang mit Identitätsmanagement – wurde bereits in den Kapiteln *1.7.3.1 Datenschutz, 1.7.3.2 Arbeitsrechtliche Grundlagen der Informationssicherheit in Unternehmen, 2.3.2.2 Zusammenhang von Identitätsmanagement und Datenschutz* ausgeführt. „*Identitätsmanagement in Nutzerhand ist der Datenschutz der Zukunft*“, formuliert *Marit Hansen,* die Leiterin des Bereichs Zukunftstechnologien beim *Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein* (kurz*: ULD*)[641].

Eine wesentliche Bedingung für einen umfassenden Einsatz bildet die Nutzung von Standards und verbreiteten Technologien.

Frei nach Köhntopp [Köhntopp, 2000] werden folgende globale Anforderungen an ein Identitätsmanagementsystem formuliert:

- Möglichst hohes Niveau an Datenschutz für alle beteiligten Komponenten: Da ein Identitätsmanagementsystem personenbezogene Daten verwaltet, ist Vertrauenswürdigkeit von großer Bedeutung. Daher sollte die gesamte Identitätsmanagement-Infrastruktur einen möglichst hohen Grad an Datenschutz und Datensicherheit (siehe *1.7 Schutzmaßnahmen und Gegenstrategien*) aufweisen. Umfassende Transparenz für den Benutzer im Aufbau der Systeme und in ihrer Bedienung erhöht die Vertrauenswürdigkeit. Biometrische Verfahren (siehe *1.7.2.3 Biometrie*) können zum Einsatz kommen, um die Personenbindung des IMS an die Benutzer zu gewährleisten. Ein integraler Bestandteil eines Identitätsmanagementsystems ist die Kommunikation mit anderen Teilnehmern (z. B.: für Transaktionen im E-Commerce oder E-Government). Ist diese nicht abgesichert oder fallen dabei neben den vom IMS verwalteten personenbezogenen Daten weitere identifizierende Informationen an, kann das IMS umgangen werden. Die zugrundeliegenden Kommunikationsnetze müssen eine Anonymität (siehe *2.2.3 Anonymität*) der Benutzer gewährleisten, die gegen die Betreiber der Systeme oder unerwünschte Beobachter durchgesetzt werden kann. Auf den höheren Schichten der Services und Anwendungen bestehen alle Freiheitsgrade in der Realisierung, in der je nach Anwendungskontext eine möglichst weitreichende Anonymität, verschiedene Arten von Pseudonymität (siehe *2.2.2*

[641] http://www.uld-i.de/themen/idm/ [13. November 2007]

Pseudonymität) oder die Information über die Identität (siehe *2.2.1 Digitale Identität*) der Teilnehmer erforderlich oder sinnvoll sein können.

- Stärkung des Benutzers und seiner Selbstdatenschutzkompetenz (siehe *2.4.2.3 Selbstdatenschutz*): Durch ein Identitätsmanagementsystem soll der Benutzer befähigt werden, seine informationelle Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung*) besser ausüben zu können. Aus diesem Grund sind komfortable Bedieneroberflächen (siehe *3.4.4.2.9 User Interface*) essentiell, die dem User ermöglichen, seine verschiedenen Pseudonyme oder Rollen (siehe *3.6.3 Von der Identität* zur Rolle) zu verwalten. Bedienfehler (siehe *1.3.3 Menschliches Versagen*) können dazu führen, dass Dritten versehentlich Daten über den Benutzer offenbart oder dass Pseudonyme versehentlich aufgedeckt werden. Informationen über die Konfiguration des IMS können ebenso aussagekräftig sein wie personenbezogene Daten und sollten daher gegen unbefugte Zugriffe geschützt werden. Der Benutzer sollte die Möglichkeit haben, die über das IMS abgewickelte Kommunikation zu protokollieren, um bei Bedarf nachvollziehen zu können, wer welche Daten über ihn gesammelt hat. Des Weiteren sollten Benutzerkontrollfunktionen (z. B.: Einwilligung, Korrektur) in ein IMS integriert werden.
- Erforderlichkeitsprinzip, Grundsatz der Datenvermeidung (siehe *2.4.2.2 Datensparsamkeit*) und die Repräsentation von Pseudonymen und Rollen mit verschiedenen Eigenschaften: Für die Realisierung von Pseudonymen lassen sich kryptographische Methoden wie digitale Signaturen (siehe *1.7.2.1.7 Elektronische Signatur*) verwenden. Verschiedene Arten von Treuhändern sind denkbar, um zum Beispiel beim Werteaustausch zu unterstützen oder in Haftungsfragen einzuspringen, so dass eine faire Abwicklung von Transaktionen gegeben ist, ohne dass in jedem Fall die Identität der Beteiligten offengelegt werden muss. In jedem Anwendungszusammenhang ist zunächst nach dem Erforderlichkeitsprinzip eine Analyse zu machen, wer welche personenbezogenen Informationen benötigt. In Überprüfung der Verfahren in Verwaltung und Unternehmen unter dem Gesichtspunkt einer möglichen Datenvermeidung fällt auf, dass Informationen wie Name oft nicht erforderlich sind. Wenn bestimmte Eigenschaften (z. B.: dass für erbrachte Leistungen tatsächlich bezahlt wird, dass ein Produkt an eine Adresse geliefert werden kann) zugesichert werden können, kann auf diese Daten verzichtet werden. Begleitend dazu sollten bisherige Rechtsnormen, die von der vollständigen Identität (Name, Adresse, Geburtsort etc.) ausgehen, neu überdacht werden.
- Einzelnutzungsnachweis: Die Kommerzialisierung personenbezogener Daten wird als Bedrohung für den Datenschutz (siehe *2.3.3 Technologien und Entwicklungen mit Einfluss auf Privacy*) empfunden. Die Kommerzialisierung weniger sensitiver personenbezogener Daten hingegen kann als Chance für mehr Transparenz für die Betroffenen genutzt werden. Ähnlich wie es bei der Telekommunikation einen Einzelverbindungsnachweis gibt, der mitteilt, wofür der Kunde

bezahlen muss, sollte ein Einzelnutzungsnachweis dem Betroffenen detailliert jede Nutzung seiner personenbezogenen Daten mitteilen.

Eine interdisziplinäre Forschung für die Konzeption, das Design und die Implementierung von Identitätsmanagementsystemen ist notwendig (siehe *3.3.2 Forschungsprojekte in der Europäischen Union*). Sie sollte eine Rückkoppelung zwischen Recht und Technik berücksichtigen, um sowohl rechtliche Anforderungen technisch umzusetzen als auch technische Ergebnisse bei der Interpretation geltenden Rechts und der Rechtsfortbildung einfließen zu lassen. Dies wird ein wichtiger Beitrag für den Diskussionsprozess sein, wie das Recht auf informationelle Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung, 3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*) in den nächsten Jahren umgesetzt werden soll.
Nach Wörndl [Wörndl, 2002, S 25ff] lassen sich die Anforderungen an ein Identitätsmanagementsystem von drei Ausgangspunkten ableiten:

- Gesetzliche Rahmenbedingungen (siehe *1.7.3.2 Arbeitsrechtliche Grundlagen der Informationssicherheit in Unternehmen, 2.3.2.2 Zusammenhang von Identitätsmanagement und Datenschutz*).
- Notwendigkeit eines Zugriffskontrollsystems (siehe *3.5.2.1 Gesetze, Regulative, Compliance*).
- Schutzziele mehrseitiger Sicherheit (siehe *2.1 Problemstellung und Herausforderung*).

Dem Benutzer müssen demnach Mechanismen zur Verfügung gestellt werden, mit denen er die Hoheit über seine Identität inne hat. Folgende konkrete Anforderungen können dabei festgehalten werden:

- Absicherungsziele (Integrität, Verbindlichkeit, Zurechenbarkeit):
  - Speicherung des Profils unter der Kontrolle des Benutzers.
  - Regelung der Weitergabe von Daten.
  - Möglichkeit, Zugriffsrechte zeitlich zu beschränken und wieder zurückziehen zu können.
  - Entscheidungsmöglichkeit beim Benutzer bezüglich der Herausgabe von Daten.
  - Möglichkeiten der Zurechenbarkeit und Unabstreitbarkeit (z. B.: Nachweis einer Bestellung).
  - Einhaltung gesetzlicher Rahmenbedingungen.
  - Verantwortlichkeit derjenigen Organisation, die personenbezogene Daten speichert.
  - Möglichkeit der Durchsetzung der erläuterten Prinzipien gegenüber Organisationen, die personenbezogene Daten verarbeiten.
  - Schutz der Daten gegen Verfälschung insbesondere bei Übertragung in offenen Netzen.
  - Möglichkeit der Signierung eines Zugriffsrechts.

- Autorisierungsziele (Bereitstellung einer geeigneten Zugriffskontrolle):
  - Wählbare Granularität (z. B.: Rechte für einzelne Profilattribute).

- Kontrolle der Weitergabe von Daten.
- Flexibilität bei der Zugriffskontrolle (z. B.: durch Aushandlung).
- Möglichkeit, Optionen wie „Zugriff nur bei gesicherter Übertragung“ zu realisieren.
- Möglichkeiten zur zeitlichen Begrenzung und Zurückziehbarkeit von Rechten.
- Möglichkeiten, Profile über Unternehmensgrenzen hinweg zu synchronisieren, um den Überblick über die gespeicherten Daten für Benutzer zu verbessern.
- Möglichkeit, Zugriffsregeln zu formulieren.
- Geeignete Benutzerschnittstellen zur Administration von Rechten.

- Identitätsziele (Anonymität, Pseudonymität):
  - Überprüfung der Identität der Kommunikationspartner.
  - Möglichkeit für Benutzer, anonym zu kommunizieren.
  - Möglichkeit der Verwendung eines Pseudonyms bzw. verschiedener Stufen von Pseudonymität.
  - Unverkettbarkeit von Pseudonymen bzw. Verkettbarkeit nur unter der Kontrolle des Benutzers.

- Transparenzziele (Überwachungs- und Kontrollfunktionen für Benutzer):
  - Möglichkeit, vergebene Zugriffsrechte jederzeit überprüfen zu können.
  - Möglichkeit für Benutzer, Zugriffe überwachen zu können, Protokollierung aller Zugriffe.
  - Benutzerschnittstellen zur Festlegung von Rechten.
  - Vertrauenswürdiges User Interface.

- Vertraulichkeitsziele (Vertraulichkeit, Verdecktheit, Unbeobachtbarkeit):
  - Möglichkeit zur Festlegung von Zugriffsrechten für Benutzerprofil-Attribute.
  - Flexibilität bei der Zugriffskontrolle (z. B.: durch Regeln).
  - Realisierung von Unbeobachtbarkeit und Verdecktheit in den Kommunikationsbeziehungen.
  - Möglichkeit, Daten über eine gesicherte Verbindung zu übertragen.
  - Datensparsamkeit, Datenvermeidung bzw. Erforderlichkeit eines Zugriffs.
  - Einhaltung von technischen und organisatorischen Richtlinien zur Sicherheit bei der Datenspeicherung und -verarbeitung.

3.2.2 BENUTZER-ZENTRIERTE IDENTITÄT

Unter *User Centric Identity* (deutsch: *Benutzer-zentrierte Identität* oder: *Identity 2.0*) wird die nächste Generation des Identitätsmanagements verstanden. Dabei stehen die neuen Möglichkeiten mit Web 2.0 (siehe *3.5.4.3.5 Künftige Anforderungen an die IT: Web 2.0*), Federation (siehe *3.2.3*

Identitätsföderation und -kontrolle), CardSpace (siehe *3.3.1.2 Microsoft CardSpace*), OpenID (siehe *3.3.1.3.4 OpenID*) und die digitale Selbstbestimmung eines Anwenders (siehe *2.3.2.1 Informationelle Selbstbestimmung*) im Vordergrund. Der Benutzer rückt in den Mittelpunkt, weil er die Kontrolle über seine Identitätsinformationen erhält[642] (siehe *3.2.3 Identitätsföderation und -kontrolle: user-controlled identity pillar*).

Die bisherigen Ausführungen über die Anforderungen an Identitätsmanagementsysteme (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme*) werden durch *Kim Cameron's Seven Laws of Identity*[643] bestätigt beziehungsweise verstärkt:

1. *User Control and Consent*: Identitätsmanagementsysteme dürfen Informationen, die den Benutzer identifizieren, nur mit dessen Zustimmung weitergeben. Die Anwender bestimmen den Erfolg eines IMS. Ein solches System muss daher einerseits einfach zu bedienen und bequem zu nutzen sein und andererseits Vertrauen schaffen. Dies gilt für jeden denkbaren Kontext, sei es innerhalb eines Unternehmens oder im Internet.
2. *Minimal Disclosure for a Constrained Use*: Minimale Informationspreisgabe für einen konkreten Anwendungsfall. IMS müssen von der Annahme ausgehen, dass ein Sicherheitsvorfall nicht die Ausnahme ist, sondern jederzeit eintreten kann. Deshalb darf immer nur so viel Information bevorratet und herausgegeben werden, wie es unbedingt erforderlich ist. Wenn ein System darauf ausgerichtet ist, möglichst wenig Informationen vorzuenthalten, macht es sich weniger attraktiv für die Angriffe Unberechtigter. Von besonderer Bedeutung ist in diesem Zusammenhang die Frage, welche Informationen gespeichert werden sollen. Daten sollten deshalb so spezifisch wie möglich gespeichert und weitergegeben werden.
3. *Justifiable Parties*: Identitätsmanagementsysteme müssen so konzipiert werden, dass die Preisgabe identifizierender Informationen nur an berechtigte Parteien erfolgt. Zudem hat ein IMS nicht nur sicherzustellen, dass sich ein Anwender gegenüber einem Serviceanbieter ausweist, sondern auch alle beteiligten Parteien sich gegenseitig ausweisen müssen.
4. *Directed Identity*: Die digitale Identität einer Person darf immer nur zielgerichtet gegenüber einer oder mehreren anderen Identitäten bekannt gegeben werden, nicht gegenüber der Allgemeinheit. Sie ist also unidirektional und steht nicht jedermann zur Verfügung. Im Gegensatz dazu gibt das digitale Zertifikat eines Webservers dessen Identität all denen bekannt, die die Services des Webservers aufrufen. Diese öffentliche Identität ist omnidirektional und übermittelt ihre Identitätsinformationen an alle, die in den Sendebereich der Identität gelangen. Es gibt zahlreiche

[642] Vgl. http://www.iam-wiki.org/Identity_2.0?highlight=%28identity%29%7C%282.0%29 [12. November 2007]

[643] Kim Cameron ist bei Microsoft Vordenker hinsichtlich Identitätsmanagement und publiziert die Webseite http://www.identityblog.com/ [12. November 2007]; Vgl. http://www.microsoft.com/germany/technet/technetmag/issues/2006/07/identityaccessmgmt_infocard.mspx [12. November 2007]

Techniken und Technologien, die gegen das Prinzip der Direktionalität arbeiten. Erstes Beispiel Bluetooth (siehe *1.5.3 Personal Area Network*): Wird diese drahtlose Übertragungstechnik an einem mobilen Gerät aktiviert, dann verbreitet das Gerät innerhalb der technischen Reichweite Identitätsinformationen an alle anderen Bluetooth-Geräte. Zweites Beispiel RFID (siehe *2.3.3.3 RFID*): Während die omnidirektionale Abrufbarkeit einer Identitätsinformation für ein Produkt (z. B.: Käseverpackung) sinnvoll sein kann, verbietet sich der Einsatz dieser Technologie im Reisepass.

5. *Pluralism of Operators and Technologies*: Ein universelles Identitätsmanagementsystem muss mit den relevanten Identitätstechnologien und verschiedenen Identity Providern interoperabel sein. Ein IMS muss kontext-spezifisch differenzieren können und berücksichtigen, dass der Anwender in zahlreichen Kontexten (Bürger, Kunde, Mitarbeiter, Forumsteilnehmer etc.) handelt.
6. *Human Integration*: Identitätsmanagementsysteme müssen den Benutzer als integralen Teil des Systems definieren, um ihn gegen Missbräuche schützen zu können. Dabei müssen eindeutige, unmissverständliche Mensch-Maschine-Kommunikationsmechanismen bei gleichzeitigem Schutz gegen Identity-Attacken (siehe *1.3.5.3 Identitätsdiebstahl*) verwendet werden.
7. *Consistent Experience Across Contexts*: Ein universelles Identitätsmanagementsystem sollte die Möglichkeit bieten, zwischen unterschiedlichen Kontexten differenzieren zu können. Zudem sollte es dem Anwender eine durchgängig einfache Interaktion im Umgang mit seinen Identitäten in den unterschiedlichen Kontexten zur Verfügung stellen, beispielsweise indem er sich kontext-spezifische Basisidentitäten definieren kann.

3.2.3 IDENTITÄTSFÖDERATION UND -KONTROLLE

Unternehmen sehen sich zunehmend mehr dazu gezwungen, aus Effizienz- (siehe *3.5.2 Anforderungen, Nutzen und treibende Faktoren* aus Unternehmenssicht) und Wettbewerbsgründen firmenübergreifende Wertschöpfungsketten zu etablieren. Das effektive Koordinieren und Integrieren von Geschäftsprozessen mit Kunden und Partnern stellt eine komplexe Herausforderung für die Unternehmen dar. Dabei kommt es auf die Koordination, die Integration und den sicheren Betrieb aller unterstützenden IT-Systeme (z. B.: Legacy-Applikationen, Web Services) an. Bedingung ist, dass die Rechte der diversen Benutzergruppen aller Unternehmen und ihre Zugriffe auf die IT-Systeme exakt definiert und kontrolliert werden.

Unter Identitätsföderation (engl. *Identity Federation*) wird die Idee bzw. die Architektur verstanden, wie Unternehmen mit Hilfe von digitalen Identitäten Information untereinander austauschen und sicheren Zugriff auf die jeweiligen Partnersysteme gewähren können, ohne dabei die Eigenständigkeit zu verlieren[644].

[644] Vgl. http://www.iam-wiki.org/Identity_Federation [20. Oktober 2007]

Eine föderierte Identität erstreckt sich über mehr als ein System, die Identitätsdaten werden in verschiedenen Systemen gehalten. Wenn beispielsweise Unternehmen A sein Bürozubehör bei Unternehmen B bestellt, dann sind die bestellungsberechtigten Personen und deren Rollen (siehe *3.6.3 Von der Identität zur Rolle*) in Unternehmen A definiert. In Unternehmen B ist festgelegt, welche Bestellungen von welcher Rolle ausgeführt werden dürfen. Für die Abwicklung des Bestellprozesses müssen die Identitätsdaten beider Unternehmen zusammengefasst werden. Der Datenaustausch erfolgt mit Techniken und Standards wie SAML (siehe *3.4.4.2.6 SAML*). Für das Funktionieren von Identity Federation bedarf es noch weiterer Technologien. *Browser-basierte Föderation* bedeutet, dass ein beim Unternehmen A registrierter Benutzer über einen Link ohne erneute Authentifizierung direkt auf den geschützten Bereich des Partnerunternehmens B gelangt. Die Authentifizierung kann dabei auf Basis von Rollen erfolgen. In einer *Dokumenten-basierten Föderation* hingegen schickt der User A ein XML-Dokument in einem SOAP-Umschlag (siehe *3.4.4.2.3 SOAP*) an den Web Service (siehe *3.4.4.2 Web Services*) des Partners. Das Unternehmen authentifiziert diesen und leitet die Anfrage entsprechend der Berechtigungen an andere Web Services innerhalb der Föderation weiter. Neben Mitarbeiterdaten lassen sich auf diese Weise Applikationen oder Web Services verknüpfen, so dass diese innerhalb des Netzwerkes vertrauenswürdiger Partner auf IT-Ressourcen zugreifen können. Das ist eine der entscheidenden Voraussetzungen beim Aufbau Service-orientierter Architekturen (siehe *3.4.4.2.8 SOA*). Zudem können Rechte in föderalen Umgebungen delegiert werden, so dass zum Beispiel Geschäftsprozesse, die über einen Zwischenhändler (engl. *Intermediaries*) abgewickelt werden, effizient und sicher realisiert werden können. Der Schutz von Web Services (siehe *3.4.4.2.5 WS-Security*) ist deshalb entscheidend für den Aufbau von SOA-Infrastrukturen, weil diese vom Einbeziehen diverser Zwischenstationen gekennzeichnet sind. Zudem beantwortet Identity Federation die sicherheitsrelevanten Fragen der Autorisierung, Authentifizierung, Integrität oder Vertraulichkeit bei der mehrstufigen Web Services-Bearbeitung. Der SOA-Idee folgend lassen sich Sicherheitsservices dabei zum Teil durch zentrale Server-Plattformen betreiben und können ihrerseits als Dienst angefordert werden[645].

Der Vorteil des föderierten Ansatzes für das Identitätsmanagement besteht darin, dass die Daten an ihrem eigentlichen Speicherort verbleiben können. Anstatt zentrale Datenbanken aufbauen zu müssen, sorgt Identity Federation für einheitliche Standards zum Informationsaustausch. Dazu werden sogenannte *Circles of Trust* geschaffen, wo gemeinsame organisatorische Regeln und technische Standards entwickelt werden. In der Praxis bedeutet das, dass ein Benutzer, der von einer teilnehmenden und als vertrauenswürdig geltenden Stelle identifiziert worden ist, auf Inhalte und Dienstleistungen zugreifen kann, ohne sich jedes Mal neu authentifizieren zu müssen. Die Information darüber, welche Berechtigungen jemand hat, residiert weiterhin in den jeweiligen Systemen der

[645] Vgl. http://www.securitymanager.de/magazin/artikel_1522.html [27. Oktober 2007]

einzelnen Mitglieder. Ein föderales System schafft Transparenz und erfüllt damit die Forderung nach informationeller Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung, 3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*).

Von Identity Federation profitieren daher sowohl die Benutzer als auch die Unternehmen. Die User können sich innerhalb des Verbundes frei bewegen, während die Unternehmen ihre IT-Systeme einem größeren Nutzerkreis zugänglich machen, ohne dass der Administrationsaufwand für das Berechtigungsmanagement wächst.

In den vergangenen Jahren haben sich zwei unterschiedliche Gruppen von technischen Standards für die Bildung von Identity Federations herausgebildet: die *WS-* Standards*[646] von Microsoft und IBM auf der einen Seite, und die *Liberty-Standards* der *Liberty Alliance*[647], der eine große Zahl namhafter Unternehmen angehören, auf der anderen Seite. Inhaltlich unterscheiden sie sich zwar erheblich, im Kern adressieren sie beide das Management digitaler Identitäten über die Anwendungs- und Unternehmensgrenzen hinweg. Zudem zeigen Implementierungen beider Standards mittlerweile, dass auch das jeweils andere Modell adressiert werden kann und damit zunehmend Interoperabilität[648] und Konvergenz[649] entsteht. Deutlich wird das beispielsweise beim *Windows Server 2003 R2*[650] und dessen *Active Directory Federation Services* (kurz: *ADFS*), die auf Browser-basierende Zugriffe ausgerichtet sind.

Die Behörden bedienen sich für *Government to Government* (kurz: *G2G*)- bzw. *Government to Citizen* (kurz: G2C)-Beziehungen zunehmend mehr dieser Standards. Aus diesem Grund hat die Liberty Alliance im August 2006 eine internationale Gruppe innerhalb der Organisation ins Leben gerufen, die die Regierungen bestmöglich unterstützen soll[651]: „*The E-Government Group will focus on business, technical and policy issues, with an emphasis on privacy and security issues*. *The alliance has supported a range of protocols and standards that companies can implement to allow users to move easily from one Web site to another without having to key in a login and password again, among other functions. Governments have considerable influence as role models for the consumer sector, and there is scope for sharing identity networks with the private sector.*"

Die Kontrolle über die digitale Identität kann nach *Ernst*[652] in Unternehmens- und Microsofthoheit bzw. in Benutzer-Hand liegen:

---

[646] http://www.ws-standards.com/ [28. Feber 2008]
[647] http://www.projectliberty.org/ [28. Feber 2008]
[648] Vgl. http://www.projectliberty.org/liberty/liberty_interoperable [27. Oktober 2007]; http://utilitycomputing.itworld.com/4603/070110libertyalliance/page_1.html [27. Oktober 2007]
[649] Vgl. http://www.kuppingercole.de/articles/ms-sun,19,5,05 [27. Oktober 2007]
[650] http://www.microsoft.com/germany/windowsserver2003/default.mspx [26. Oktober 2007]
[651] Vgl. http://www.infoworld.com/article/06/08/17/HNegovernmentgroup_1.html?IDENTITY%20MANAGEMENT [27. Oktober 2007]
[652] Vgl. http://netmesh.info/jernst/Digital_Identity/three-standards.html [27. Oktober 2007]

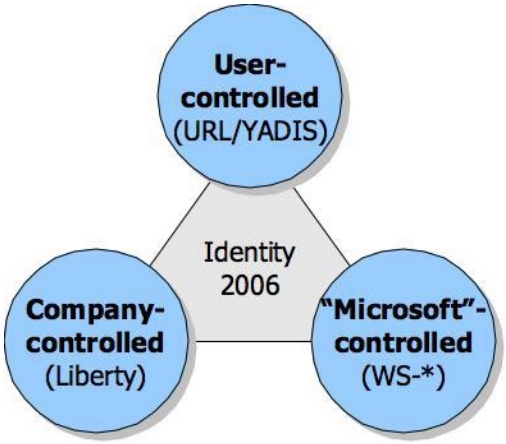


Abbildung 44: *-controlled identity pillars

„*The **company-controlled identity pillar**, which is rooted in the Liberty standards. This pillar is ready-made for corporate adoption: identity is „given" to the individual (e.g. the employer) by the corporation, and it is the corporation that decides which identity attributes are managed and shared with whom. Even if the corporation gives the individual many choices, it is ultimately the corporation who decides whether or not to give those choices to the individual.*

*The **„Microsoft"-controlled identity pillar**. On one hand, Microsoft of course does not control WS-* (at least not by itself) which is a major component of this pillar. On the other hand, the adoption of this pillar will be driven by Windows Vista and CardSpace adoption and the particular subset of WS-* that Microsoft has chosen to support.*

*The **user-controlled identity pillar**, where the individual is fully in control, over identity providers, over attributes, over whether or not to have an identity or how many, over the software to run, and over the feature set associated with their identity. It's most visible sign is the use of URLs to point to people, just like we use URLs to point to companies or documents. This pillar is rapidly coming together in the YADIS community* (siehe *3.3.1.3.5 Yadis*), *which essentially facilitates an open marketplace of interoperable identity-related features from which the individual may pick as many or as few as they like.*"

3.2.3.1 Vertrauensstellung

Identity Federation ist ein elementares Thema von Identitätsmanagement. Als Voraussetzung dafür müssen Vertrauensstellungen geschaffen werden (siehe *3.5.3 Praxisbeispiel: Identitätsmanagement für Behörden in Form des Portalverbunds*). Da das Föderationskonzept impliziert, dass ein Partner – zumindest teilweise – von den Informationssicherheitssystemen und Praktiken eines anderen abhängig ist, müssen alle diesbezüglichen Vereinbarungen die Anforderungen, Erwartungen, Handhabung der Haftpflicht, Festlegung der Service-Levels, Maßnahmen im Falle einer tatsächlichen

Informationssicherheitsverletzung und Kontrollmöglichkeiten, die dem Partner bei der Ausgabe von Benutzerzugangsdaten zur Verfügung stehen, definiert werden. Zudem sind Überlegungen über rechtliche und vertragliche Aspekte des Vertrauens, den Umgang mit Problemfällen (Eskalationsmanagement), behördliche Auflagen, die technische Infrastruktur und die Kostenaufteilung anzustellen [CA, 2005-2, S 6ff].

Während die meisten Einsatzbereiche der Identity Federation bislang auf eine überschaubare Anzahl an Teilnehmern beschränkt waren, steigt die Zahl der aktiv teilnehmenden Partner stetig. Wenn beispielsweise von zehn größeren Herstellern und 500 Zulieferern in einer Branche ausgegangen wird und jeder Hersteller mit der Hälfte der Zulieferer Federation-Beziehungen aufbaut und vice versa, dann bleiben für jeden Hersteller 250 Zulieferer und für jeden Zulieferer fünf Hersteller. Diese 250 Vertrauensstellungen gilt es zu definieren und zu pflegen.

Neben dem manuellen Management von Federation-Beziehungen gibt es mehrere Ansätze zur Lösung dieser Herausforderung. Ein Weg könnte die Nutzung der Idee für das User centric Identity Management (siehe *3.2.2 Benutzer-zentrierte Identität*) sein. Anstelle der Realisierung eines relativ komplexen Verbundes von Vertrauensstellungen – Circle of Trust – könnte jeder Service Provider einem Identitätsanbieter oder dem Benutzer selbst, beispielsweise bei einer selbst ausgestellten Karte (siehe *3.3.1.2 Microsoft CardSpace*), vertrauen.

Der zweite Ansatz ist der eines sogenannten *Trust Brokers*. In diesem Fall übernimmt ein Unternehmen das zentrale Management der Identitäten. Jeder der Zulieferer und Hersteller müsste nur noch genau eine Vertrauensstellung definieren.

Die verschiedenen Lösungsansätze machen die Dynamik des Federation-Marktes deutlich, alle Ansätze haben ihre Berechtigung – auch, weil sie sich nicht ausschließen, sondern unterschiedliche Teilbereiche der Herausforderung *Trust Management* adressieren[653].

3.3 IDENTITÄTSMANAGEMENT-KONZEPTE, INITIATIVEN UND FORSCHUNG

Im Folgenden soll auf die konzeptionellen Ansätze von Identitätsmanagement, die Idee des föderalen Ansatzes und die diesbezügliche Forschungsarbeit in Europa eingegangen werden.

3.3.1 KONZEPTE UND INITIATIVEN

Bereits 1985 hat *Chaum* [Chaum, 1985] eine Welt skizziert, in der für jeden Menschen ein persönlicher *Card-Computer* alle Bezahlvorgänge und anderen Transaktionen erledigt und dabei Datenschutz gewährleistet. In den grundlegenden Ausführungen werden die dafür notwendigen technischen Bausteine und mögliche Lösungen vorgestellt. Obwohl seitdem vielfach Überlegungen

[653] Vgl. https://www.kuppingercole.de/articles/federation_trust_mgmt [12. November 2007]

angestellt und Vorschläge ausgearbeitet wurden, sind noch nicht alle von Chaums Ideen umgesetzt respektive allgemein verfügbar gemacht worden.

In den neunziger Jahren wurden einige Vorstellungen von Chaum im Konzept des *Identity Protectors* von *Borking* [Borking, 1997, S 654ff] in die Realität umgesetzt, indem die persönlichen Daten des Benutzers anwendungsbezogen geschützt werden können. Der Identity Protector kann unter anderem die Identität kontrolliert freigeben oder Pseudonyme (siehe *2.2.2 Pseudonymität*) generieren.

Im Bereich der Telefonie wurde ein System für Identitätsmanagement konzipiert und implementiert. Integriert in einen mobilen Sicherheitsmanager, verwaltet das System die verschiedenen möglichen (Pseudo-) Identitäten (siehe *2.2.1 Digitale Identität*) einer Person auf einem *Personal Digital Assistant* (kurz: *PDA*) und unterstützt die Benutzer bei der Auswahl von Identitäten oder Pseudonymen für verschiedene Zwecke.

Mit der Entwicklung zum Web 2.0 (siehe *1.1 Problemstellung und Herausforderung*) und der damit verbundenen Abbildung von sozialen Beziehungen ist das Interesse am Umgang mit Identitätsdaten gestiegen (Anm.: Für den Autor ergibt das eine paradoxe Situation. Zum einen geben Menschen auf diversen Seiten persönliche Daten preis, auf der anderen Seite wollen sie ihre Identität geschützt wissen.). Ziel der Bestrebungen ist es, hinreichende Sicherheit über die Identität des Online-Kommunikationspartners bei gleichzeitig sparsamem Umgang mit personenbezogenen Daten zu bekommen.

Während für den privaten Web-User eher Lösungen im Open Source-Bereich (*Higgins*[654], *OpenID*[655], etc.) zu finden sind, haben für Unternehmen mehr die Angebote von kommerziellen Herstellern (*CA Identity Manager*[656], *Evidian IAM Suite 8*[657], Microsoft *CardSpace*[658] und Microsoft *Identity Lifecycle Management*[659], *Novell Identity Manager*[660], *Sun Identity Management*[661] etc.) Bedeutung. Eine Übersicht über kommerzielle bzw. frei verfügbare Identitätsmanagementlösungen ist zu finden unter:

http://www.iam-wiki.org/alle_Seiten_in_Kategorie_Hersteller bzw.

http://www.iam-wiki.org/alle_Seiten_in_Kategorie_Opensource.

(Anm.: eine Kategorisierung hinsichtlich der Kontrolle von Identitäten siehe *3.2.3 Identitätsföderation und -kontrolle: Abbildung 44: *-controlled identity pillars*)

Strukturell gibt es zwei Ansätze, Identitäten zu verwalten. Während beim serverbasierten Ansatz die Attribute einer Identität bei einem zentralen Dienst abgelegt werden, verwalten beim clientbasierten Ansatz die Dienstanbieter die Identitätsdaten ihrer Kunden selbst und implementieren ein festgelegtes

[654] http://www.eclipse.org/higgins/index.php [28. Oktober 2007]
[655] http://openid.net/ [28. Oktober 2007]
[656] http://ca.com/us/products/product.aspx?ID=5655 [28. Oktober 2007]
[657] http://www.evidian.com/security/index.htm [28. Oktober 2007]
[658] http://msdn2.microsoft.com/en-us/library/aa480189.aspx [28. Oktober 2007]
[659] http://www.microsoft.com/windowsserver2003/technologies/idm/ilm.mspx [30. Dezember 2007]
[660] http://www.novell.com/products/identitymanager/ [2. November 2007]
[661] http://www.sun.com/software/products/identity/index.jsp [30. Dezember 2007]

Protokoll, um den Austausch der Identitätsdaten zwischen ihren Partnern zu ermöglichen [Rickert, 2004, S 21f].

Im Jahre 1996 wurde von namhaften Unternehmen (CA, Novell, *Oracle*[662], *Ping Identity*[663], *Sun*[664] etc.) unter dem Begriff *Identity Governance Framework*[665] (kurz: *IGF*, auch: *IGF-Standards, Open Source-Framework*) eine Initiative ins Leben gerufen, in welcher die Grundsätze identitätsbasierter Informationen in Unternehmen diskutiert und definiert werden. Seit Feber 2007 werden die Aktivitäten unter der dem *Projekt Liberty* der Liberty Alliance (siehe *3.2.3 Identitätsföderation*) weiter geführt. IGF ist ein programmatisches Rahmenwerk der Industrie, um Organisationen bei der Erfüllung behördlicher Auflagen wie der europäischen Datenschutz-Initiative oder Sarbanes-Oxley (siehe *1.8.4.3.2 Sarbanes Oxley Act*) zu helfen. Das Rahmenwerk etabliert für Unternehmen eine standardisierte Methode, wie Strategien zur Nutzung von persönlichen Informationen entworfen werden können. Sicherheit, Datenschutz und Vertrauenswürdigkeit zwischen Anwendungen und verschiedenen Identitätsquellen spielen dabei eine zentrale Rolle. Eine der Zielsetzungen des IGF ist eine standardisierte Entwicklung mit Multi-Protokoll-Implementierungen. Das bedeutet Unterstützung für SAML (siehe *3.4.4.2.6 SAML*), WS-* und OpenID-Spezifikationen und die Zusammenarbeit mit anderen Identitäts-Initiativen wie dem Higgins-Projekt (siehe *3.3.1.3.1 Higgins-Projekt*).

Im Folgenden sollen ausgewählte kommerzielle und frei verfügbare Lösungen vorgestellt werden.

3.3.1.1 Novell Identity Manager

Novell (Anm.: Wird von Gartner unter „*leaders*“ im „*Magic Quadrant for User Provisioning, 2H07*“[666] eingestuft) wird an dieser Stelle stellvertretend für das breite Angebot an Identitätsmanagement-Lösungen in Unternehmen vorgestellt. So wie Novell bestehen Unternehmenssuiten in der Regel aus mehreren Modulen. Bei der im Sommer 2007 vorgestellten Release 3.5 wird neben der Integration von Informationssicherheitsprodukten vor allem auf Workflow-, Self Service- und Rollenmanagement-Funktionen (siehe *3.4 Komponenten und Funktionen eines Identitätsmanagementsystems*) Wert gelegt.

Bei Workflow profitiert der Identity Manager von der konsequenten Weiterentwicklung des Novell *Designer for Identity Manager*. Dieses Eclipse-basierte Werkzeug wird für die Offline-Konfiguration und für Tests der Infrastruktur verwendet. In der aktuellen Version wurden unter anderem neue, vordefinierte Szenarien für das Deployment definiert, auf deren Basis sich typische Infrastrukturen schneller umsetzen lassen. Zudem wurden die Modellierung von Workflows verbessert und die

[662] http://www.oracle.com/index.html [2. November 2007]
[663] http://www.pingidentity.com/ [2. November 2007]
[664] http://www.sun.com/ [2. November 2007]
[665] http://www.oracle.com/technology/tech/standards/idm/igf/index.html [2. November 2007]; http://www.openliberty.org/wiki/index.php/IGF_Introduction [2. November 2007]
[666] Vgl. http://mediaproducts.gartner.com/reprints/oracle/150475.html [30. Dezember 2007]

Funktionen für das Richtlinien-Management ausgebaut. Eine wesentliche Neuerung sind die erweiterten Web Service-Funktionen (siehe *3.4.4 Portale und Web Services*). Damit können beispielsweise bestehende, externe Beschaffungsworkflows in Provisioning-Prozesse (siehe *3.4.2.4 Provisioning*) integriert werden, aber auch generell komplexere Funktionen realisiert werden.
Grundlegend überarbeitet hat Novell die Self Service-Schnittstellen (siehe *3.4.2.5 Self Service*). Die wesentlich einfacher zu implementierenden und zu nutzenden Self Service-Funktionen sind für Identity Management-Projekte von zentraler Bedeutung. Sie sind die Schnittstelle, die Anwender sehen und die damit über die Akzeptanz von Identity Management-Lösungen entscheiden und darüber, ob sich erhoffte Einsparpotenziale realisieren lassen.
Bei der Integration mit anderen Produkten ist vor allem das Zusammenspiel mit *Sentinel*[667] zu erwähnen. Mit Sentinel lassen sich Überwachungsregeln für Compliance-Standards und interne Regelungen umsetzen. Bei erkannten Sicherheitsproblemen, die aus Verletzungen von in Sentinel definierten Regeln stammen, werden automatisch Aktivitäten angestoßen, die zu einer entsprechenden Konfigurationsänderung über den Identity Manager führen, indem Benutzer beispielsweise aus bestimmten Rollen entfernt werden. Weiters erwähnenswert ist die Integration mit Novell *SecureLogin*, der Enterprise Single-Sign-On-Lösung von Novell. Mit deren Hilfe können Credentials für das Single-Sign-On automatisch aus einem Provisioning-Prozess heraus generiert werden.
Eine wichtige Änderung ist das erweiterte Rollenmanagement (siehe *3.6.3 Von der Identität zur Rolle*). Ein starkes Rollenmanagement ist sowohl für die effiziente Realisierung von Provisioning-Prozessen als auch den Aufbau von Federation-Lösungen unverzichtbar. Die Rollen lassen sich auf unterschiedlichen Ebenen verwalten, sowohl als abstrahierte Business-Rollen als auch als technisch geprägte Rollen. Unterstützt werden erweiterte Reporting-Funktionen und die *Segregation of Duties* (kurz: *SoD*), also die Überprüfung von potenziellen Konflikten zwischen Rollen. Mit SoD kann beispielsweise sichergestellt werden, dass jemand nicht gleichzeitig die Berechtigungen zu Änderungen an wichtigen Daten und zur Kontrolle solcher Änderungen im Rahmen der Revision hat[668].

3.3.1.2 Microsoft CardSpace

CardSpace ist eine Technologie von Microsoft (Anm.: Wird mit Windows *Vista*[669] standardmäßig ausgeliefert), welche eine technologieübergreifende dezentrale Verwaltung kontext-abhängiger digitaler Identitäten ermöglicht. Der Benutzer soll damit bei der Verwaltung und Weitergabe von persönlichen Daten unterstützt werden. CardSpace soll das Einloggen auf Webseiten sicherer gestalten bzw. Single Sign-On (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) ermöglichen.

[667] http://www.novell.com/products/sentinel/?Subject=ISMag [2. November 2007]
[668] Vgl. http://www.tecchannel.de/index.cfm?pid=905&pk=465577 [2. November 2007]
[669] http://www.microsoft.com/germany/windows/products/windowsvista/default.mspx [28. Oktober 2007]

Die Karten selbst enthalten nur Meta-Informationen, die angeben, wie Daten (z. B.: Name, Geburtsdatum, Wohnort, Geschlecht, Telefonnummern, Kreditkartendaten, Führerscheinklassen) über den Benutzer von Identity Providern angefragt werden können. CardSpace soll dafür sorgen, dass nur das Mindestmaß an benötigten sensiblen Daten am Computer gespeichert oder in Transaktionen verwendet wird. Für Online-Zugänge, in denen es nicht erforderlich ist, dass die Informationen über den Benutzer durch eine Autorität bestätigt werden, kann sich der Benutzer selbst Karten ausstellen (engl. s*elf-issued cards*), wobei die Daten auf dem lokalen Rechner abgelegt werden. Auf diese Art und Weise können bestehende Benutzerkonten bei Anbietern, die als Identity Provider fungieren, für die Registrierung und Authentifizierung bei anderen Diensten genutzt werden. Bei der Herausgabe von Informationen vom Identity Provider wird der Benutzer mit einbezogen, womit er die Kontrolle über die weitergegebenen Informationen behält. CardSpace bietet dem Benutzer einen einfachen Weg für Registrations- und Anmeldevorgänge, zudem kann damit auch Phishing (siehe *1.4.1.2 Exkurs: Phishing*) verhindert werden[670].

Eine Empfehlung von Microsoft[671] zur kontextuellen Verwendung von CardSpace sieht folgendermaßen aus: „[…] *die Ansprüche der meisten Benutzer liegen bei mindestens drei Karten. Eine davon wäre eine selbst ausgestellte Anonymuskarte mit oberflächlichen und falschen Angaben. Diese Karte kann bei nicht-vertrauenswürdigen Websites verwendet werden. Die zweite Karte wäre wieder selbst ausgestellt und enthält wahrheitsgemäße persönliche Angaben. Mit dieser wäre eine Identifizierung bei vertrauenswürdigen Websites, die nur selbst ausgestellte Identitäten akzeptieren, möglich. Die dritte Karte wäre von einem anerkannten Identitätsanbieter (z. B.: VeriSign) ausgestellt. Diese Karte wird bei vertrauenswürdigen Websites eingesetzt. Zusätzlich wären einige spezifische Karten ratsam, zum Beispiel eine von der Hausbank ausgestellte Karte, die über den Kreditrahmen Auskunft gibt, oder Bewertungskarten von Unternehmen wie eBay*."

3.3.1.3 Open Source

Microsoft geht in die Offensive (Stand: September 2007) und unterstützt einige Projekte, die eine Entwicklung quelloffener und plattformübergreifender Lösungen für das Identitätsmanagement im Internet zum Ziel haben. Dazu stellt Microsoft seine Spezifikation *Identity Selector Interoperability Profile* (kurz: *ISIP*)[672] unter sein lizenzfreies *Open Specification Promise* (kurz: *OSP*). Entwickler müssen damit keine Lizenzen erwerben und keine späteren rechtlichen Schritte wegen der Nutzung dieser Spezifikation befürchten. Zudem werden Open Source-Projekte gefördert, die CardSpace für

[670] Vgl. http://www.iam-wiki.org/CardSpace?highlight=%28cardspace%29 [28. Oktober 2007]; http://cardspace.netfx3.com/ [28. Oktober 2007]
[671] Vgl. http://www.microsoft.com/germany/technet/technetmag/issues/2006/07/identityaccessmgmt_infocard.mspx [28. Oktober 2007]
[672] ISIP dient dem Austausch von Identitätsprofilen.

verschiedene Plattformen implementieren sollen, so etwa Java, *Apache Tomcat*[673] und *IBM Websphere*[674]. Schließlich soll die Synchronisation von Identitätsprofilen zwischen Microsoft Active Directory und *OpenLDAP*[675] (siehe *3.4.1 Verzeichnistechnologien*) verbessert werden. Dazu entwickelt Microsoft den *Identity Lifecycle Manager 2007*[676] weiter[677].

Mit dem *Higgins-Projekt*, dessen Weiterentwicklung *Identity Mixer*, und dem *Bandit-Projekt* werden einige Entwicklungsumgebungen im Open Source-Bereich vorgestellt. OpenID und Yadis sind zwei Vertreter von immer zahlreicher werdenden Open Source-Alternativen zu CardSpace. Sie zählen zu den sogenannten *URL-basierten Identitäten*. Unter URL-basierter Identität (auch: *Light-Weight Identity*) wird die Authentifizierung eines Users anhand einer fixen, ihm gehörenden URL bezeichnet. Die URL ist dabei wie eine Webadresse eindeutig und kann zur Authentifizierung für Webdienste verwendet werden. Ausgestellt wird die URL von einem Identity Provider. Es zeichnet sich ab, dass die zueinander kompatiblen CardSpace und OpenID zu Quasi-Standards für URL-basierte Authentifizierung werden[678].

3.3.1.3.1 Higgins-Projekt

„*Higgins is a collaborative project focused on the creation of interoperable, protocol- and platform-independent identity components*.“ [679]

Higgins ist ein Entwicklungsframework für Browser-Anwendungen und Web Services zur Integration von Identitäten über verschiedene Systeme hinweg: Directories, Collaboration Tools und Kommunikationstechnologien (Microsoft WS-*, LDAP, E-Mail, Instant Messaging etc.).

Higgins ergänzt sich mit CardSpace dadurch, dass dieses als Authentifizierungsmechanismus mit dem Higgins-Framework zusammenarbeitet[680].

3.3.1.3.2 Identity Mixer

Identity Mixer (kurz: *Idemix*)[681] ist eine von IBM getriebene Weiterentwicklung des Higgins-Projekts. Im Unterschied zur konventionellen Identitätsmanagement-Software, wo mit Teilen der User-ID gearbeitet wird, gibt Idemix lediglich Pseudonyme (siehe *2.2.2 Pseudonymität*) weiter. Jede Identität kann somit mehrere verschiedene Pseudonyme haben. Informationen wie Kontoverbindung, Kreditkartennummer oder Geburtsdatum sollen damit nicht an die anfragende Partei übermittelt

[673] Apache Tomcat stellt eine Umgebung zur Ausführung von Java-Code auf Webservern bereit. http://tomcat.apache.org/ [30. Oktober 2007]
[674] http://www-306.ibm.com/software/websphere/ [30. Oktober 2007]
[675] http://www.openldap.org/ [30. Oktober 2007]
[676] http://www.microsoft.com/windowsserver/ilm2007/default.mspx [30. Oktober 2007]
[677] Vgl. http://www.pcwelt.de/index.cfm?pid=1871&pk=82155 [30. Oktober 2007]
[678] Vgl. http://blog.doubleslash.de/category/openid/ [2. November 2007]
[679] Vgl. http://www.eclipse.org/higgins/ [30. Oktober 2007]
[680] Vgl. http://www.iam-wiki.org/Higgins?highlight=%28higgins%29 [30. Oktober 2007]
[681] http://www.zurich.ibm.com/security/idemix/ [2. November 2007]

werden. Die Idee ist, dass pro Transaktion ein digitaler Berechtigungsnachweis vom datenhaltenden Anbieter des Anwenders (Bank, Krankenhaus, Behörde etc.) erstellt werden soll. Die Software stellt somit eine Art „Schutzschicht" dar, die integere Daten von einem *sicheren* Gegenüber anfordert und an einen möglicherweise *weniger sicheren* Dritten verschlüsselt verschickt[682].

3.3.1.3.3 Bandit-Projekt

Bandit[683] ist eine freie und kompatible Alternative zu Identitätsmanagementlösungen wie CardSpace. Eine erste Version namens *DigitalMe Information Card Selector*[684] ist seit Juli 2007 für Linux und Apple verfügbar. Dabei nutzt das von Novell unterstützte Bandit-Projekt Teile von Higgins und gibt die DigitalMe-Komponenten im Sinne des Open Source-Gedankens wieder an dieses Projekt zurück.
Im Vordergrund steht der Benutzer, der seine Informationen sowie den Zugriff darauf selbst verwalten und kontrollieren kann. Dies soll für eine höhere Sicherheit sorgen, da die Anwender nur die Informationen preisgeben, die für eine Transaktion nötig sind[685].

3.3.1.3.4 OpenID

OpenID ist ein dezentrales Open Source-Framework zur Authentifizierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*). Die Idee ist, dass sich bei OpenID registrierte Benutzer mit diesen Kontendaten auf beliebigen OpenID-unterstützten Webseiten anmelden können, ohne dass für jede Webseite eigene Credentials benötigt werden. Dabei wird das Konzept der URL-basierten Identität umgesetzt.
Eine OpenID-Identität ist eine URL, ein Benutzer kann mehrere OpenID-Identitäten haben. OpenID prüft die Identität eines Benutzers und agiert als Single-Sign-On-System (siehe *3.4.2.1 Passwort-Management und Single-Sign-On).*
OpenID wird laufend weiterentwickelt (Stand Jänner 2008: Version 2.0) und meist zusammen mit Yadis (siehe *3.3.1.3.5 Yadis*) verwendet. Vergleichbare Systeme, die bei höherer Komplexität mehr Funktionen bieten, sind die auf SAML (siehe *3.4.4.2.6 SAML*) aufbauenden Projekte CardSpace (siehe *3.3.1.2 Microsoft CardSpace*) oder *Shibboleth* (siehe *3.4.2 Access-Management und Technologien zur Autorisierung und Authentifizierung*). Seit Feber 2008 ist auch Microsoft im *Board of Directors* der OpenID-Foundation vertreten, damit involviert sich der nächste prominente IT-Konzern in diese Schlüsseltechnologie[686].
Die zentrale Verwaltung der Benutzeraccounts birgt Sicherheitsrisiken. Mit dem Diebstahl der OpenID-Daten (siehe *1.3.5.3 Identitätsdiebstahl*) kann der Angreifer Zugangsberechtigungen gleich

[682] Vgl. http://www.golem.de/0701/50176.html [2. November 2007]
[683] http://www.bandit-project.org/index.php/Welcome_to_Bandit [30. Oktober 2007]
[684] http://www.bandit-project.org/index.php/Digital_Me_Download [30. Oktober 2007]
[685] Vgl. http://www.golem.de/specials/identitaetsmanagement/ [30. Oktober 2007]
[686] Vgl. http://www.pressetext.at/pte.mc?pte=080208015 [8. Feber 2008]

für mehrere Websites bekommen. Das Auslagern von Benutzerdaten auf externe Server kann ebenfalls problematisch sein. Dies kann dadurch gelöst werden, indem ein eigener OpenID-Host betrieben wird. Jeder Domaininhaber kann einen OpenID-Server betreiben[687].

3.3.1.3.5 Yadis

„*Yadis is an open initiative to build an interoperable lightweight discovery protocol for decentralized, user-centric digital identity and related purposes. With Yadis, the capabilities of identities can composed from a open-ended set of services, defined and/or implemented by many different parties. By allowing each party in an online relationship to choose the authentication and data sharing protocols they want to use to share their information, Yadis fosters the development of mutual trust and respect. Yadis aims to make the internet a more people-friendly place by putting the human being at the centre of their own online experience, letting them define what information they expose and which services they use*."[688]

Unter Yadis wird ein freies Protokoll und Datenformat verstanden, mit dem Informationen nach dem Konzept der URL-basierten Identitäten beschrieben und abgerufen werden können. Yadis wurde im Sommer 2005 wieder aufgegriffen und bezeichnet eine Interoperabilitätsoffensive zwischen OpenID und *LID*[689] (steht für: *Lightweight Identity*). Verwendung findet Yadis für Single-Sign-On über mehrere Webseiten hinweg, beim Austausch von Profilen und zum Ausfüllen von Formularen.

3.3.2 FORSCHUNGSPROJEKTE IN DER EUROPÄISCHEN UNION

In der Europäischen Union gibt es gegenwärtig einige Forschungsprojekte rund um Identitätsmanagement und Privacy: *PRIME* (steht für: *Privacy and Identity Management for Europe*)[690], *FIDIS* (steht für: *Future of Identity in the Information Society*)[691] und *PRISE* (steht für: PRIvacy *enhancing shaping of SEcurity research and technology*)[692]. Für das behördliche Umfeld wurde im Juli 2007 das vier Jahre laufende *GUIDE* (steht für: *Government User IDentity for Europe*)[693]-Projekt abgeschlossen und auf der E-Government-Roadmap 2010 [EU, 2006] sind einige Punkte unter dem Titel „*eIDM*" umzusetzen.

Österreich leistet durch das *Institut für Technikfolgen-Abschätzung*[694] der *Österreichischen Akademie der Wissenschaften* seinen Beitrag.

Repräsentativ soll im Folgenden PRIME und GUIDE vorgestellt werden.

---

[687] Vgl. http://www.iam-wiki.org/OpenID [2. November 2007]
[688] Vgl. http://yadis.org/wiki/Main_Page [2. November 2007]
[689] LID benutzt URLs als Identifier, ist dezentral aufgebaut und unterstützt zugrundeliegende Protokolle wie OpenID oder Yadis.
[690] https://www.prime-project.eu/ [4. November 2007]
[691] http://www.fidis.net/ [4. November 2007]
[692] http://www.prise.oeaw.ac.at/ [4. November 2007]
[693] http://istrg.som.surrey.ac.uk/projects/guide/ [4. November 2007]

3.3.2.1.1 PRIME

Mit Systemen zum Identitätsmanagement soll das Problem der sicheren Identifikation von Benutzern im Internet gelöst werden. Der Druck auf die Entwicklung eines entsprechend sicheren Kommunikationsraums im Internet geht von Online-Händlern und von der Politik aus. Da sich eine zentrale, von einem Konzern verwaltete Lösung bisher aufgrund vielfacher Bedenken nicht durchsetzen konnte, geht der Trend zu nutzerzentrierten Lösungen (siehe *3.2.2 Benutzer-zentrierte Identität*).

Leitgedanke von PRIME ist, die personenbezogenen Daten unter der Kontrolle des Benutzers zu belassen. Unter PRIME sollen Lösungen für ein datenschutzförderndes Identitätsmanagement entwickelt werden, die die Souveränität der Benutzer über ihre Privatsphäre stärken und zur datenschutzgerechten Datenverarbeitung durch alle Beteiligten beitragen sollen. Ziel ist es, bei der Herausgabe persönlicher Daten für die Inanspruchnahme von Online-Services den jeweils maximal möglichen Datenschutz zu gewährleisten. Dies soll bei dieser Form des technischen Datenschutzes (siehe *2.4.3 Säule 3: Datenschutz durch Technik*) über die Durchsetzung von speziellen Regeln etwa zur Speicherdauer von Informationen erreicht werden, sobald der Benutzer personenbezogene Daten aus seinem Verfügungsbereich herausgibt.

Beim PRIME-Projekt geht es um Standardisierung und um die Entwicklung von sogenannten Tutorials und Prototypen. Eine Middleware soll Einblick in die Datenschutzregeln von Websitebetreibern verschaffen (siehe *2.4.2.1 Platform for Privacy Preferences*) und den Abgleich ihrer Präferenzen für freigegebene Informationen mit den diesbezüglichen Vorlieben anderer Webbenutzer und -anbieter ermöglichen. Dabei sollen Pseudonyme oder Anonymisierungsdienste zur Anwendung kommen. Vorgesehen ist beispielsweise auch, dass nicht mehr benötigte Lieferadressen oder Bankverbindungen automatisch im System eines Händlers gelöscht werden[695].

PRIME geht auf technische, rechtliche, soziale, wirtschaftliche sowie ergonomische Anforderungen ein. In einem *Network of Excellence* werden Experten aus Wirtschaft, öffentlicher Verwaltung, Verbraucherschutz- und Bürgerrechtsorganisationen, Forschung und Entwicklung, von Standardisierungsgremien, Datenschutzbehörden und Strafverfolgungsorganen beteiligt[696].

Die EU fördert PRIME im Rahmen des sechsten Europäischen Rahmenforschungsprogramms „Technologien für die Informationsgesellschaft (kurz: IST)“[697]. Das Projekt läuft seit März 2004 für die Dauer von vier Jahren mit einer Dotierung von zehn Millionen Euro.

---

[694] http://www.oeaw.ac.at/ita/ [4. November 2007]
[695] Vgl. http://www.heise.de/security/news/meldung/91826 [4. November 2007]
[696] Vgl. http://www.uld-i.de/projekte/prime/ [4. November 2007]
[697] http://cordis.europa.eu/ist/home.html [4. November 2007]

3.3.2.1.2 GUIDE

„*GUIDE is a technology research project, coordinated by BT alongside a consortium of 22 other commercial and academic partners. Its purpose is to define a solution for what is at face-value a simple technological problem: how can the potential benefits of ICT be most effectively harnessed in the context of Identity Management for E-Government? In practice, the problem is more complex: the field of Identity Management is subject to a wide array of non-technological restrictions – both harder legal/policy issues (e.g. data protection law), and softer socio-political issues (e.g. citizen concerns about privacy). GUIDE's objective is to create a solution – a secure "open architecture" for IM – that successfully accommodates all such restrictions, ensures full interoperability between existing Member States services, and is compliant with the core „principle of subsidiarity*"".[698]

Im Herbst 2007 gibt es ein offiziell publiziertes Ergebnis[699]: „*The GUIDE project has created an independent forum to help governments apply common standards for the secure exchange of personal data. People who come to work in the EU from America or Asia may find they have to rebuild their credit records before they can buy a car or a house. EU citizens generally have an easier time when moving between Member States, but accessing social security, employment and health services across borders is still cumbersome and error-prone. Rising concern about crime linked to identity theft makes reliable data exchange even more important.*

To improve this situation, the GUIDE project was set up to create uniform systems of identity management to support e-government services across Europe. GUIDE paves the way for trusted „identity providers" in different Member States to supply reliable information on the identities of individuals and businesses to those who rely on it, such as government departments offering important services. Different Member States have different rules about privacy and electronic record-keeping, but there is enough consistency to stop this from being a serious problem for data exchange. There are also well-proven computing techniques for exchanging information securely (siehe *1.3.4.2.5 SSL/TLS-Sicherheit*)."

Es gilt, zwei Herausforderungen zu lösen: „*The first is to persuade governments to trust one another with their citizens' data, and to make sure that these citizens have given permission for their data to be used across borders. The second is about technology: techniques that work for on-line shopping are not always appropriate for data exchange between huge government databases. On the topic of trust, GUIDE's independence has allowed it to generate interest, gain co-operation and propose standards in ways that would not have been possible between individual governments. On the technical side, the GUIDE partners have used and further developed existing security standards to meet the needs of e-government. Basic concepts like public key cryptography* (siehe *1.7.2.1.5 Public Key Infrastructure*) *have supported the creation of computer tools, such as SAML* (siehe *3.4.4.2.6 SAML*). *GUIDE has*

[698] Vgl. http://istrg.som.surrey.ac.uk/projects/guide/overview.html [4. November 2007]

taken the OASIS and Liberty standards and developed practical ways to use them for e-government data.

Identity management was originally done individually, system by system, with all the attendant problems of duplication and data integrity. It then evolved into a federated model where different organizations and systems use and rely on each other's identity data. GUIDE has taken this one step further, to create a pan-organization, pan-EU „federation of federations".

Die an GUIDE mitarbeitenden Partner haben die Lösungen in zwei Feldversuchen erfolgreich getestet: *"The first concerned form E101, used to record the social security details of people who are working temporarily in another country. This trial, which took place in the Netherlands, Belgium and Estonia, was a great success. It was followed by a second trial, this time on cross-border e-procurement in Germany, Spain and Finland.*"

Das Projekt ist von 1. Jänner 2004 bis 30. Juni 2007 mit einer Dotierung von knapp sieben Millionen Euro gelaufen[700]. Die Ergebnisse der Forschungsarbeiten bilden die Basis für weitere nutzenbringende E-Government-Anwendungen: „*For instance, the EU is committed to making all public procurement available electronically, and we are helping to make that possible. GUIDE has delivered what it was supposed to do, and it will help us all to become true European citizens*."

3.4 KOMPONENTEN UND FUNKTIONEN EINES IDENTITÄTSMANAGEMENTSYSTEMS

Identitätsmanagementsysteme basieren auf einer Bündelung von verschiedenen Techniken und Technologien. Viele dieser Komponenten (z. B.: Verzeichnisdienst, Webserver, Passwortmanagement) finden in der Regel in Organisationen ihren Einsatz. Diese meist isoliert agierenden Systeme gilt es im Hinblick auf ein unternehmensweites IMS zu adaptieren, zu ergänzen und in diesem Kontext zusammenzuführen. Die grundlegenden Leistungsmerkmale eines Identitätsmanagementsystem sollten sein: integrierbar, modular, interoperabel, skalierbar, konsistent, umfassend und ständig verfügbar [CA, 2005-1, S 6].

Ein Set an Techniken und Technologien – insbesondere jene auf Webbasis – ist die Grundlage für die Umsetzung der vier wichtigsten Komponenten eines IMS (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz*): *Verzeichnisse* mit den persönlichen Daten der Zugangsberechtigten; ein *Managementsystem*, mit dem sich Teilnehmerinformationen, Berechtigungen und Rollen hinzufügen, modifizieren und löschen lassen; ein *Sicherheitssystem*, das den Zugang zum Netzwerk oder einzelnen Diensten kontrolliert sowie ein *Auditsystem*. Mit letzterem soll sichergestellt werden, dass gesetzliche Grundlagen wie zum Datenschutz (siehe *1.7.3 Gesetzeslage, 2.3.2.2 Zusammenhang von Identitätsmanagement und Datenschutz*) technisch

[699] Vgl. http://istresults.cordis.europa.eu/index.cfm?section=news&tpl=article&ID=89061 [4. November 2007]
[700] Vgl. http://istlab.dmst.aueb.gr/content/projects/p_guide.html [4. November 2007]

abgebildet und eingehalten werden. Durch das integrative Zusammenwirken aller Module soll insbesondere dem Anspruch auf Privacy (siehe *2.3 Privacy*) entsprochen und das Recht auf informationelle Selbstbestimmung (siehe *2.3.2.1 Informationelle Selbstbestimmung*) umgesetzt werden.

3.4.1 VERZEICHNISTECHNOLOGIEN

Die Herausforderung besteht darin, dass die meisten Anwendungen ihre eigene Benutzerverwaltung implementiert haben. Standards wie LDAP haben zwar zur Öffnung beigetragen, aber die Realität in den Unternehmen ist von heterogenen Infrastrukturen mit unterschiedlichsten Identitätsspeichern geprägt (Anm.: Die Heterogenität wird mit jedem Firmenzusammenschluss größer). Diese Identitätsinformationen gilt es zu integrieren, um anwendungsübergreifende Prozesse realisieren zu können. Dafür gibt es verschiedene technische Ansätze:

- Die Verwendung eines gemeinsamen Verzeichnisdienstes für mehrere Anwendungen, die auf die gleichen Daten zugreifen.
- Ein Metadirectory, um Informationen in verschiedene Verzeichnisse zu synchronisieren.
- Die virtuellen Verzeichnisdienste, mit denen Informationen aus verschiedenen Verzeichnissen für eine Anwendung kombiniert werden können.
- Die Identity Federation (siehe *3.2.3 Identitätsföderation und -kontrolle*) als definierter, dynamischer Prozess der Übergabe von Identitätsinformationen zwischen Anwendungen.

Keiner dieser Ansätze kann gleichzeitig alle Anforderungen und Problemstellungen (Komplexität der Datenstrukturen, Komplexität der Einführung, Komplexität des Betriebs, erreichbare Datenqualität, Verfügbarkeit, Performance, Anpassungsbedarf von Anwendungen, Einsetzbarkeit im Unternehmen, Einsetzbarkeit über Unternehmensgrenzen hinweg, Sicherheitsaspekte, Datenschutz, Umgang mit Kennwörtern, Kosten, neue Anwendungen) adressieren. Eine enge Koppelung über gemeinsame Verzeichnisse setzt meist Anpassungen an Anwendungen voraus und hat auch andere praktische Grenzen. Eine lose Koppelung nur über das Provisionieren von Informationen in verschiedene Verzeichnisse ignoriert, dass Änderungen oft auch lokal in diesen erfolgen [KCP, 2004, S 3f].

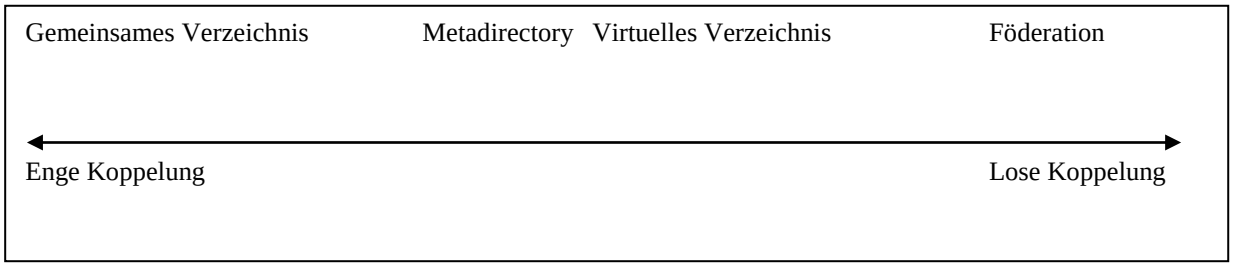


Abbildung 45: Koppelung von Identitätsinformationen

„*Directory is a key component of identity management systems. For many enterprise-centric systems, the directory acts as a hidden internal deployment. In many situations, particularly Government related, there are requirements to share secure identity between organizations. In order to do this, exposing the directory externally to the organization becomes important*.“[701]

3.4.1.1 Verzeichnisdienst

Ein Verzeichnisdienst (engl. *Directory Service*) ist ein System, das ein Verzeichnis verwaltet. Die in der Regel in einer hierarchischen Datenbank[702] gespeicherten Daten können damit nach dem Client-Server-Prinzip verglichen, gesucht, gelesen, erstellt, modifiziert und gelöscht werden. Somit wird es möglich, nach bestimmten Attributen von Anwendern (z. B.: E-Mail-Adresse) oder Ressourcen (z. B.: nächstgelegener Farbdrucker) zu suchen bzw. diese zu ändern.
In der technischen Umsetzung kommt dabei das *Directory Access Protocol* (kurz: *DAP*) zum Einsatz, Standardimplementierungen dieses Protokolls sind die X.500-Architektur sowie LDAP. Bekannte Verzeichnisdienste, praktisch alle auf dem LDAP-Standard basierend, sind[703]: Microsoft *Active Directory*, Novell *eDirectory*, *OpenLDAP* (Open Source) etc.[704]
Verzeichnisdienste nehmen eine zentrale Stellung beim Identitätsmanagement ein, weil in ihnen die Identitätsinformationen gespeichert werden. In den letzten Jahren hat sich LDAP als Zugriffsprotokoll etabliert, mittlerweile gewinnt das LDAP-basierte DSML immer mehr an Bedeutung.

3.4.1.1.1 X.500

X.500 ist ein Standard der *International Telecommunication Union* (kurz: *ITU*)[705], welcher den Aufbau eines Verzeichnisdienstes beschreibt. Die Idee von X.500 ist ein globales, verteiltes, baumartig strukturiertes Verzeichnis, auf das von überall zugegriffen werden kann. Jedoch kann ein unkontrollierter Zugriff bei einigen der gespeicherten Daten (z. B.: sensible Daten) nicht erwünscht sein. Daher kann festlegt werden, welche Objekte auf welche Einträge und Attribute Zugriff haben. Eine Authentifizierung kann entweder *einfach* über ein Passwort oder *stark* über Public-Key-Zertifikate erfolgen. Auf diese Weise können Teile des Verzeichnisbaumes nur bestimmten Personen zugänglich gemacht werden. Eine weite Verbreitung aus der X.500-Familie erreicht der Standard X.509 für Public Key Infrastruktur (siehe *1.7.2.1.5 Public Key Infrastructure*).

[701] Vgl. http://www.isode.com/whitepapers/identity-directory.html [21. September 2007]
[702] In einer hierarchischen Datenbank werden die Daten in einer Baumstruktur abgebildet. Jeder Datensatz hat mit Ausnahme der Wurzel genau einen Vorgänger. Hierarchische Datenbanken ermöglichen einen schnellen Zugriff, setzen jedoch eine einheitliche Beziehung vom Typ 1:n (Vater-Sohn) voraus.
[703] http://www.verzeichnisdienst.de/ [4. September 2007]
[704] Vgl. http://www.tecchannel.de/netzwerk/grundlagen/401675/ [4. September 2007]
[705] http://www.itu.int/ [5. September 2007]

3.4.1.1.2 LDAP und DSML

Ein verbreitetes Protokoll, das auf X.500 basiert, aber nicht all dessen Anforderungen entspricht, ist LDAP (steht für: *Lightweight Directory Access Protocol; RFC 4511*[706]). Es erlaubt die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes über ein TCP/IP-Netzwerk. Damit die Organisation der Daten nicht willkürlich geschieht, verwendet jedes LDAP-Verzeichnis eine genormte Struktur, ein sogenanntes Schema (Anm.: Da viele verschiedene Schemata in unterschiedlichen Versionen in Benutzung sind, ist ein globales LDAP-Verzeichnis nicht realisierbar.). Ein LDAP-Schema (siehe *3.5.3.2.6 Verzeichnisdienst LDAP-gv*.at) definiert Klassen mit Attributen. Die Verzeichniseinträge werden als LDAP-Objekte bezeichnet und gehören zu mindestens einer Klasse. Jedes Objekt setzt sich aus Attributen zusammen und wird eindeutig durch den *Distinguished Name* (kurz: *DN*) identifiziert. Jedes Attribut eines Objekts hat einen bestimmten Typ und mindestens einen Wert. Die Typenbezeichnungen eines Attributs sind meist einfache Kürzel wie beispielsweise *cn* für *common name*, *ou* für *organizational unit* oder *c* für *country*.

LDAP kann als De-facto-Standard für Autorisierung, Authentifizierung und Benutzerverzeichnisse bezeichnet werden. Der schnelle Verbindungsaufbau, das einfach strukturierte Protokoll und die performante Abfragesprache sorgen für eine schnelle Verarbeitung. Durch die verteilte Datenhaltung und lose gekoppelte Replikation erreicht LDAP eine hohe Verfügbarkeit[707].

DSML (steht für: *Directory Services Markup Language*) ist ein OASIS-Standard[708], der den Zugriff auf Verzeichnisse mittels XML-Schema und SOAP (siehe *3.4.4.2.3 SOAP*) als Transportmechanismus spezifiziert. Damit stellt DSML eine Verbindung zwischen Verzeichnis und Web Services (siehe *3.4.4.2 Web Services*) dar. DSML bietet eine Abbildung des kompletten LDAP-Datenmodells mit allen LDAP-Operationen. In Verbindung mit Technologien wie SAML (siehe *3.4.4.2.6 SAML*) oder SOA (siehe *3.4.4.2.8 SOA*) bietet DSML eine skalierbare Basis für die technische Realisierung von Identitätsmanagement[709].

3.4.1.2 Metadirectory und Virtuelles Verzeichnis

Jedes Unternehmen besitzt Daten über seine Kunden, Mitarbeiter und Ressourcen (z. B.: Netzwerkadressen von Servern, PCs, Drucker), welche in unterschiedlichen Verzeichnissen und Datenbanken (CRM, Personalinformations-, Betriebs-, Messaging-, Internet-, Telefonanlagen-, Zutrittskontrollsystem etc.) eingetragen sind. Hinzu kommt, dass es sich meist um eine gewachsene heterogene Netzwerkinfrastruktur verschiedenster Technologien und unterschiedlichster Entwicklungsstufen handelt.

[706] http://www.ietf.org/rfc/rfc4511.txt [5. September 2007]
[707] Vgl. http://www.tecchannel.de/ueberblick/archiv/401872/index13.html [5. September 2007]; http://www.mitlinx.de/ldap/ [5. September 2007]
[708] http://www.oasis-open.org/specs/index.php#dsmlv2 [6. September 2007]

Ein Metadirectory stellt ein *Überverzeichnis* dar, ermöglicht den Zugang zu sämtlichen Informationen einer Organisation, die in unterschiedlichen Verzeichnissen gespeichert sind sowie deren Administration von einer einzigen Stelle aus. Metadirectories synchronisieren und aggregieren Daten aus angeschlossenen Verzeichnissen und speichern diese in einem zentralen Verzeichnis. Der Vorgang des Erstellens, Änderns und Löschens von Benutzerdaten in den verbundenen Verzeichnissen erfolgt automatisiert. Die Identitäten (siehe *2.2.1 Digitale Identität*) werden auf diese Weise über alle angeschlossenen Verzeichnisse eindeutig, aktuell, vollständig und korrekt gehalten. Vorteile eines Metadirectorys sind somit[710]:

- Konsistenz und Aktualität der Daten über alle angebundenen Informationsquellen (Benutzer, Passwörter, Telefonnummern etc.),
- Automatisation der Benutzerverwaltung durch Synchronisation von Benutzerkonten und Passwörtern,
- Vereinfachung durch zentralisierte Verwaltung der Informationen mit einheitlichen Werkzeugen,
- Reduzierung der Verwaltungs-, Administrations- und Supportkosten,
- Integration von Workflows,
- Flexibilität für die Anbindung künftiger Anwendungen,
- Erhöhung der Informationssicherheit durch automatisiertes Deaktivieren/Löschen von abgelaufenen Benutzerkonten in allen angebundenen Systemen.

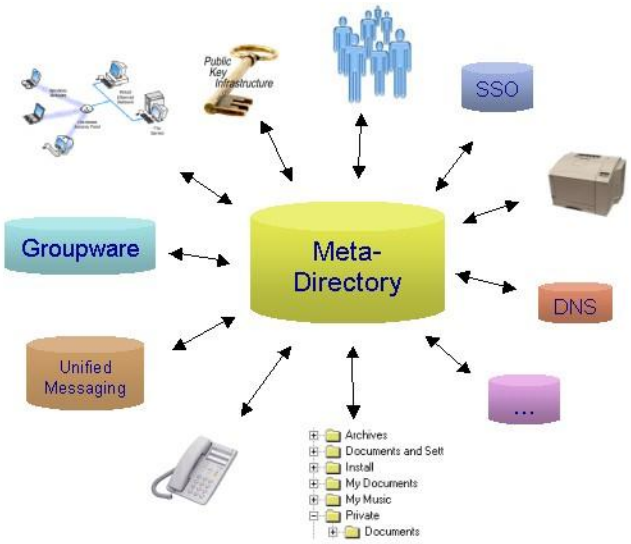


Abbildung 46: Metadirectory

Zum Informationsaustausch eines Metadirectory mit den verschiedenen Informationsquellen werden Schnittstellen, sogenannte *Konnektoren*, benötigt. Eine wichtige Anwendung des Metadirectory ist der

[709] Vgl. http://www.iam-wiki.org/Directory_Service_Markup_Language_%28DSML%29 [5. September 2007]

Bereich der Autorisierung und Authentifizierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität, 3.4.2 Access-Management und Technologien zur Autorisierung und Authentifizierung).* LDAP-fähige Internetportale ermöglichen eine Anmeldung von Benutzern und die Zuteilung von Rechten mit Hilfe von Verzeichnisdiensten, die ein Autorisierungs- und Authentifizierungssystem bilden. Auf der Grundlage dieses Verfahrens ist Single-Sign-On (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) für das Einwählen, VPN (siehe *1.3.4.2.5 SSL/TLS-Sicherheit*) und Portalfunktionalitäten (siehe *3.4.4 Portale und Web Services*) realisierbar.

Eine wichtige Rolle spielen Metadirectories beim Aufbau einer PKI (siehe *1.7.2.1.5 Public Key Infrastructure*) für Anwendungen mit erhöhten Sicherheitsbedürfnissen. Die organisatorischen Abläufe zur Erstellung und Verwaltung von Zertifikaten können durch ein Metadirectory optimiert werden. Die notwendigen Daten zur Zertifizierung hält das Metadirectory vor und ein Konnektor zum Zertifizierungsserver generiert eine Zertifizierungsanforderung. Bei erfolgreicher Zertifizierung gibt der Zertifizierungsserver das digitale Zertifikat an das Metadirectory zurück.

Hinsichtlich Informationssicherheit sind einige Grundsätze festzuhalten. In ein Metadirectory sollten nur so viele Daten wie nötig und so wenig wie möglich aufgenommen werden. Die personenbezogenen Daten zur Identifizierung (z. B.: Geburtsdatum) dürfen nach außen nicht sichtbar sein und nur bei Notwendigkeit der Identifizierung ausgewertet werden (siehe *2.4.2.2 Datensparsamkeit*). Benutzer sollten keinen direkten Zugriff auf das Metadirectory erhalten. Die Konnektoren sollten verschlüsselte Verbindungen benutzen. Der Metadirectory-Server sollte sich in einem eigens dafür vorgesehenen Servernetz befinden, dass durch geeignete Maßnahmen vor dem Zugriff aus dem Intranet und Internet geschützt ist (siehe *1.7.2.4 Perimetersicherheit*). Zur Verringerung der Angriffsfläche (z. B.: durch Schwachstellen auf dem System) wird der Einsatz eines Paketfilters (siehe *1.7.2.4.1 Firewall, 1.7.2.4.2 Content-Filter*) empfohlen.

Die Einführung eines Metadirectory geht mit einer umfassenden Analyse der Geschäftsabläufe einher und wird damit zu einem umfangreichen Projekt. Der Schritt zum Metadirectory sollte gut überlegt sein, oft führt ein Super-Directory nur zu überhöhten Kosten ohne die erwartete Effektivität [Evidian, 2005, S 4].

Virtuelle Verzeichnisse können Technologien wie Metadirectory zwar nicht ersetzen, aber sinnvoll ergänzen, weil Daten in einer anderen Strukturierung dargestellt werden können. Im Gegensatz zum Metadirectory werden die Benutzerdaten nicht synchronisiert, sondern in Form einer losen Koppelung während dem Zugriff über das virtuelle Verzeichnis in Echtzeit aus der Informationsquelle geladen. Die Daten existieren daher nur einmal in der angebundenen Datenquelle[711].

[710] Vgl. http://www.it-innovations.de/ks/Directory+Services/Meta+Directory.htm [5. September 2007]
[711] Vgl. http://www.kuppingercole.de/articles/im_kerntechnologien [6. September 2007]

3.4.2 ACCESS-MANAGEMENT UND TECHNOLOGIEN ZUR AUTORISIERUNG UND AUTHENTIFIZIERUNG

Grundlegende respektive projektspezifische Informationen hinsichtlich Authentifizierung sind in *1.4.1.2 Exkurs: Phishing, 1.7.2.3 Biometrie, 1.7.2.1.6 Digitale Zertifikate, 2.2.6 Autorisierung, Authentifizierung und Authentizität, 2.3.3.3 RFID* bzw. *3.5.3.2.5 Autorisierung und Authentifizierung* zu finden.

Grundsätzlich wird zwischen internem und externem Zugriff auf Daten (engl. *Access-Management*) unterschieden. Beim klassischen Access-Management geht es darum, die Zugriffsberechtigungen für interne Anwendungen zentral zu steuern. Web Access-Management hingegen regelt den Zugriff externer Benutzer auf interne Anwendungen. Mit Web Access-Management wird eine zentrale Sicherheitsschicht für unterschiedliche webbasierte Anwendungen und die Systeme, auf die diese Anwendungen zugreifen, realisiert. Diese ergänzt andere Sicherheitsmechanismen (siehe *1.7.2.4 Perimetersicherheit*), bietet aber den Vorteil zentraler Steuerung und Überwachung[712].

Der technischen Realisierung von Access-Management liegen Technologien wie *AAA*[713], *GSSAPI*[714], Kerberos, LDAP (siehe *3.4.1.1.2 LDAP und DSML*), *PAM*[715], *RADIUS*[716], SAML (siehe *3.4.4.2.6 SAML*), *SASL*[717], Shibboleth[718], *SPML* (siehe *3.4.4.2.7 SPML*), *WfMC*[719], *XPDL*[720] oder X.509 (siehe *1.7.2.1.5 Public Key Infrastructure, 1.7.2.1.6 Digitale Zertifikate*) zugrunde.

Die Authentifizierung über Benutzername-/Kennwort-Kombinationen (siehe *2.2.1 Digitale Identität*) oder PKI (siehe *1.7.2.1.5 Public Key Infrastructure*) mit digitalen Zertifikaten (siehe *1.7.2.1.6 Digitale Zertifikate*) sind nicht die einzigen Ansätze. Es gibt eine Fülle weiterer Mechanismen. Das beginnt bei PIN/TAN (siehe *1.4.1.2 Exkurs: Phishing*), Einmal-Kennwörtern (siehe *1.7.2.5 Graphisches*

[712] Vgl. http://www.kuppingercole.de/articles/im_kerntechnologien [8. September 2007]

[713] AAA (steht für: Triple-A-System) werden bei Netzwerkbetreibern und Internetdienstanbietern eingesetzt. Die drei A stehen dabei für Autorisierung, Authentifizierung und Abrechnung des Netzwerkzugangs von Kunden. Oft werden Triple-A-Systeme mit Verwaltungssystemen (z. B.: können Identitätsmanagementsysteme Teile dieser Kundendaten liefern bzw. die kommerziellen Aspekte und Daten der Endkunden verwalten) gekoppelt und beliefern wieder andere Systeme (z. B.: Rechnungswesen).

[714] GSSAPI (steht für: Generic Security Services Application Program Interface) ist eine standardisierte Schnittstelle zum Programmieren von Applikationen, die auf Sicherheitsgeräte zugreifen.

[715] PAM (steht für: Pluggable Authentication Module) ist eine Softwarebibliothek, die eine Programmierschnittstelle (kurz: API) für Authentisierungsdienste zur Verfügung stellt.

[716] RADIUS (steht für: Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur Autorisierung, Authentifizierung und zum Accounting (Triple-A-System) von Benutzern bei Einwahlverbindungen (Modem, ADSL, VPN, WLAN etc.) in ein Netzwerk dient.

[717] SASL (steht für: Simple Authentication and Security Layer) ist ein Rahmenwerk, das von verschiedenen Protokollen zur Authentifizierung im Internet verwendet wird.

[718] Shibboleth ist ein Verfahren zur verteilten Autorisierung und Authentifizierung für Web Services. Das Konzept von Shibboleth sieht vor, dass sich der Benutzer nur einmal (Single-Sign-On) bei seiner Stammeinrichtung authentifizieren muss, um ortsunabhängig auf Dienste oder lizenzierte Inhalte verschiedener Anbieter zugreifen zu können. Shibboleth basiert auf einer Erweiterung des Standards SAML.

[719] WfMC (steht für: Workflow-Management-Coalition) ist ein Verbund von mehr als 300 Herstellern, Nutzern und Wissenschaftlern im Bereich des Workflow-Managements. Hauptziel der WfMC ist die Etablierung eines Workflow-Referenzmodelles und der damit verbundenen XML Process Definition Language.

Passwort) über RFID (siehe *2.3.3.3 RFID*) bis hin zu biometrischen Verfahren (siehe *1.7.2.3 Biometrie*), bei denen Fingerabdrücke, die Struktur der Iris oder der Herzschlag[721] für die Identifikation eingesetzt werden.

3.4.2.1 Passwort-Management und Single-Sign-On

44 Stunden pro Jahr[722] bringt jeder Angestellte im Schnitt nur damit zu, sich in Systeme einzuloggen. Die Zielsetzung ist es, die Anzahl der Passwörter zu reduzieren, indem die gleichen Kennwörter für möglichst viele Systeme verwendet werden. Damit lassen sich die Helpdesk-Kosten reduzieren, die zu einem beträchtlichen Teil durch das Zurücksetzen von Kennwörtern verursacht werden (siehe *2.2.1.1 Lebenszyklus einer Identität*: […] das Passwortmanagement verursacht Kosten von 300 Dollar pro Benutzer und Jahr bzw. beansprucht 16 Minuten pro Benutzer und pro Tag an (Helpdesk-) Zeit.) Einheitliche Credentials bergen das Risiko, dass ein Angreifer auf viel mehr Systeme zugreifen kann, wenn er sich des einen, zentralen Kennworts habhaft gemacht hat.

In diesem Kontext gibt es drei Lösungsansätze[723]: Password Reset-Lösungen setzen Kennwörter in den verbundenen Systemen zurück, erkennen aber keine Änderungen. Die Benutzer können über Self Service (siehe *3.4.2.5 Self Service*) etwa durch Beantwortung einiger – vorher selbst festgelegter und definierter – Fragen (Geburtsname der Mutter, Ort der Volksschule etc.) oder über das Telefon in Verbindung mit Spracherkennungssystemen nutzen. Der Nachteil liegt darin, dass es immer auch andere Schnittstellen gibt, über die Kennwörter geändert werden können.

Hier setzen Lösungen für die Kennwort-Synchronisation an, die Änderungen an Kennwörtern erkennen und die geänderten Kennwörter auf andere Systeme verteilen.

Schließlich gibt es Single-Sign-On-Lösungen (kurz: SSO). Diese speichern die Credentials (z. B.: Benutzername-/Kennwort-Kombination, digitale Zertifikate) in einem gesicherten, verschlüsselten Speicher. Der Benutzer muss sich gegen das SSO-System nur einmal authentifizieren. Dieses stellt dann die Credentials für den Anwendungszugriff automatisch und transparent für die Benutzer bereit. Gerade im Hinblick auf Portale (*3.4.4 Portale und Web Services*) ist diese Möglichkeit aus Anwender- und Unternehmenssicht wünschenswert.

[720] XPDL (steht für: XML Process Definition Language) ist innerhalb des Workflow-Managements eine XML-basierte Sprache zur Beschreibung von Geschäftsprozessen und genauer Arbeitsabläufe.
[721] Die Heartbeat-ID ist ein Forschungsprojekt aus dem ein Herzsignalscanner (z. B.: im Handy verwendbar) entstehen soll, mit dem der menschliche Herzschlag zur sicheren Bestimmung und Authentifizierung einer Person verwendet wird.
[722] Vgl. http://www.cio.de/knowledgecenter/security/819775/ [8. September 2007]
[723] Vgl. http://www.kuppingercole.de/articles/im_kerntechnologien [8. September 2007]

3.4.2.2 DRM-Funktion

DRM (siehe *2.3.3.5 Digital Rights Management*) kann im Bereich von Identitätsmanagement Anwendung finden, da es granulierte Sicherheitsmechanismen mit sich bringt (z. B.: darf lesen, darf kopieren, darf ändern) [Hansen-2, 2006, S 14].

3.4.2.3 Chipkarten

Chipkarten (auch: *Smartcards*) sind spezielle Plastikkarten mit eingebautem Chip, der eine Hardware-Logik, Speicher oder einen Mikroprozessor enthält. Abhängig vom verwendeten Chip können die Daten durch PIN, Passwort oder Biometrie vor dem Auslesen oder der Veränderung durch Dritte geschützt werden.

Leistungsfähige Smartcards[724] und insbesondere die Kombination verschiedener Funktionen („Chip-basierender Unternehmensausweis“) gewinnen immer mehr an Bedeutung [Piller, 2005-2, S 39f]: zur Überprüfung des physischen Zugangs zum Unternehmen, zur Authentifizierung (Single-Sign-On) am PC, im LAN, im Intranet und im Internet (Portal), zur E-Mail- bzw. Daten-Signierung, zur Verschlüsselung (siehe *Absicherungs- und Vertraulichkeitsziele* in *2.1 Problemstellung und Herausforderung*), als Bürgerkarte, zur Zeiterfassung, zum Bezahlen in der Kantine etc.

Dadurch lassen sich die Kosten für Kartensysteme reduzieren, die in erheblichem Umfang einerseits durch Lesegeräte und andererseits durch das Handling der Karten verursacht werden. Zur Verwaltung der ausgegebenen Chipkarten, wie Ausstellung von Ersatzkarten, Widerruf von Karten und Zertifikaten usw. bedarf es in größeren Unternehmen wohl überlegter Prozesse.

Bemerkenswert in diesem Zusammenhang sind die Ansätze für eine differenziertere Autorisierung, basierend auf dem Ansatz der mehrstufigen Authentifizierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*). Wird etwa die Kontrolle des physischen Zugangs zu einzelnen Unternehmensbereichen mit der Netzwerkauthentifizierung kombiniert, kann der Zugriff auf bestimmte Anwendungen für Situationen einschränkt werden, in denen sich ein Mitarbeiter in einem bestimmten Gebäude aufhält[725].

Hinsichtlich Informationssicherheit gibt es immer wieder Verletzlichkeiten in den verschiedenen – in Chipkarten verwendeten – Verschlüsselungsalgorithmen zu berichten. Ein Beispiel[726] vom Herbst 2006 legt dar, mit welchen technischen Fertigkeiten nach Angriffspunkten für Attacken gesucht wird. Werden in integrierten Schaltkreisen Daten verarbeitet, so hängt die von den Schaltkreisen aufgenommene elektrische Leistung von den ausgeführten Verarbeitungsschritten ab. An den zugänglichen Anschlüssen von Schaltkreisen auf Chipkarten, die der Verschlüsselung von Daten

[724] Während die kontaktbehafteten Chipkarten bereits vielerorts im Einsatz sind, finden die kontaktlosen (auch: Proximity Cards) erst zunehmend durch Technologien wie RFID Verbreitung.
[725] Vgl. http://www.kuppingercole.de/articles/cards_280807 [31. August 2007]
[726] Vgl. http://www.bris.ac.uk/ [10. September 2007]

dienen, lässt sich der Verlauf der Leistungsaufnahme mit aufzeichnen. Aus den ausgewerteten Mustern konnten Spezialisten Rückschlüsse auf die verwendeten Schlüssel ziehen und die Sicherheit des Systems gefährden, was beispielsweise im Falle von Bankomatkarten höchst problematisch sein kann.

Chipkarten sind ein zentrales Element in jedem Sicherheitssystem, das digitale Signaturen (siehe *1.7.2.1.6 Digitale Zertifikate*) verwendet.

Das im Sicherheitssoftwarebereich tätige Unternehmen *Isode*[727] hat in einem Whitepaper[728] die Verwendbarkeit von Chipkarten (PKI, digitale Signatur) in föderalen Strukturen (siehe *3.2.3 Identitätsföderation und -kontrolle*) untersucht: „[…] *The most important thing to note with smartcard based authentication is that authentication happens locally.* […] *how federated identity works for password based authentication, and how federated identity can also be used to support smartcards. This is contrasted with the X.509 CA and Directory based model for supporting smartcard based authentication. Federated identity is a useful approach for supporting password based authentication between organizations. Where smartcards are used, distributed PKI is an alternative to federated identity, and it offers substantial benefits over federated identity. In order to implement smartcard authentication based on distributed PKI, PKI information (certificates and CRLs) is needed at the point of verification. Directory plays a key role in making this information available*."

3.4.2.4 Provisioning und Reporting

Als Provisioning[729] werden jene operativen Prozesse (siehe *3.5.4.2.2 Ablauforganisation: operativen Prozesse*) bezeichnet, die nötig sind, um IT-Anwender mit den notwendigen Ressourcen (z. B: Benutzername, Passwort, E-Mail-Adresse, Applikation) zu versorgen (siehe *3.6.3 Von der Identität zur Rolle*). Ziel von Provisioning ist eine größtmögliche automatisierte Verteilung in verschiedene Systeme, Verzeichnisdienste und Anwendungen zu erreichen. Die Prozesse, die zu einem Provisioningsystem gehören können, sind vielfältig. Hierunter fallen beispielsweise die Propagation von Änderungen an angeschlossene Systeme oder die Vereinheitlichung der Administration. Um die Administratoren zu entlasten und Helpdesk-Kosten zu reduzieren, bieten Provisioningsysteme oft Self Service-Funktionen (siehe *3.4.2.5 Self Service*) an.

Im Umfeld von Provisioning spielt Privacy (siehe *2.3 Privacy*) in mehrfacher Hinsicht eine Rolle [IT-Research, 2003, S 13]:

- Im Rahmen der Provisioning-Workflows kann die Einhaltung von Datenschutzvorschriften überprüft werden.

[727] http://www.isode.com/ [13. September 2007]
[728] Vgl. http://www.isode.com/whitepapers/smartcard-federated-directory.html [12. September 2007]
[729] Vgl. http://www.iam-wiki.org/Provisioning?highlight=%28provisioning%29 [22. September 2007]

- Bei der Konfiguration von Richtlinien, über die das Provisioning gesteuert wird, können Regeln für den Schutz der privaten Daten von Benutzern definiert werden.
- Benutzer können im Rahmen des Self Service die Möglichkeit erhalten, Zugriffsregeln für eigene Daten zu konfigurieren, respektive den Status hinsichtlich Privacy für ihre Daten zu überprüfen.

In der Regel verfügen User Provisioning-Systeme über Reportingfunktionalitäten, sodass sie den Zustand der Berechtigungen der digitalen Identitäten zu jedem Zeitpunkt revisionssicher dokumentieren (siehe *3.4.3 Auditing*). Damit ermöglichen sie die Nachvollziehbarkeit aller relevanten Aktionen und helfen damit, gesetzliche Vorschriften (siehe *3.5.2.1 Gesetze, Regulative, Compliance*) zu erfüllen.

Provisioning funktioniert für zentrale und verteilte Systeme. Zentrale Systeme nehmen Provisionierungsanfragen entgegen und veranlassen die Änderungen direkt in den angeschlossenen Systemen (z. B.: Virtuelles Verzeichnis). Bedingung für ein zentrales System ist, dass diese direkten Zugriff auf die angeschlossenen Systeme haben. Bei verteilten Systemen, bei denen kein zentrales autoritatives System existiert, sondern die Systeme innerhalb eines Circle of Trust (siehe *3.2.3 Identitätsföderation und -kontrolle*) agieren und jeweils eigenständige Benutzerverwaltungen besitzen, arbeiten die einzelnen Systeme als vollwertige Provisionierungssysteme, die Anfragen entgegennehmen bzw. Anfragen an andere Systeme versenden. Dabei kann eine Kombination beider Strategien Sinn machen. Unternehmensintern ist es in der Regel einfacher, eine virtuelle Directory-Lösung (siehe *3.4.1.2 Metadirectory und Virtuelles Verzeichnis*) zu verwenden. Da die Umsetzung eines unternehmensübergreifenden Identitätsmanagementsystems aufwendig ist und jedes Unternehmen die Datenhoheit beansprucht, kann verteiltes Provisioning eine Lösung sein.

Die Berechtigungsvergabe zum Zugriff auf betriebliche Ressourcen soll modellbasiert und automatisiert erfolgen. Die Bildung von hinreichend semantikreichen Berechtigungsmodellen über die Modellierung von Benutzerrollen und -regeln (siehe *3.6.3.1 Rollenkonzepte*) ist in der Vergangenheit an einem nicht ausreichenden Organisationsgrad der Unternehmen gescheitert. Projekte mit diesen Zielen sind meist vom IT-Bereich ausgegangen, hatten somit wenig Möglichkeit, die Reife der Unternehmensprozesse (siehe *3.5.4.2.2 Ablauforganisation*) insgesamt zu beeinflussen. Mit dem Zwang, zu bestimmten gesetzlichen Regelungen kompatibel sein zu müssen, erfährt die modellbasierte Berechtigungsvergabe neue Bedeutung. Automatisiertes Benutzerprovisioning bedingt die Zustimmung der Unternehmensführung.[730]

[730] Vgl. http://www.kuppingercole.de/events/eic2007 [22. September 2007]

3.4.2.5 Self Service

Mittels *Self Service* (kurz: *SS;* auch *Employee Self Service* – kurz: *ESS*) können Mitarbeiter eines Unternehmens anhand einer Anwendung eigene Daten selbst anlegen, anzeigen oder ändern. Durch die Zugriffsmöglichkeit der Mitarbeiter auf eigene Daten und Prozesse der Personal- bzw. IT-Abteilung über das Intranet (siehe *2.3.3.2.7 Portale, 3.4.4.1 Portalfunktionen*) werden Abläufe der Administration vereinfacht, beschleunigt und vereinheitlicht. Dies bedeutet, dass Aufgaben, die der Benutzer selbst erledigen kann, an ihn delegiert werden. Hierunter fällt zum Beispiel das Rücksetzen und Ändern eigener Passworte, die Pflege bestimmter Identitätsattribute wie Adresse oder Telefonnummer. Prozesse wie Vertreterregelungen, automatisierter Berechtigungsentzug bei Beendigung der Geschäftsbeziehung, Aufteilung von Administrationsaufgaben gehören ebenfalls in diese Kategorie (siehe *3.6.2 Aufteilung der Verwaltung* der Benutzerdaten).

Personalinformationssysteme bieten beispielsweise die Funktion ESS. Dabei verwalten Mitarbeiter einen Teil ihrer Personaldaten selbst und entlasten damit die Personalabteilung von Routineaufgaben. Die gängigsten Funktionen eines solches Services sind die Änderung persönlicher Daten, das Abholen von Schulungsinformationen, offenen Stellen, Urlaubsplanung, Reisekostenabrechnung sowie die Möglichkeit sich Bescheinigungen eigenständig auszudrucken.

Ein anderes Beispiel[731] zeigt ESS für den Bereich der Speicherplatzreservierung für Mitarbeiter. Durch eine Anwendung wird es möglich, automatisch Speicherplatzzuteilungen für Benutzer und Abteilungen zu machen. Durch die Definition von Speicherplatzgrenzen und die Einbeziehung des Vorgesetzten soll der Benutzer sensibilisiert werden, Unternehmensrichtlinien zu respektieren und die Verantwortung für die Verwaltung des zugesicherten Speicherplatzes zu übernehmen. Damit der Mitarbeiter diese Verwaltung leichter durchführen kann, erhält er eine einfache Sicht auf seine gespeicherten Daten ohne Verzeichnis-Grenzen. Per Knopfdruck kann er diese Daten nach Größe, Alter, Typ oder doppelten Dateien sortieren und anzeigen lassen. Auf diesem Weg wird die Speichernutzung wesentlich effizienter, da nur der Endbenutzer entscheiden kann, welche Daten gelöscht und welche archiviert werden können. Die Durchgängigkeit des Systems erlaubt, dass neue Speicherplatzanforderungen von Benutzern durch einen Klick des Vorgesetzten genehmigt oder abgelehnt werden. Zur Entscheidungsunterstützung erhalten der zuständige Manager[732] und der Benutzer einen Bericht über die aktuelle Nutzung des Speicherplatzes. Durch die Automatisierung des Prozesses ist die IT-Abteilung nicht länger involviert und wird dadurch entlastet. Im Einzelnen lassen sich Benachrichtigungen einstellen, wie oft und wann welche Speicher für die automatische Zuordnung erlaubt sind. Es lassen sich auch Eskalationswege definieren, die festlegen, wer bekommt

[731] Vgl. http://www.securitymanager.de/magazin/news_h25897.html [3. September 2007]
[732] Der zuständige Manager wird vom System automatisch durch das entsprechende Personalinformationssystem ermittelt.

wann eine Nachricht, wenn der zuständige Manager nicht innerhalb einer definierten Frist auf die Anforderung reagiert. Sämtliche Anfragen, ob genehmigt oder abgelehnt, werden gespeichert.

3.4.3 AUDITING

Als *Auditing*[733] werden beim Identitätsmanagement die Bemühungen bezeichnet, vergangene und aktuelle Zugriffsrechte eines Benutzers auf IT-Ressourcen nachvollziehen und prüfen zu können (siehe *3.5.2.1 Gesetze, Regulative, Compliance*). Als Basis dazu dienen Loggingmechanismen (engl. *Audit Trails*), wo laufend mit protokolliert wird, um jederzeit feststellen zu können, welche digitale Identitäten aus welchem Grund auf welche IT-Ressourcen Zugriff gehabt haben bzw. aktuell haben und wer diese Rechte vergeben hat (siehe *3.4.2.4 Provisioning und Reporting*).

3.4.4 PORTALE UND WEB SERVICES

3.4.4.1 Portalfunktionen

Während in den Ausführungen in *2.3.3.2.7 Portale* allgemeine Aussagen zu Portalen im Kontext von Privacy getroffen wurden, soll an dieser Stelle auf die für Identitätsmanagement im betrieblichen Umfeld relevanten Aspekte eingegangen werden.
Als Portal wird eine Anwendung auf Webbasis bezeichnet, welche durch folgende Eigenschaften und Funktionalitäten gekennzeichnet ist [Fraunhofer, 2003, S 5]:

- Integration von Anwendungen, Services (siehe *3.4.4.2 Web Services*), Informationen und Prozessen.
- Bereitstellung von Funktionen (Personalisierung, Informationssicherheit, Navigation und Benutzerverwaltung; Suche und Präsentation von Informationen; Dokumenten-, Content-, Wissens-, Geschäftsprozess-Management, Collaboration).

Eine manuelle Anmeldung bei den in das Portal integrierten Anwendungen ist durch Single-Sign-On (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) nicht mehr erforderlich, es gibt einen zentralen Zugriff über eine homogene Benutzungsoberfläche. Portale bieten die Möglichkeit, Prozesse und Zusammenarbeit innerhalb heterogener Gruppen (intern, extern) zu unterstützen (*Collaboration*).
Die einzelnen Anwendungen werden in sogenannten *Portlets*[734] organisiert. In den Portlets werden Inhalte aus unterschiedlichen Quellen auf einer Portalseite zusammengefasst (siehe *3.4.4.2 Web*

[733] Vgl. http://www.iam-wiki.org/Auditing [14. November 2007]
[734] Applet/Servlet/Portlet:
Ein Applet ist ein Programm, das im Rahmen eines anderes Programms (z. B.: Webbrowser) betrieben wird. Applets dienen dazu, Programme in Webseiten ablaufen lassen zu können, die im Client-Webbrowser arbeiten und direkt mit dem Benutzer interagieren können, ohne Daten über die Leitung zum Server schicken zu müssen.

Services: Mashup). Die einzelnen Portlets können personalisiert werden (siehe *3.5.3.2 Definition Portalverbund*).

Diese Funktionen kommen vor allem dann zum Tragen, wenn bei der Portalumsetzung konsequent die Sicht auf Geschäftsprozesse gehalten wird. Daher ist ein Unternehmensportal ein Baustein des Konzepts der Service-orientierten Architektur (siehe *3.4.4.2.8 SOA*).

Moderne Portaltechnologien eröffnen Unternehmen zahlreiche Möglichkeiten, Geschäftsprozesse zu beschleunigen, Aufwände zu minimieren und damit Kosten zu sparen. Dazu müssen die Systeme für Mitarbeiter, Partner und Kunden jederzeit und ortsungebunden über das Portal erreichbar sein. Eine wesentliche Säule zur Gewährleistung der Verfügbarkeit ist Informationssicherheit. Im Konkreten ist für Portallösungen neben dem Schutz vor Schadprogrammen (siehe *1.3.4 Computer Anomalien/Malicious Code*) der Einsatz von Content Filtern (siehe *1.7.2.4.2 Content-Filter*) erforderlich. Angriffe wie Cross-Site-Scripting (siehe *1.4.3.5.1 Cross Site-Scripting*) und SQL-Injection (siehe *1.4.3.5.3 SQL-Injection*) können dann ebenso geprüft werden wie das Einspielen unerwünschter Inhalte und Formate.

Eine weitere Hauptforderung an moderne Portallösungen ist die sichere Interaktion des Portals mit den angeschlossenen Backend-Systemen (z. B.: CRM, Personalinformationssystem). Zudem werden vermehrt heterogene Lösungen eingesetzt, die unterschiedliche Plattformen, auch die der Partner, in einen Lösungsansatz integrieren. Sicherheit beschränkt sich in diesen Ansätzen auf die Sicherheit der Infrastruktur wie etwa Reverse Proxy-Lösungen (siehe *1.7.2.4.3 Proxy, 1.7.2.4.4 Intrusion Detection Systeme und Intrusion Prevention Systeme*).

Vor allem in größeren Organisationen kommt dem Management von Identitäten (siehe *2.2.1.1 Lebenszyklus einer Identität*) besondere Bedeutung zu. Unabhängig davon, ob ein Zulieferer oder eine Fachabteilung eine Anwendung nutzen möchte, bringt ein entsprechender Prozess Transparenz und Struktur in eine Organisation. Aus diesem Grund sollte in ein IMS ein adäquates Workflow-System (siehe *3.5.4.2.2 Ablauforganisation: operativen Prozesse*) integriert sein, wobei „*alle gängigen Workflows als Templates* (deutsch: Vorlagen) *abgebildet sein sollten*." [Doubleslash, 2006, S 18].

Portale kommunizieren mit den angeschlossenen Applikationen über technische Konzepte. Dieser Ansatz schränkt die spezifische Rechtevergabe auf den einzelnen Systemen ein. Daher ist eine standardisierte Lösung, die Prozesse an den Zielsystemen mit den entsprechenden Credentials

---

Servlets laufen im Gegensatz zu Applets auf Servern und dienen zur dynamischen Erstellung von Webinhalten. Mit Servlets werden Java-Klassen bezeichnet, deren Instanzen innerhalb eines Applikationservers Anfragen von Clients entgegen nehmen und beantworten.

Portlets sind als Erweiterung von Servlets zu sehen, im Unterschied zu Servlets erzeugen Portlets keine vollständigen Seiten, sondern Fragmente, die vom Portal zu einer Seite zusammengestellt werden. Portlets sind beliebig kombinierbare Komponenten einer Benutzeroberfläche, die von einem Portalserver angezeigt und verwaltet werden. Eine Portalseite besteht aus mehreren Portlet-Fenstern, in denen jeweils ein Portlet (z. B.: Nachrichtenteil, Diskussionsforum, E-Mail) ausgeführt wird.

ergänzen kann, notwendig. Identitätsmanagementsysteme können eingebunden werden und ermöglichen dadurch eine nahtlose Integration in Unternehmensumgebungen[735].

3.4.4.2 Web Services

Web Services sind selbstbeschreibende[736], gekapselte[737] und lose gekoppelte[738] Software-Komponenten, die Schnittstellen anbieten, über die ihre Funktionen entfernt[739] aufgerufen werden können. Das Ziel ist die Interoperabilität von Softwaresystemen, um unabhängig von Plattform und Programmiersprachen miteinander kommunizieren und arbeiten zu können. Auf Web Services kann über Standardprotokolle des Internets (z. B.: HTTP, SMTP) zugegriffen werden, der Datenaustausch erfolgt unter Verwendung von XML[740].

Web Services basieren auf den drei XML-Standards WSDL (siehe *3.4.4.2.1 WSDL*), UDDI (siehe *3.4.4.2.2 UDDI*) und SOAP (siehe *3.4.4.2.3 SOAP*).

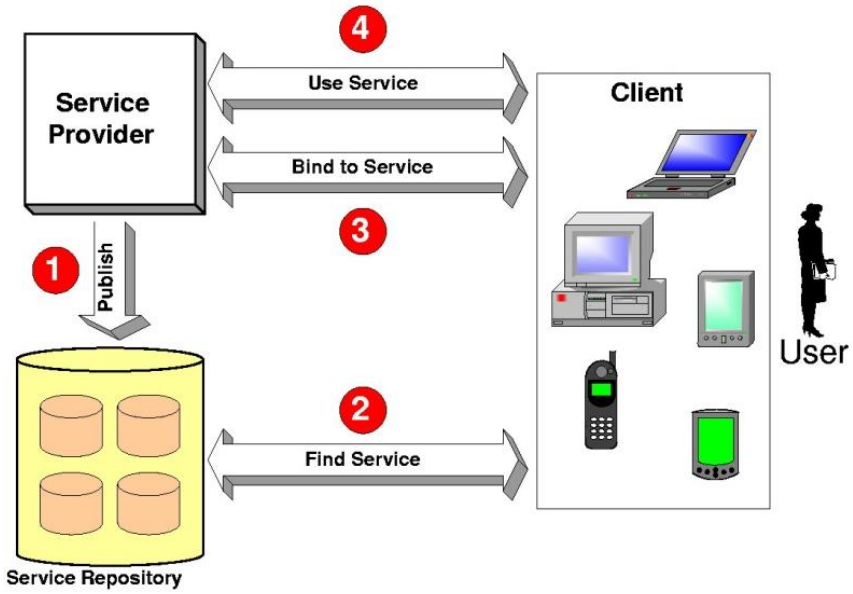


Abbildung 47: Web Service-Grundprinzip

[735] Vgl. http://www.digitalidworld.de/agenda.php#V22 [3. September 2007]
[736] Web Services enthalten Metadaten, die während der Laufzeit von weiteren Web Services ausgewertet werden können. Name, Beschreibung, Version und Dienstgüte sind typische Beschreibungsmerkmale.
[737] Gekapselte Anwendungen erfüllen genau eine definierte Aufgabe.
[738] Die Implementierungsdetails bleiben Konsumenten und Anbietern verborgen.
[739] Web Services sind ortsunabhängig und können jederzeit von jedem Ort aus unter der Voraussetzung entsprechender Zugriffsrechte aktiviert werden.
[740] XML (steht für: Extensible Markup Language) ist eine Auszeichnungssprache zur Darstellung strukturierter Daten in Form von Textdateien. XML wird für den Austausch von Daten zwischen unterschiedlichen IT-Systemen eingesetzt, speziell über das Internet. Die von W3C herausgegebene XML-Spezifikation definiert eine Metasprache, auf deren Basis anwendungsspezifische Sprachen entwickelt werden. Beispielsweise wurde die bekannte Dokumentsprache HTML in dieses Konzept integriert, so dass ihr nun XML zugrunde liegt.

Abbildung 46 illustriert das Grundprinzip von Web Services: Ein Dienstanbieter veröffentlicht ein Service in einem Dienstverzeichnis (1). Ein User findet das Service (2), bindet es in seine IT ein (3) und nutzt es (4).

Web Services orientieren[741] sich an Service-orientierten Architekturen (siehe *3.4.4.2.8 SOA*), mit der sich Informationsdienste im Internet automatisieren lassen.

Ein typisches Beispiel eines Web Services ist die Google Suche. Durch dieses Service werden einer beliebigen Webseite die gleichen Funktionalitäten geboten wie sie die Benutzerschnittstelle auf der Website[742] selbst offeriert. Programme können durch das Ansprechen der Schnittstelle direkt nach Informationen im Internet suchen, erhalten über die Schnittstelle die Ergebnisdaten und können diese für ihre eigenen Aufgaben verwenden.

In diesem Zusammenhang wird der Begriff „*Mashup*" verwendet. Mashup bezeichnet die Erstellung von neuem Content durch die Kombination bereits bestehender Inhalte. Texte, Bilder, Musik oder Videos werden durch das Ausnutzen offener Programmierschnittstellen, die andere Webanwendungen zur Verfügung stellen, neu kombiniert. So können beispielsweise Anbieter von Webseiten über die API von Google Maps Landkarten und Satellitenfotos auf der eigenen Webseite einbinden und zusätzlich mit individuellen Markierungen versehen.

Web Services sind schon seit einiger Zeit etabliert. Neben unternehmensweiten Lösungen erleichtert die Verwendung von Web Services die Anwendungsintegration bei der Anbindung mobiler Geräte und dedizierter Hardware signifikant[743].

3.4.4.2.1 WSDL

WSDL (steht für: *Web Service Description Language*) ist eine XML-basierte Metasprache, um die Funktionalitäten von Web Services bzw. deren Schnittstellen zu beschreiben. Die Beschreibung erfolgt auf einer abstrakten und einer technischen Ebene. Dabei werden jene Informationen transportiert, die der Web Service-User braucht, um das Web Service zu nutzen. So lässt sich mithilfe von WSDL definieren, welche Methoden bei der Server-Komponente vom Client ausgeführt werden können, welche Parameter dabei übergeben werden müssen und welchen Rückgabewert diese einzelnen Methoden liefern[744].

[741] Web Services können entweder in weitere Web Services zerlegt werden oder mehrere, wieder verwendbare Basis-Web Services können zu einem neuen Web Service zusammengestellt werden.
[742] Vgl. http://code.google.com/ [1. September 2007]
[743] Vgl. http://www.tecchannel.de/webtechnik/soa/457051/ [1. September 2007]; http://www.w3.org/2002/ws/ [1. September 2007]; http://www.jeckle.de/semanticWebServices/index.html [1. September 2007]
[744] Vgl. http://www.tecchannel.de/webtechnik/soa/464653/ [1. September 2007]

3.4.4.2.2 UDDI

UDDI (steht für: *Universal Description, Discovery and Integration*)[745] ist ein Verzeichnisdienst für Web Services. Der Dienst spezifiziert eine standardisierte Verzeichnisstruktur für die Verwaltung von Web Services-Metadaten. Es handelt sich dabei um eine Art „Gelbe Seiten", in dem Web Services und ihre Schnittstellen registriert sind. Dadurch lassen sich Services suchen und finden. Zu den Metadaten gehören allgemeine Anforderungen, Web Services-Eigenschaften oder die benötigten Informationen zum Auffinden von Web Services[746].

3.4.4.2.3 SOAP

SOAP (steht für: *Simple Object Access Protocol*) ist ein plattformunabhängiges, XML-basiertes Protokoll zur Kommunikation, zum Nachrichtenaustausch und zur Durchführung von *Remote Procedure Calls* (kurz: *RPC*)[747] über Web oder in heterogenen Computernetzen[748]. SOAP stützt sich auf Dienste anderer Standards: XML zur Repräsentation der Daten und Internet-Protokolle der Transport- und Anwendungsschicht (siehe *Abbildung 4: Protokolle des OSI-Schichtenmodells*) zur Übertragung der Nachrichten. Eine gängige Kombination ist SOAP über HTTP (siehe *1.3.4.2.3 HTTP-Sicherheit*) und TCP (siehe *1.3.4.2.1 TCP/IP-Sicherheit*).
Der Nachteil von SOAP ist, dass es über keine Sicherheitsmechanismen verfügt. Die Daten werden im Klartext übermittelt, es gibt keine Maßnahmen für Verschlüsselung oder Authentifizierung. Diese Funktionen müssen entweder die zugrundeliegenden Übertragungsprotokolle (z. B.: Einsatz von HTTPS-Verbindungen) oder die kommunizierenden Programme abdecken. Erweiterungen von SOAP um Sicherheitsaspekte finden sich in Form der WS-Security-Spezifikation wieder[749].

3.4.4.2.4 REST und AJAX

Neben SOAP gibt es alternativ *REST* (steht für: *REpresentational State Transfer*) für die Realisierung von Web Services. REST basiert auf Prinzipien, die im World Wide Web eingesetzt werden. Verwendung finden ausschließlich reife und standardisierte Techniken wie HTTP. Die Interaktion zwischen Client und Server wird bei REST-konformen Web Services unter Verwendung der durch HTTP definierten, einheitlichen Schnittstelle abgewickelt. REST macht sich die Ideen des Webs wie Hypertext und einen unbegrenzten, globalen Adressraum zunutze. Das Modell soll als Anleitung und

[745] http://www.uddi.org/ [1. September 2007]; http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec [1. September 2007]
[746] Vgl. http://www.tecchannel.de/webtechnik/soa/472223/index4.html [1. September 2007]
[747] Remote Procedure Call (deutsch: Prozedur-Fernaufruf) ist eine Technik zur Netzwerkkommunikation auf den Anwendungsschichten fünf und sechs des OSI-Modells. Mit Hilfe von RPC können über ein Netzwerk Funktionsaufrufe auf entfernten Rechnern durchgeführt werden.
[748] Vgl. http://www.semantic-web.at/6.52.37.catchword.soap.htm [8. August 2007]
[749] Vgl. http://www.fh-wedel.de/~si/seminare/ws00/Ausarbeitung/6.soap/soap09.htm [1. September 2007]

als Referenz für zukünftige Erweiterungen dienen. Viele Suchmaschinen, Webshops oder Buchungssysteme sind – ohne Absicht – bereits als REST-basierte Web Services verfügbar[750].

Hinsichtlich Performance von Webanwendungen ist in diesem Zusammenhang *AJAX* (steht für: *Asynchronous JavaScript and XML*) zu erwähnen. AJAX bezeichnet ein Konzept der asynchronen Kommunikation zwischen Server und Browser, das es ermöglicht, dass der User weiter mit der Oberfläche arbeiten kann, während Daten vom Server geladen werden. Der Vorteil besteht darin, dass nur bei Bedarf Teile einer HTML-Seite oder Daten nachgeladen werden. AJAX-Anwendungen sind demnach in der Lage, Anfragen an den Server zu schicken, bei denen nur die Daten angefordert werden, die tatsächlich benötigt werden. Der Aufruf eines Web Services erfolgt dabei über REST (oder SOAP). Bei AJAX werden verschiedene bekannte Technologien (HTML, JavaScript etc.) eingesetzt, um interaktive, Desktop-ähnliche Webanwendungen zu realisieren. Diese vermitteln den Eindruck, als ob das Problem der zustandslosen Webanwendung (siehe *1.4.3.5.2 Session-Hijacking, 2.3.3.2.3 Cookies, 3.5.3.2.1 Portalverbundprotokoll*) behoben sei[751]. Das zugrunde liegende JavaScript und die asynchrone Datenübertragung bergen Risiken (Cross Site-Scripting, DoS etc.), die bei Design und Programmierung moderner Webanwendungen zu beachten sind [c't, 2008, S 130f].

3.4.4.2.5 WS-Security

Aufgrund ihrer technischen Struktur sind Web Services diversen Sicherheitsrisiken (siehe *1.3 Taxonomie von Angriffen auf den Wert Information*) ausgesetzt. Bei Web Services steht nicht die Interaktion mit einem Benutzer sondern die direkte Koppelung von Anwendungsservern im Vordergrund. Die Kommunikation findet daher großteils zwischen Rechnern und Applikationen statt, Menschen sind nur bei wenigen Transaktionen beteiligt. Dies erhöht das Sicherheitsrisiko, da Manipulationen schnell bis in die Backend-Systeme durchschlagen können. Eine zu meisternde Herausforderung ist die eingeschränkte Kontrollmöglichkeit. Ein Web Service kann überall laufen, damit auch in einer Umgebung mit geringen Sicherheitsansprüchen, die dem Unternehmen, das einen Web Service aufruft, nicht genügen könnte. Um geschäftskritische Anwendungen in komplexen und unübersichtlichen Umgebungen zu betreiben, müssen bestimmte Sicherheitsanforderungen gewährleistet sein. Web Services sollen garantieren, dass die Integrität und Authentizität der ausgetauschten Informationen sowie die Vertraulichkeit und Verbindlichkeit von Transaktionen (siehe *1.2.2 Anforderungen an die Informationssicherheit*) gegeben ist.

Zur Realisierung dieser Sicherheitsanforderungen gibt es technische Lösungen, die sich im Wesentlichen in zwei Verfahrensklassen einordnen lassen: Kryptografie (siehe *1.7.2.1.1 Verschlüsselungsverfahren*) und elektronische Signatur (siehe *1.7.2.1.7 Elektronische Signatur*).

[750] Vgl. http://www.oio.de/public/xml/rest-webservices.htm [7. Jänner 2007]
[751] http://www.ajax-community.de/ [7. Jänner 2007]

WS- (steht für *Web Service-*) Security kann als Rahmenwerk betrachtet werden, dass alle relevanten Punkte zum Thema Sicherheit bei Web Services beinhaltet. Dazu unterstützt, integriert und vereinheitlicht WS-Security diverse populäre Sicherheitsmodelle, -mechanismen und -technologien, die die Zusammenarbeit einer Vielzahl an Systemen in einer plattform- und sprachunabhängigen Art und Weise ermöglichen sollen. Mit WS-Security werden keine neuen Verfahren entwickelt, sondern bestehende Techniken zusammengefasst.

WS-Security erweitert SOAP (siehe *3.4.4.2.3 SOAP*) um Sicherheitsaspekte, in dem es Verschlüsselungs- und Signaturfunktionen, die auf XML-Encryption[752] und XML-Signature[753] basieren, integriert. Dabei beschreibt WS-Security wie die in XML-Encryption und XML-Signature definierten Kopfzeilen zur Gewährleistung der Integrität, Vertraulichkeit und Authentizität der Nachrichten (siehe *1.2.2 Anforderungen an die Informationssicherheit*) im Kopfzeilenbereich der SOAP-Nachrichten eingefügt werden können. WS-Security unterstützt die Anwendung von elektronischen Signaturen, indem es zulässt, dass jede einzelne SOAP-Kopfzeile und der eigentliche Inhalt der Nachricht unabhängig voneinander digital signiert werden können. Somit können – je nach Bedarf – Signaturen zwischen zwei Endpunkten individuell hinzugefügt werden.

Ausgearbeitet wurde WS-Security von Microsoft, IBM und *Verisign*[754] und wird nunmehr von OASIS weiterentwickelt (Anm.: die aktuelle Version 1.1 wurde im Feber 2006 freigegeben[755]).

Das Konzept von WS-Security ist so ausgelegt, dass eine breite Palette von Sicherheitsmodellen wie SSL (siehe *1.3.4.2.5 SSL/TLS-Sicherheit*), SAML (siehe *3.4.4.2.6 SAML*), Kerberos oder PKI (siehe *1.7.2.1.5 Public Key Infrastructure*) einsetzbar werden. WS-Security bietet auch genügend Raum für Erweiterungen, die bei speziellen Anforderungen helfen können: *WS-Policy* beschreibt Sicherheitsvorkehrungen und Einschränkungen, *WS-Trust* ist ein Framework für Vertrauensmodelle, *WS-Privacy* enthält Datenschutzwünsche, *WS-Secure-Conversation* behandelt die sichere Kommunikation, *WS-Federation* beschäftigt sich mit Vertrauensverhältnissen in heterogenen Umgebungen und *WS-Authorization* handelt von Autorisierungsdaten und -richtlinien.

Etablierte Standards wie Verschlüsselungsverfahren bilden eine solide Grundlage für den Aufbau von Web Service-Architekturen. Dank der Erweiterbarkeit von XML ist es gelungen, das bislang unsichere

[752] Die XML-Encryption definiert eine Reihe von Möglichkeiten, wie XML-Dokumente ver- und entschlüsselt werden. Die Palette reicht von Verschlüsselung des gesamten XML-Dokuments über Verschlüsselung eines einzelnen Elementes und seiner Unterelemente bis zur Verschlüsselung für mehrere Empfänger.
http://www.w3.org/Encryption/2001/ [1. September 2007]

[753] XML-Signature definiert eine XML-Schreibweise für elektronische Signaturen. Sie findet Einsatz in Web-Standards wie etwa SOAP oder SAML. Mit XML-Signaturen können Daten jedes Typs signiert werden, sofern sie in das XML-Dokument der Signatur integrierbar sind (enveloped signature) oder mit einer URL adressierbar sind (detached signature).
http://www.w3.org/Signature/ [1. September 2007]

[754] http://www.verisign.com/ [27. August 2007]

[755] Vgl. http://www.oasis-open.org/specs/index.php#wssv1.1 [27. August 2007]

SOAP um wirksame Sicherheitsmaßnahmen zu ergänzen. Standards wie SAML und vor allem WS-Security können nahtlos in bestehende Informationssicherheitsstrukturen integriert werden[756].

3.4.4.2.6 SAML

SAML (steht für: *Security Assertion Markup Language*)[757] ist eine XML-basierte Auszeichnungssprache zur Beschreibung von Sicherheitsinformationen (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*). Sie liefert einen Rahmen für die Definition von Autorisierungen, Authentifizierungen, Berechtigungen und Profilinformationen in XML-Dokumenten. Dies geschieht in Form von sogenannten *Security Assertions*, die Benutzern, Anwendungen oder einem Web Service zugewiesen und in LDAP-Verzeichnissen (siehe *3.4.1 Verzeichnistechnologien*) verwaltet werden. Mit SAML können insbesondere Single-Sign-On-Systeme (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) realisiert werden, zudem ist sie für verteilte Transaktionen geeignet, wo mehrere Benutzer gemeinsam an einer Transaktion arbeiten und sich die Sicherheitsinformationen teilen. Die Vertrauenswürdigkeit der SAML-Informationen ist abhängig von der Vertrauenswürdigkeit des Übermittlers (z. B.: Portals).

Eine der Stärken von SAML ist der hohe Grad an Interoperabilität mit beliebigen Sicherheitssystemen. SAML unterstützt viele Systeme, beginnend mit Passwörtern über Public Keys (siehe *1.7.2.1.5 Public Key Infrastructure*) bis hin zu Zertifikaten (*1.7.2.1.6 Digitale Zertifikate*). SAML hat auch die Unterstützung für XML-Signatures (siehe *3.4.4.2.5 WS-Security*) eingebaut, womit es nicht nur für Autorisierung und Authentifizierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*), sondern auch für Gewährleistung der Integrität und Verbindlichkeit (siehe *1.2.2 Anforderungen an die Informationssicherheit*) von Nachrichten verwendet werden kann[758].

3.4.4.2.7 SPML

Provisioning ist die Automatisierung von Schritten zum Anlegen, Ändern und Löschen von digitalen Identitäten oder Benutzerberechtigungen (siehe *2.2.1.1 Lebenszyklus einer Identität*, *3.4.2.4 Provisioning und Reporting*). *Service Provisioning Markup Language* (kurz: *SPML*) ist ein dafür vorgesehenes XML-basiertes Framework, entwickelt von OASIS (Anm.: aktuelle Version ist 2.0[759]), für den Austausch von Benutzer-, Ressourcen- und Provisionierungs-Informationen zwischen kooperierenden Organisationen.

Das Ziel von SPML ist es, Organisationen die schnelle und sichere Erstellung von Benutzerschnittstellen für Web Services zu ermöglichen ohne an proprietäre Lösungen gebunden sein zu müssen. Dies wird dadurch erreicht, dass SPML Plattformen wie Webportalen oder

[756] Vgl. http://www.tecchannel.de/webtechnik/soa/479383/ [27. August 2007]
[757] http://www.oasis-open.org/specs/index.php#samlv2.0 [2. September 2007]
[758] Vgl. http://www.tecchannel.de/webtechnik/soa/479383/index8.html [2. September 2007]

Applikationsservern ermöglicht, interne wie unternehmensübergreifende Provisionierungsanfragen zu generieren[760].

3.4.4.2.8 SOA

Geschäft und IT wachsen immer enger zusammen und müssen exakt aufeinander abgestimmt sein. Verändern sich kurzfristig die Marktgegebenheiten und Geschäftsziele, muss die IT unmittelbar darauf reagieren können. Eine reine Unterstützung der Abläufe und Prozesse ist zu wenig – die IT muss einen nachweislichen Beitrag zum Geschäftserfolg leisten.

SOA[761] (steht für: *Service Oriented Architecture*) ist ein Rahmenwerk für die Integration von Geschäftsprozessen und unterstützender IT-Infrastruktur in Form von sicheren, standardisierten Komponenten (*Services*[762]), die sich wiederverwenden und kombinieren lassen, um wechselnde Geschäftsanforderungen abzubilden. SOA lässt sich als Strategie auffassen, die darauf zielt, alle Softwareteile eines Unternehmens gemäß der Service-orientierten Programmiermethode zu entwickeln. Im SOA-Rahmenwerk lassen sich Softwareservices erstellen, verwalten und kombinieren. Services können beispielsweise über Webtechnologien miteinander verknüpft werden. Methodik und Technik sind standardisiert über Vereinbarungen des *OASIS*[763]-Konsortiums. Dadurch werden die Verbreitung und Unterstützung durch die tragenden Unternehmen der IT-Branche (HP, IBM, Microsoft, Oracle, SAP, Sun etc.) gewährleistet. Weil Services mehrfach verwendet werden können, verspricht SOA Kostenvorteile.

Durch SOA ergeben sich vielfältige Anwendungsmöglichkeiten, die für sich alleine genommen oft aufwendig in der Umsetzung sind, durch Standardisierung von Schnittstellen und Kommunikation in einer bereits vorhandenen Umgebung neue und effiziente Möglichkeiten eröffnen[764]:

- Umfangreichere und flexiblere Nutzung vorhandener Investitionen (Datenaustausch mit Altsystemen, Migrationen etc.),

---

[759] Vgl. http://www.oasis-open.org/specs/index.php#spmlv2.0 [27. Oktober 2007]
[760] Vgl. http://www.iam-wiki.org/SPML?highlight=%28spml%29 [27. Oktober 2007]
[761] Vgl. http://www.service-architecture.com/web-services/articles/service-oriented_architecture_soa_definition.html [9. August 2007];
http://www.cio.de/knowledgecenter/soa/832511/index.html [9. August 2007];
http://www.tecchannel.de/webtechnik/soa/569662/ [9. August 2007]
[762] Services sind in diesem Zusammenhang als Softwarekomponenten zu verstehen, die so konstruiert sind, dass sie sich auf einfache Weise mit anderen Softwarekomponenten verbinden lassen. Die Idee dahinter ist, dass Software in Services dargestellt werden soll, die nicht nur für Programmierer sondern auch für Mitarbeiter aus Fachabteilungen verständlich sind.
[763] OASIS ist ein globales Konsortium, das die Entwicklung, Konvergenz und laufende Anpassung von Standards im E-Business vorantreibt. Zudem werden Themen wie E-Government oder Gesundheitswesen auf Basis von XML- und Web-Services-Standards diskutiert. Namhafte Organisationen wie IBM, Microsoft, Oracle, SAP oder Airbus sind Mitglieder bei OASIS. http://www.oasis-open.org/ [9. August 2007]
[764] Vgl. http://www.computerwoche.de/soa-expertenrat/ [2. September 2007]; http://www.service-architecture.com/ [2. September 2007]; http://www.informationweek.de/soa/ [2. September 2007]

- Verknüpfung unternehmensweiter Datensammlung (Compliance-Ansprüche, Identitätsmanagement, CRM etc.),
- Geschäftsprozess-Orientierung zur Marktausrichtung,
- Portale.

Bei der Abbildung von Geschäfts- in IT-Prozesse darf der Sicherheitsaspekt nicht außer Acht gelassen werden. Identitätsmanagement kann mit dem in diesem Zusammenhang wichtigen Baustein Identitätsföderation (*3.2.3 Identitätsföderation und -kontrolle*) einen wesentlichen Beitrag leisten. Identitätsmanagement muss sich selbst als Satz von Services verstehen, um eine moderne Anwendungswelt optimal zu unterstützen[765].

Web Oriented Architecture (kurz: *WOA*) ist ein sich derzeit etablierender Begriff, wobei „*the only real difference between traditional SOA and the concept of WOA is that WOA advocates REST* (siehe *3.4.4.2.4 REST und AJAX*)*, an increasingly popular, powerful, and simple method of leveraging HTTP as a Web service in its own right*“[766].

Das Ziel ist eine an Geschäftsprozessen ausgerichtete IT-Infrastruktur, die schnell auf veränderte Anforderungen reagiert.

3.4.4.2.9 User Interface

Die Akzeptanz eines Identitätsmanagementsystems (siehe *3.5.4.2.1 Stakeholder, 3.5.4.3.3 Usability*) steht in engem Zusammenhang mit der Gestaltung der Benutzeroberfläche (engl. *User Interface* (kurz: *UI*)). Ein IMS soll in einer weitgehend automatisierten Umgebung „*zur Formung und Beobachtung von Kommunikation helfen*“, dass der einzelne Benutzer sein Recht auf informationelle Selbstbestimmung (siehe *3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*) in Anspruch nehmen kann. Solche Systeme „*nötigen dem einzelnen PC-Benutzer eine Technisierung sämtlicher Kommunikation auf*“[767]. Das UI muss die Komplexität eines IMS für einen nicht-professionellen Benutzer intuitiv zugänglich und einfach nutzbar machen. Deshalb sollte die Benutzeroberfläche auf Erfahrungen und Abbildern aus der realen Welt aufbauen. Die Benutzeroberfläche muss die Sicherheit des Identitätsmanagementsystems in verständlicher Weise widerspiegeln, da der Benutzer die Sicherheitsmechanismen des IMS nicht überprüfen und einschätzen kann. Die Benutzungsoberfläche darf zudem keine Sicherheit vortäuschen, die das System nicht bietet [Jendricke, 2001, S 3].

Der zunehmenden Mobilität wird beispielsweise mit einem Forschungsprojekt namens *Identity Service*[768] Rechnung getragen. Identity Service ist ein interaktives, mobiles Interface, das dem

[765] Vgl. http://www.kuppingercole.de/events/eic2007 [2. September 2007]
[766] Vgl. http://blogs.zdnet.com/Hinchcliffe/?p=27 [7. Jänner 2007]
[767] Vgl. http://www.maroki.de/pub/privacy/tm.html [13. November 2007]
[768] http://www.cutecircuit.com/now/projects/telecom-and-services/identity-service/ [13. November 2007]

Benutzer ermöglichen soll, unterwegs über mobile Endgeräte auf alle denkbaren persönlichen Informationen zuzugreifen, sowie mit Partnern (Einzelpersonen, Unternehmen etc.) zu interagieren.

3.5 IDENTITÄTSMANAGEMENT IM BETRIEBLICHEN UMFELD

Die folgenden Ausführungen verbinden theoretisches Wissen mit den praktischen Erfahrungen des Autors. Um den Praxisbezug zu verstärken, sind zudem die Ergebnisse der „Identity Management 2007"-Studie [Deron, 2007] in den Ausführungen eingearbeitet. Deron hat mit Unterstützung des Fraunhofer Instituts und einiger Universitäten eine repräsentative Datenerhebung (Anm.: der Autor hat für seine Organisation die Daten erhoben und geliefert) im deutschen Sprachraum bezüglich Identitätsmanagementsystemen durchgeführt.

3.5.1 ANFORDERUNGEN UND NUTZEN AUS MITARBEITERSICHT

Die Folge der Heterogenisierung der IT-Infrastrukturen ist ein Ansteigen der Zahl an Systemen. Betriebssysteme, Applikationen und Portale haben ihre jeweils eigenen Authentifikationsmechanismen und Credentials. Dies belastet den Anwender (siehe *3.5.4.2.1 Stakeholder*) mit einer größer werdenden Anzahl an Benutzernamen und Passwörtern. Die Mitarbeiter benötigen orts- und zeitungebunden Zugriff auf interne Ressourcen. Im Arbeitsalltag verlangen die Mitarbeiter unter Produktivitätsdruck, dass fachliche Änderungen IT-technisch schnell nachgezogen werden.

Für den Mitarbeiter ergeben sich aus dem Einsatz eines Identitätsmanagementsystems folgende Vorteile:

- eine einzige Identität für viele Applikationen und Ressourcen in Form eines Benutzernamens und eines Passworts (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*),
- starke Authentifizierung bei einfacher Handhabung (siehe *1.7.2.3 Biometrie, 1.7.2.5 Graphisches Passwort, 2.2.6 Autorisierung, Authentifizierung und Authentizität, 3.4.2.3 Chipkarten*),
- Hoheit über die persönlichen Daten (*3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*),
- schneller Zugang zu IT-Ressourcen (siehe *3.4.2.4 Provisioning und Reporting*),
- Möglichkeit, *sich selbst helfen zu können* (siehe *3.4.2.5 Self Service*),
- Schutz vor Überwachung und Verwendung von Pseudonymen (siehe *2.3.4 Exkurs: Privacyaspekte für den betrieblichen User, 2.2.2 Pseudonymität*).

Während für den Benutzer der Komfort und die Datenhoheit im Vordergrund stehen, gilt es für den IT-Administrator (Anm.: ist für den Autor aufgrund seiner beruflichen Tätigkeit eine wichtiger Aspekt), neben Produktivitätsvorgaben und Zeitersparnis Selbstschutzmaßnahmen setzen zu können. Beim Management einer Identität – vor allem bei der Rechtevergabe – und beim Auftreten von

System-Anomalien ist es wesentlich, das „Vieraugenprinzip“ (siehe *3.6.2 Aufteilung der Verwaltung* der Benutzerdaten) zu beachten. Wesentlich aus Sicht der Systemverwaltung ist:

- die Protokollierung (siehe *3.4.2.4 Provisioning und Reporting, 3.4.3 Auditing*),
- ein hoher Grad an Automatismus (siehe *3.4.2.4 Provisioning und Reporting, 3.4.4 Portale und Web Services*),
- die Verwendung anonymisierter Daten (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz*).

Für die Mitarbeiter in der Personalverwaltung ergibt sich aus dem Einsatz eines IMS eine Zeitersparnis in den Verwaltungsarbeiten der Mitarbeiterdaten und eine Absicherung im Sinne der Nachweisbarkeit von Datenmanipulationen (siehe *3.4.2.4 Provisioning und Reporting, 3.4.3 Auditing)*.

Für Führungskräfte geht es in erster Linie darum, fundierte Grundlagen für Entscheidungen schnell zur Verfügung zu haben (siehe *1.8 Unternehmenssicherheit, 3.4.2.4 Provisioning und Reporting, 3.4.2.5 Self Service*) und um die Einhaltung gesetzlicher Vorgaben (siehe *1.7.3.1 Datenschutz, 1.7.3.2 Arbeitsrechtliche Grundlagen der Informationssicherheit in Unternehmen, 1.7.3.2.1 Mitwirkung des Betriebsrates, 1.7.3.2.2 Personalinformationssysteme, 1.7.3.2.3 Haftung und Schadenersatz, 2.3.2.2 Zusammenhang von Identitätsmanagement und Datenschutz, 3.4.3 Auditing, 3.5.2.1 Gesetze, Regulative, Compliance*). Beides kann durch Funktionalitäten eines Identitätsmanagementsystems bedient werden.

3.5.2 ANFORDERUNGEN, NUTZEN UND TREIBENDE FAKTOREN AUS UNTERNEHMENSSICHT

Neben den traditionellen Informationssicherheitsbedrohungen sind in jüngster Zeit neue Risikoszenarien für die Organisationen entstanden, ausgelöst durch die zunehmende Integration von Unternehmensprozessen sowie die Anbindung externer Partner und Kunden an bislang geschlossene interne IT-Systeme (siehe *3.2.3 Identitätsföderation und -kontrolle*). Diese Anforderungen lassen sich angesichts einer immer komplexeren Anwendungs- und Systemlandschaft nur dann sicher und flexibel realisieren, wenn alle Komponenten auf gemeinsame Identitäten zugreifen können. Die Grenzen zwischen innerer und äußerer Welt der User verschwinden. Es gibt gestiegene Anforderungen an ein systemübergreifendes Reporting sowie verschärfte Compliance-Anforderungen[769]. Die Integration von Identitäten ist Voraussetzung, wenn die IT den Business-Anforderungen des Unternehmens gerecht werden soll.

[769] Vgl. http://www.digitalidworld.de/agenda.php [18. November 2007]

Eine Sicherheitsstudie[770] von CA (Sommer 2006) belegt die zentrale Rolle des Identitätsmanagements für Unternehmen. Rund vier Fünftel der Befragten betrachten unsichere Kennwörter (90 Prozent), mangelnde Nachvollziehbarkeit von Zugriffsberechtigungen (85 Prozent), nicht gelöschte Benutzerkonten ehemaliger Mitarbeiter (80 Prozent) sowie nicht konsistente Zugriffsbedingungen (80 Prozent) als wichtige Informationssicherheitsproblematiken im Unternehmen (siehe *1.8 Unternehmenssicherheit*).

Ohne funktionierendes Identitätsmanagement lassen sich steigende Effizienz und sinkende Kosten, die durch die Vernetzung der Wirtschaft und einzelner Unternehmen ausgelöst worden sind, nicht realisieren. Andererseits eröffnen sich durch professionelles Identity Management neue Chancen in der Optimierung von Kundenbeziehungen und Geschäftsprozessen[771].

Die Vorteile aus dem Einsatz eines Identitätsmanagementsystems aus Sicht des Unternehmens bzw. deren Verantwortlichen (Anm.: variabler Gehaltsanteil abhängig von Verkaufserfolg und Kosteneffizienz) werden im Folgenden dargestellt.

3.5.2.1 Gesetze, Regulative, Compliance

Unternehmen stehen aufgrund von Gesetzen und Regulativen (siehe *1.8.4.3 Gesetze und Vorschriften*) zunehmend mehr in der Pflicht, Informationen, Transaktionen und Geschäftsgebarung nachweislich festzuhalten. Die Auflagen richten sich in zweierlei Hinsicht auf Daten: Persönlicher Datenschutz und finanzielle Gültigkeit. Die wichtigste Anforderung nahezu aller sicherheitsbezogenen Auflagen schließt die Erstellung strikter interner Kontrollen ein. Das bedeutet, dass alle Benutzer eindeutig identifiziert und alle ihre Zugriffe auf geschützte Ressourcen kontrolliert werden müssen. Der Zugriff auf diese Ressourcen muss auf einer definierten Sicherheitsrichtlinie (siehe *1.8.2.5 Umsetzung des IT-Sicherheitsplans*) basieren [CA, 2005-1, 4f]. Mittels Identitätsmanagementsysteme lassen sich durch transparente Rechtevergabe, Reporting- und Auditing-Funktionen (siehe *3.4.2.4 Provisioning und Reporting, 3.4.3 Auditing*) die regulativen Anforderungen erfüllen. Ohne IMS ist es für die Unternehmen ein erheblicher Aufwand, die aktuellen und vergangenen Berechtigungen festzustellen. Nur 8 Prozent können Änderungen in allen, 76 Prozent in einigen und 16 Prozent in keinen Anwendungen und Systemen nachvollziehen [Deron, 2007, S 51].

Gartner[772] bestätigt: „*Identity management systems can improve overall security and privacy while providing an audit trail to meet the requirements of the Health Insurance Portability and Accountability Act or the Sarbanes-Oxley Act. Because of that, compliance issues are driving identity projects that couldn't be justified by return on investment alone. Without an identity management*

[770] Vgl. http://www.compliancemagazin.de/markt/studien/ca151106.html [18. November 2007]
[771] Vgl. http://www.kuppingercole.de/pages/about/fid=12 [18. November 2007]
[772] Vgl. http://www.computerworlduk.com/technology/security-products/authentication/in-depth/index.cfm?articleid=139 [8. Dezember 2007]

infrastructure, organizations are finding that it's either very painful to produce compliance reports, or they can't do it at all".

3.5.2.2 Produktivität und Kosten

Der Kostendruck auf die Unternehmen und damit auch auf die IT nimmt zu. Wesentliche Fixkosten sind in erster Linie Systemverwaltung und *Helpdesk*. Ein Produktivitätsverlust, der auf die Notwendigkeit des Einsatzes unterschiedlicher Anwendungen zurückzuführen ist, bedeutet für viele Organisationen Kosten in beträchtlicher Höhe. Diese Kosten steigen weiter an, wenn aufgrund von Anomalien Benutzerberechtigungen *verloren gehen*, Konten gesperrt werden und Lizenzen brach liegen. Darüber hinaus ist manuelles Provisioning ineffizient und teuer. Bei Unternehmensgrößen ab 1.000 Mitarbeitern nimmt die Komplexität der Account-Verwaltung exponentiell zu [Deron, 2007, S 14f]. Neue Benutzer müssen oft tagelang warten bis ihre Konten und Zugriffe eingerichtet sind, wodurch Zeit verloren geht und die Produktivität verringert wird. Der durchschnittliche Zeitaufwand zum Anlegen eines neuen Mitarbeiterkontos kann durch den Einsatz eines Identitätsmanagementsystem um bis zu 49 Prozent reduziert werden [Deron, 2007, S 20]. Dazu kommt, dass durch ein IMS mehrere Accounts eines Anwenders pro System verhindert werden können [Deron, 2007, S 23]. Für das Management des Identitätslebenszyklus ist eine Verbesserung gegenüber monolithischen Applikationen von bis zu 40 Prozent erhoben worden [Deron, 2007, S 44].
In Summe kann sich durch den Einsatz eines Identitätsmanagementsystems in den entsprechenden Bereichen ein Einsparungspotenzial von bis zu 63 Prozent ergeben [Deron, 2007, S 57]. Durch Zentralisierung, Verminderung der Datenredundanzen und der damit verbundenen Verbesserung der Qualität und Aktualität der Daten sowie der Verteilung bzw. Automatisierung administrativer Aufgaben und *Selbstbedienung* der Benutzer („*Health First rolled out a password self-service application that cut help desk calls from more than 6,683 to 534 a year.*"[773]) sind Effizienzgewinne beim laufenden Betrieb und den Infrastrukturkosten zu erzielen.
Auf den ersten Blick kann die Beschaffung eines Identitätsmanagementsystems teuer erscheinen. Werden jedoch das Potenzial für die Optimierung von Prozessen, der reduzierte Administrationsaufwand und die Compliance-Anforderungen gegenübergestellt, wird ersichtlich, dass ein Identitätsmanagementsystem zum einen Teil Lösung bzw. Service ist, zum anderen Teil zwingende Infrastrukturmaßnahme [IT-Research, 2005, S 14]. Gartner[774] formuliert es folgendermaßen: „*Deployments can be costly and complexity increases with the size of the organization. IT executives should expect to pay $20 to $30 per user for the software and two to six times that amount on integration. A centralized identity management infrastructure is foundational for*

[773] Vgl. http://www.computerworlduk.com/technology/security-products/authentication/in-depth/index.cfm?articleid=139 [8. Dezember 2007]

projects that can cut administrative costs and increase productivity. The systems can reduce replication of administrative tasks by allowing identity information to be updated in one repository and propagated out to all others. User provisioning tasks can be automated or delegated to others. Self-service initiatives, such as automating the password-reset process, can cut down on help desk calls."

Beim Beschaffungsvorgang eines Identitätsmanagementsystems ist es wichtig, die *Total Cost of Ownership* (kurz: *TCO*)[775] im Blick zu haben. Unternehmen können ihre Kosten für den Support der eingesetzten IT-Lösungen signifikant reduzieren, wenn standardisierte Konfigurationen verwendet werden. Sobald die Anzahl von unterschiedlichen Konfigurationen steigt, können sich neben den Ausfallsraten für wichtige Applikationen auch die Kosten für die Wartung mehr als verdoppeln. Die Kosteneinsparungen werden dann sichtbar, wenn in der TCO-Analyse mehrere Szenarien verglichen werden[776].

Eine Entscheidungshilfe stellt die Return On Security Invest-Berechnung (siehe *1.8.5 Kommerzieller Aspekt*) dar. Die IDC-Studie „*Demonstrating Return on Investment with Enterprise-Class Identity and Access Management Technology*"[777] vom November 2007 bestätigt die Wirtschaftlichkeit eines IMS. Im Schnitt sparen die in der Studie befragten Unternehmen jährlich 40.000 Euro pro hundert Benutzer ein. Im Vergleich zu den Investitionen, die die Befragten im Laufe der dreijährigen IMS-Projektphase eingesetzt haben, ergeben sich für diesen Zeitraum Nettoeinsparungen von mehr als 75.000 Euro pro hundert Benutzer. Die Investitionen in eine IMS-Lösung amortisieren sich bereits nach 6,3 Monaten, der durchschnittliche ROSI beträgt 358 Prozent.

3.5.2.3 Prozessoptimierung und Einhaltung von Service Level Agreements

Vielen Unternehmen geht es darum, Kunden und Partner auf der ganzen Welt zu erreichen. Die dazu notwendige Abstimmung der Prozesskette setzt eine elektronische Vernetzung voraus (siehe *3.2.3 Identitätsföderation und -kontrolle, 3.4.4 Portale und Web Services*). Ebenso führt die Spezialisierung der Unternehmen zu produktiven Partnerschaften, die ohne Datenabgleich keinen langen Bestand haben können. Viele Hersteller haben das *Just-in-Time*-Modell soweit perfektioniert, dass ein großer

[774] Vgl. http://www.computerworlduk.com/technology/security-products/authentication/in-depth/index.cfm?articleid=139 [8. Dezember 2007]
[775] Unter TCO werden die Gesamtkosten für eine technische Einrichtung unter Berücksichtigung aller direkten (z. B.: Hard- und Software-, Betriebs-, Verwaltungskosten) und indirekten Kosten (z. B.: Schulungen, Nicht-Verfügbarkeit des betrachteten Systems, etc.) über die Nutzungszeit verstanden.
[776] Vgl. http://www.commercemanager.de/magazin/artikel_1339_tco_total_cost_ownership_wirtschaftlichkeit.html [21. November 2007]
[777] Vgl. http://www.computerwelt.at/detailArticle.asp?a=113976&n=2 [20. Jänner 2008]

Teil des Lagerbestandes am Transportweg ist. Nur mit einer engen Daten-Beziehung zu den Lieferanten lassen sich diese Modelle noch weiter entwickeln[778].

Die Einhaltung von *Service Level Agreements* (kurz: *SLA*s) (siehe *1.2.2 Anforderungen an die Informationssicherheit: Verfügbarkeit*) und die damit verbundene Vertragstreue ist ein wichtiges Element von Partnerschaften. Identity Management sorgt für eine personalisierte, an die Identität des Benutzers gebundene Verfügbarkeit von Daten, Programmen und Speicherplatz.

3.5.2.4 Interoperabilität, Flexibilität und Entwicklungspotenzial

Immer mehr Organisationen verwenden Webanwendungen als Bausteine zur Entwicklung komplexer und anspruchsvoller Geschäftsprozesse (siehe *3.4.4.2.8 SOA*). Dadurch entstehen neue Anforderungen an eine nahtlose Zusammenarbeit von Anwendungen einschließlich des gemeinsamen Zugriffs auf Autorisierungs- und Authentifizierungsmaßnahmen, der Konsistenzerhaltung von Identitätsinformationen während der Prozesse und der Fähigkeit, alle Aspekte des Geschäftsbetriebs zu überwachen und zu prüfen. Dies hat sich bis hin zu organisationsübergreifenden Verbindungen zwischen Geschäftspartnern (siehe *3.2.3 Identitätsföderation und -kontrolle*) ausgeweitet.

Technologieanbieter haben diese Erfordernisse erkannt und mit Ansätzen für neue Standards in Bezug auf Identitäten, Provisionierung, Zugriffssteuerung und Web Services reagiert. Dennoch besteht im Hinblick auf diese Standards noch keine vollständige Übereinstimmung. Das IT-Management sieht sich daher bei diesbezüglichen Entscheidungen gezwungen, zwischen konkurrierenden Standards zu wählen und sich sogar die Grundfrage stellen zu müssen, welche Standards befolgt werden sollten.

Die Flexibilität und Agilität eines Unternehmens [Mezler-Andelberg, 2007, S 181] wird durch das Provisioning (siehe *3.4.2.4 Provisioning und Reporting*) von Benutzerkonten und -rechten in Echtzeit, selbst organisationsübergreifend, erhöht. Identitätsmanagementsysteme offerieren ein Framework für die rasche Entwicklung neuer Web Services ohne den dafür typischen Entwicklungsoverhead [CA, 2005-1, S 5].

3.5.2.5 Informationssicherheit

Unternehmen erfahren eine enorme Zunahme unternehmenskritischer Ressourcen – von integrierten ERP- bis hin zu E-Mail-Systemen, Portalen und mobilen Anwendungen. Diese Ressourcen können sich auf unterschiedlichen Plattformen (Mainframe, Unix, Linux, Windows etc.) befinden, hinzu kommt eine komplexe Infrastruktur aus Web-, Anwendungsservern und Integrationsplattformen. Kunden, Partner und Mitarbeiter erwarten von Organisationen, dass ihre persönlichen Daten und Transaktionen vertraulich (siehe *1.2.2 Anforderungen an die Informationssicherheit: Vertraulichkeit*) behandelt werden. Die Daten und Prozesse der Organisationen sind aufgrund unzureichender

[778] Vgl. http://www.compliancemagazin.de/markt/kommentare/einfuehrungnovell161107.html [20. November 2007]

Unternehmenssicherheit (siehe *1.8 Unternehmenssicherheit*) und zunehmend raffinierter werdender Angriffe größeren Gefahren (siehe *1.3 Taxonomie von Angriffen auf den Wert Information*) ausgesetzt als je zuvor. Unternehmen benötigen die Gewissheit, dass der Zugriff auf ihre Ressourcen ausschließlich autorisierten Benutzern gewährt wird. Bezogen auf Identitätsmanagement bedeutet das Sicherheitsregelungen, Autorisierung, Authentifizierung und Zugriffskontrolle. Die zentrale Rolle von Identity Management zeigt sich etwa bei Einstellungen und Entlassungen. Mitarbeiter sind in wenigen Minuten in allen notwendigen Systemen eingerichtet und bekannt, aber auch in wenigen Minuten gesperrt – ohne dass ein System vergessen werden kann (siehe *3.4.2.4 Provisioning und Reporting*). Mit bis zu 25 Prozent ist der Anteil derer, die sich bei der Genehmigungserteilung ohne Einbindung des Vorgesetzten nur auf den Administrator verlassen und ihm die operative Verantwortung übertragen, zu hoch. Durch ein Identitätsmanagementsystem wird der Prozess „Vorgesetzter genehmigt, Administrator führt aus“ unterstützt, damit verbleibt die Verantwortung bei der übergeordneten Instanz [Deron, 2007, S 32].

Während nur 69 Prozent der befragten Unternehmen regelmäßig (alle 12 Wochen) die Passwörter ändern lassen, erhöht sich durch die einfachere Handhabe mittels IMS dieser Anteil um 10 auf knapp 80 Prozent [Deron, 2007, S 35]. Durch den Einsatz eines Identitätsmanagementsystems lässt sich der Prozentsatz an „Karteileichen“ von 22 auf nahezu 0 reduzieren [Deron, 2007, S 45]. *Dan Tesenair*[779] bringt es auf den Punkt: „*The problem is that as people change roles, they gain cumulative access to the various systems. We're very good at getting people what they need, but we're very poor at taking it away*“.

Identitätsmanagementsysteme erlauben eine fein granulierte Rechtevergabe (siehe *3.4.2.2 DRM-Funktion*) auf Basis von integeren, geschützten Daten (siehe *1.2.2 Anforderungen an die Informationssicherheit: Integrität*, siehe *1.7.2.1 Kryptologie*). Eine starke Authentifizierung und eine Erhöhung der Login-Sicherheit (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) wird mittels Zertifikaten (siehe *1.7.2.1.6 Digitale Zertifikate*), Chipkarten (siehe *3.4.2.3 Chipkarten*) oder biometrischen Geräten (siehe *1.7.2.3 Biometrie*) ermöglicht. Fehleranalysen oder das Erkennen von Anomalien werden durch das lückenlose Logging (siehe *3.4.3 Auditing*) ermöglicht [CA, 2005-1, S 5].

In Summe kann durch den Einsatz eines IMS eine deutliche Steigerung der Unternehmenssicherheit vor allem in den Funktionen Access-Management (83 Prozent, siehe *3.4.2 Access-Management und Technologien zur Autorisierung und Authentifizierung*), Passwort-Management (73 Prozent, siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) und Metadirectory (56 Prozent, siehe *3.4.1.2 Metadirectory und Virtuelles Verzeichnis*) erreicht werden [Doubleslash, 2006, S 13f].

[779] Vgl. http://www.computerworlduk.com/technology/security-products/authentication/in-depth/index.cfm?articleid=139 [8. Dezember 2007]

3.5.3 PRAXISBEISPIEL: IDENTITÄTSMANAGEMENT FÜR BEHÖRDEN IN FORM DES PORTALVERBUNDS

Die EU-Initiative „*i2010 – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung*“[780] und der im April 2006 beschlossene *Aktionsplan E-Government*[781] geben den Mitgliedsstaaten eine Orientierungshilfe zum weiteren Ausbau elektronischer Behördendienste in Europa. Die Ziele umfassen neben der Zufriedenheit der Benutzer mit Online-Services, der Verringerung des Verwaltungsaufwandes für Bürger respektive Unternehmen und die Einbeziehung aller Bevölkerungsteile ein einheitliches Identitätsmanagement.

An dieser Stelle kann auf die Ausführungen bezüglich E-Government in vorigen Kapiteln angeknüpft werden. Dabei wurde zum einen die Problematik hinsichtlich des Nachweises der Identität und der hohen Anforderungen an den Datenschutz im Bereich E-Government dargestellt (siehe *2.3.3.1.1 E-Government*), zum anderen Lösungen in Form des bereichsspezifischen Personenkennzeichens und der Bürgerkarte erläutert (siehe *2.4.7 Bereichsspezifisches Personenkennzeichen und Bürgerkarte im E-Government*). Für die Durchgängigkeit der E-Services müssen die Abläufe und technischen Voraussetzungen behördenintern vorhanden und aufeinander abgestimmt sein. Im Folgenden wird daher mit dem *Portalverbund* (kurz: *PV*) eine Form des Identitätsmanagements beschrieben, die im Backoffice-Bereich eine Grundlage für ein behördenübergreifendes Arbeiten mittels Webportal ermöglicht. Ein nächster möglicher Schritt wäre der Ausbau des Portalverbundsystems in Richtung umfassendes Identitätsmanagementsystem bei gleichzeitiger Stärkung der informationellen Selbstbestimmung (siehe *3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*).

3.5.3.1 Anforderungen und Situation

Die Bestrebung der öffentlichen Hand ist, alle sogenannten Behördenapplikationen (Zentrales Melderegister, Zentrales Vereinsregister, Führerscheinregister etc.) von diversen proprietären Plattformen auf Webbasis zu portieren, um eine effiziente, behördenübergreifende Zusammenarbeit via Portal zu ermöglichen. Der Autor ist in einem Unternehmen im öffentlichen Umfeld mit der Aufgabenstellung konfrontiert, diese webbasierte Kooperation zu etablieren. Den internen Mitarbeitern sollen über ein zentrales Webinterface die unterschiedlichen Anwendungen der verschiedenen Institutionen zugänglich gemacht werden. Da es dabei vielfach um personenbezogene Daten handelt, ist eine entsprechende Informationssicherheitsinfrastruktur erforderlich. Dazu gehört eine Berechtigungsstruktur, welche sowohl den hausinternen als auch den externen Anforderungen entsprechen muss. Für jede Applikation gibt es verschiedene Berechtigungsparameter, die für Mitarbeiter mit unterschiedlichen Rollen (siehe *3.6.3 Von der Identität zur Rolle*) zu vergeben sind. Zudem ist es erforderlich, dass alle vom Benutzer getätigten Aktivitäten in einer Applikation

[780] http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm [6. August 2007]
[781] http://europa.eu/scadplus/leg/de/lvb/l24226j.htm [6. August 2007]

nachvollziehbar dokumentiert werden. Nicht zuletzt muss auf die Benutzerfreundlichkeit Bedacht genommen werden, da die Bedienung der Anwendungen verschieden ist.

Das Besondere bei der Portalverbund-Lösung ist die Delegierung der Rechte vom Applikationsbetreiber an den Kunden. Damit wird dem Kunden auch die Verantwortung übertragen. Wer welche Rechte bekommt und deren Kontrolle obliegt dem Kunden. Die IT des Kunden hat die Infrastruktur bereitzustellen (siehe *3.5.4.3 Technische Maßnahmen*): LDAP-Verzeichnisstruktur, Anbindung an Domänenverzeichnis und Identitätsmanagementsystem. Für den Kunden bedeutet die Delegation der Benutzer- und Rechteverwaltung zum einen organisatorische Veränderungen, zum anderen durch die Zurverfügungstellung eines Identitätsmanagementsystems technische Adaptierungen.

Ein besonderer Fokus bei den Ausführungen gilt der Informationssicherheit. Die dabei wesentlichen Themenbereiche Authentifizierung (LDAP, Zertifikat, PKI etc.) und Absicherung gegen das Internet sollen im Besonderen beleuchtet werden.

3.5.3.2 Definition Portalverbund

Ein einheitliches österreichweites E-Government erfordert eine gut funktionierende, über lokale Grenzen hinweg reichende Verwaltungskooperation. Durch den Zusammenschluss von Behördenportalen werden Anwendungen einzelner Behörden im Verbund zugänglich gemacht, um bestehende Infrastrukturen gemeinsam nutzen zu können.

Der Anwendungsbetreiber legt nach gesetzlichen Datenschutzbestimmungen fest, welche Verwaltungseinheiten zugriffsberechtigt sind und definiert für seine Anwendungen Rollen mit entsprechenden Rechten. Der Betreiber von Anwendungsportalen delegiert die Autorisierung und Authentifizierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*) an andere Portale in Vertrauensstellung (siehe *3.2.3.1 Vertrauensstellung*). Das Verbundsystem erlaubt somit teilnehmenden Organisationen, ihre eigene Benutzerverwaltung auch für externe Applikationen einzusetzen. Der Applikationsbetreiber erspart sich dadurch die Benutzerverwaltung von externen Teilnehmern. Auf Anwendungen im Portalverbund (kurz: PV) können nur jene Benutzer zugreifen, die von ihrem Stammportal dazu autorisiert worden sind. Dabei wird geprüft, ob das Rechteprofil mit den Zuständigkeiten der zugriffsberechtigten Stelle übereinstimmt. Zusätzlich müssen Datensicherheitsmaßnahmen organisiert und umgesetzt werden [BMI, 2006-1]. Die Benutzerverwaltung verbleibt bei der jeweiligen personalführenden Stelle.

Als Vorteile ergeben sich ein reduzierter Aufwand für die Benutzerverwaltung und eine einfachere Verwaltung der Zugangsrechte durch Single-Sign-On (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*). Grundsätzlich haben Portale den Nutzen, dass mehrere Anwendungen über einen Punkt zugänglich gemacht werden können und der Benutzer sich nur einmal authentifizieren muss. Bisherige Parallelentwicklungen (z. B.: Verzeichnisse) können in Zukunft vermieden und somit

Kosteneinsparungen für alle Beteiligten erzielt werden. Neben der Eliminierung der redundanten Verwaltung von Benutzern, ihren Rechten und Attributen ergeben sich weitere Vorteile [BMI, 2005-2, S 5] (siehe *3.5.1 Anforderungen und Nutzen aus Mitarbeitersicht*, *3.5.2 Anforderungen, Nutzen und treibende Faktoren aus Unternehmenssicht*):

- Die Arbeitsabläufe für Beginn, Änderung und Beendigung von Dienstverhältnissen sowie organisatorischen Veränderungen können erheblich vereinfacht werden.
- Durch den Wegfall redundanter Benutzerdatenbanken werden eine bessere Datenkonsistenz und in der Folge ein höheres Sicherheitsniveau erreicht.
- Benutzer erhalten rascher Zugriff zu Anwendungen.
- Für Organisationen, die über keine eigene Infrastruktur verfügen, besteht die Möglichkeit der Inanspruchnahme eines Dienstleisters. So kann sich beispielsweise eine Gemeinde des Portals ihres Bundeslandes bedienen.
- Die Verwendung von Anwendungsportalen für interne Applikationen bietet weitere Synergieeffekte, weil die Benutzer und ihre Rechte an einer Stelle für interne und externe Anwendungen administriert werden.

Die Applikationen selbst sind Webanwendungen, die sich auf HTTP- (siehe *1.3.4.2.3 HTTP-Sicherheit*) oder SOAP-Protokolle (siehe *3.4.4.2.3 SOAP*) stützen. Während das Zurverfügungstellen von Applikationen als *Inbound* bezeichnet wird, steht *Outbound* für den Konsum einer Anwendung.
Dem Portalverbund können auch Gebietskörperschaften, sonstige Körperschaften des öffentlichen Rechts oder andere Institutionen, die staatliche Aufgaben besorgen, beitreten. Technisch und organisatorisch wird die Kommunikation im Portalverbund durch das *Portalverbundprotokoll* (kurz: *PVP*) (siehe *3.5.3.2.1 Portalverbundprotokoll*) und durch die Festlegung von *Sicherheitsklassen* (siehe *3.5.3.2.3 Sicherheitsklassen*) geregelt. Für den Beitritt ist in Form der *Portalverbundvereinbarung* (siehe *3.5.3.2.2 Portalverbundvereinbarung*) eine Beitrittserklärung auszufüllen und beim Depositar[782] zu hinterlegen[783]. Diese enthält Rechte und Pflichten, die von den teilnehmenden Portalbetreibern einzuhalten sind. Zwischen den Betreibern von Stammportalen, welche die Benutzer verwalten und Anwendungsbetreibern wird so ein Vertrauensverhältnis hergestellt[784].
Im Portalverbund verfügbare Applikationen[785] sind beispielsweise das *Zentrales Melderegister* (Appl-ID: ZMR), *Firmenbuch* (Appl-ID: FDB), *Datenverarbeitungsregister* (Appl-ID: DVR), *Grundbuch* (Appl-ID: GDB), *Zentrales Vereinsregister* (Appl-ID: ZVR), *Grundversorgung (für Asylanten)* (Appl-ID: GVS), *Identitätsdokumentenregister* (Appl-ID: IDR), *Führerscheinregister* (Appl-ID: FS-neu),

[782] Bundesministerium, das für die IT-Koordination des Bundes zuständig ist.
[783] Vgl. http://www.ag.bka.gv.at/index.php/Portalverbund:Allgemein [7. August 2007]
[784] Vgl. http://www.digitales.oesterreich.gv.at/site/5288/default.aspx [25. August 2007]
[785] Vgl. http://reference.e-government.gv.at/Portalverbund.577.0.html [25. August 2007]

Strafregister-Anfragen (Appl-ID: EKIS). Jede dieser Applikationen unterliegt einer Sicherheitsklasse, entsprechend dieser sind die organisatorischen und technischen Maßnahmen umzusetzen.

3.5.3.2.1 Portalverbundprotokoll

Das Portalverbundsystem ermöglicht die Delegierung von Benutzeridentitäten und Berechtigungen.
Das Portalverbundprotokoll (kurz: PVP) regelt die technischen Standards und erweitert die Kommunikation zwischen Stamm- und Anwendungsportalen (siehe *Abbildung 53: Portalverbund – Funktionsweise allgemein*), indem vertrauenswürdige Aussagen über Autorisierung, Authentizität (siehe 2.2.6 Autorisierung, Authentifizierung und Authentizität) und Verrechnungsdaten von Benutzern kommuniziert werden. Autorisierung bedeutet in diesem Zusammenhang, dass einem Benutzer für den Zugriff auf eine Ressource Rechte, Rechteparameter und eine Sicherheitsklasse zugewiesen werden.
Die Kommunikation zwischen den Portalen muss Integrität und Vertraulichkeit (siehe *1.2.2 Anforderungen an die Informationssicherheit: Integrität, Vertraulichkeit*, *2.1 Problemstellung und Herausforderung: Absicherungsziele, Vertraulichkeitsziele*) gewährleisten. Darüber hinaus ist PVP für die Kommunikation zwischen Behörden und Nicht-Behörden auf Grund bilateraler Vereinbarungen und für den Austausch zwischen internen Stamm- und Anwendungsportalen bzw. Anwendungsportalen und Anwendungen vorgesehen [BMI, 2004-1, S 3].
Die Informationen, die im PVP übermittelt werden, bestehen aus Attributen, die nach dem Schema von LDAP.gv.at (siehe *3.5.3.2.6 Verzeichnisdienst LDAP-gv.at*) modelliert sind.

- *Metainformation*: Die Metainformation enthält die PVP-Versionsnummer. Diese wird aufgrund der aktuellen Implementierung des Clients gesetzt.
- *Autorisierungsinformation*: Diese wird benötigt, um dem Benutzer für die Applikation die Zugriffsberechtigung zu erteilen [BMI, 2004-1, S 9].

AUTHORIZE-…	
gvOuId	Eindeutige Kennung für die Organisationseinheit des Benutzers. (LDAP: gvOrgUnit/gvOuId)
Roles	Anwendungsrechte, optional mit Rechte-Parametern. (LDAP: gvApplicationRight/cn cn (Rechte) und gvUserRestriction (Rechte-Parameter))

- *Authentifizierungsinformationen*: Sie beinhalten Organisation und Organisationseinheit sowie Identifikationsmerkmale des Benutzers (z. B.: *cn, uid, gvFunction*). Die Authentifizierungsinformation dient zur Nachvollziehbarkeit im Applikationsportal [BMI, 2004-1, S 8].

AUTHENTICATE-…	
gvOUId	Eindeutige Kennung für die Organisationseinheit des Benutzers. (LDAP: gvOrgUnit/gvOuId)
Cn	Name des Benutzers. (LDAP: gvOrgPerson/cn)
UserID	UserID, mit der der Benutzer am Stammportal authentifiziert ist. (LDAP: gvOrgPerson/uid)
gvFunction	Funktion des Benutzers.

Im Folgenden wird angegeben, wie das PV-Protokoll an das HTTP-Protokoll (siehe *1.3.4.2.3 HTTP-Sicherheit*) gebunden wird.

- Die PVP-Parameter werden über benutzerdefinierte HTTP-Header mitgegeben.
- Die Namen der HTTP-Header werden mit dem Präfix X- (für benutzerdefinierte Header) versehen.
- Bei Trennzeichen „ ,;()= “ in den Werten der HTTP-Header (z.B. *X-AUTHORIZE-roles*) sollte Leerraum vermieden werden, kann aber vorkommen.
- HTTP muss mit TLS oder SSL 3.0 (siehe *1.3.4.2.5 SSL/TLS-Sicherheit*) gesichert werden, wobei Client-Zertifikate verpflichtend sind.
- Wenn die Verrechnungsdaten vom Stamm- oder Anwendungsportal protokolliert werden sollen, muss die Anwendung die vom Benutzer eingegebenen Werte als die Cookies (siehe *2.3.3.2.3 Cookies*) *x-gvCostCenterId* und *x-gvChargeCode* übergeben, damit sie für das Anwendungsportal lesbar sind. Die Cookies bleiben nur für die Dauer einer HTTP-Transaktion erhalten.
- Jede HTTP-Transaktion wird für sich authentifiziert, da das HTTP-Protokoll zustandslos ist (siehe *1.4.3.5.2 Session-Hijacking, 2.3.3.2.3 Cookies*).
- Fehlermeldungen werden als HTTP-Code zurückgegeben.

Die Protokollbindung für SOAP (siehe *3.4.4.2.3 SOAP*) wird mit der Spezifikation WS-Security (siehe *3.4.4.2.5 WS-Security*) um Sicherheitsaspekte erweitert.
Im Portalverbundsystem sind Verwaltungszertifikate oder kommerzielle Zertifikate (siehe *1.7.2.1.6 Digitale Zertifikate*) zu verwenden. Das Zertifikat identifiziert den Stammportalbetreiber.
Sowohl Anwendungs- als auch Stammportal können als Reverse Proxy (siehe *1.7.2.4.3 Proxy*) implementiert werden.

3.5.3.2.2 Portalverbundvereinbarung

Die Teilnahme am Portalverbund wird durch die Portalverbundvereinbarung (kurz: PVV)[786] geregelt. Diese beinhaltet Rechte und Pflichten, die von den beigetretenen Portalverbundpartnern einzuhalten sind[787]:

- In der PVV werden grundlegende Begriffsbestimmungen wie Stammportal, Anwendungsportal, Portalverbundsystem, Teilnehmer, Benutzer, Portalbetreiber etc. definiert.
- Rechte und Pflichten der Anwendungsbetreiber (Verfügbarkeitszeiten, Bedingungen für Zugangsberechtigungen, Nutzungsbedingungen, Überprüfung der Rechtevergabe, Einsicht in die Revisionskontrolle des Stammportals).
- Rechte und Pflichten der Anwendungsportalbetreiber (z. B.: Plausibilitätsprüfungen von Zugriffs- und Rechteprofil, Überprüfung der Benutzerberechtigung, Umsetzung von Datensicherheitsmaßnahmen, Aktionsplan für Störfälle).
- Rechte und Pflichten der Stammportalbetreiber (Organisation Benutzerverwaltung, Einrichtung von Zugriffsprofilen, Benutzerschulung (siehe *1.8.2.5.2 Sensibilisierung und Schulung*, *1.8.3 Der Faktor Mensch*), jährliche Sicherheitsrevision).
- Der zugriffsberechtigten Stelle werden bestimmte Rechte und Pflichten eingeräumt (Zuweisung von Zugriffsrechten, Zuteilung von Rechteprofilen).
- Zu den sonstigen Pflichten der Portalbetreiber zählen die Aufzeichnung und Aufbewahrung der Datensicherheitsmaßnahmen und die Bekanntgabe von Ansprechpartnern (siehe *1.8.2.4.3 IT-Sicherheitsplan*).
- Technische und organisatorische Vorkehrungen (Mindeststandards, Anforderungen an Geräte für die Kommunikation im Portalverbund) müssen getroffen werden.
- Regelungen des Entzugs von Zugriffsberechtigungen und Konditionen des Ausscheidens eines Teilnehmers müssen festgelegt werden.

Die Akteure sind eine Organisation mit den einzelnen Benutzern, der Betreiber des Stammportals, der Betreiber des Anwendungsportals und der Verantwortliche der einzelnen Anwendung. Der Gültigkeitsbereich der einzelnen Vereinbarungen ist Abbildung 48 zu entnehmen.

[786] Vgl. http://reference.e-government.gv.at/Portalverbund.577.0.html [25. August 2007]
[787] Vgl. http://www.ag.bka.gv.at/index.php/Portalverbund:Vereinbarung [7. August 2007]

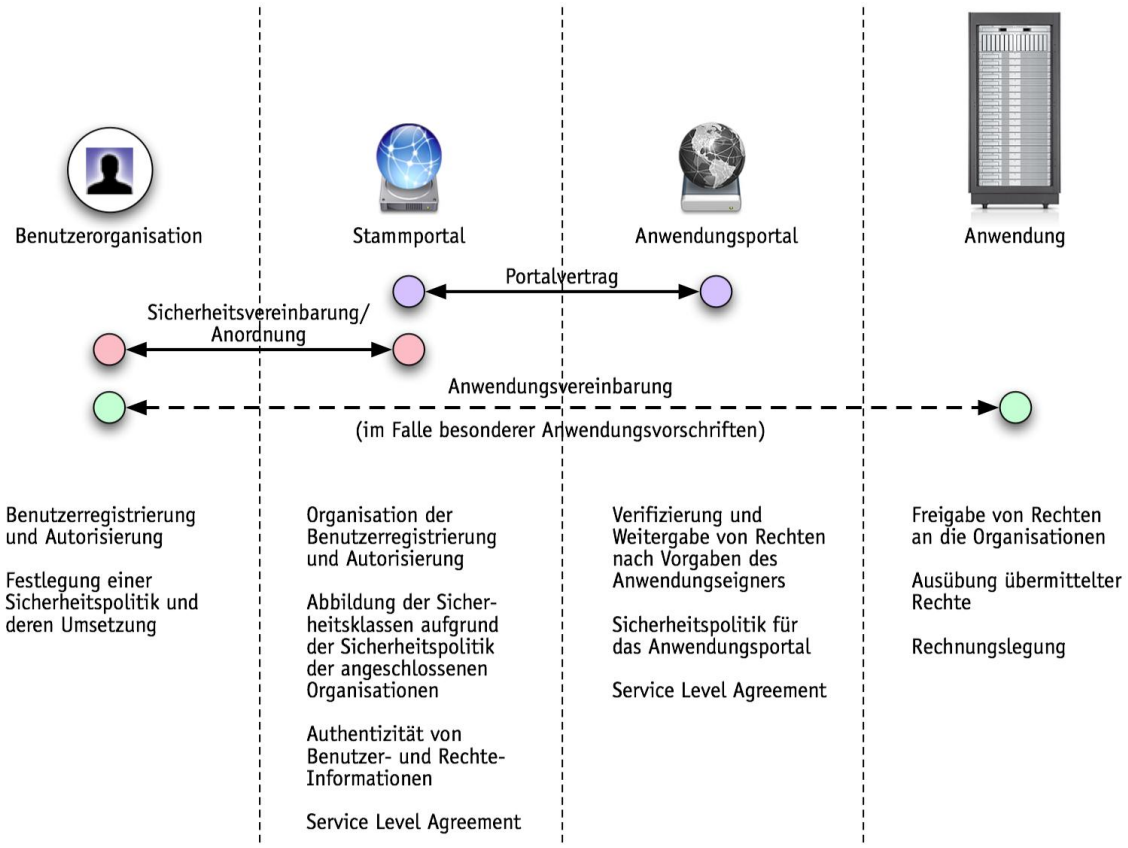


Abbildung 48: Portalverbundvereinbarungen

3.5.3.2.3 Sicherheitsklassen

Sicherheitsanforderungen können von Anwendung zu Anwendung verschieden sein. Ausschlaggebend für den geforderten Sicherheitsgrad sind die Daten, die verarbeitet werden. Die Sicherheitsmaßnahmen, die auf Benutzer- und Betreiberseite gesetzt werden, müssen unterschiedlichen Faktoren Rechnung tragen. Räumliche und physische Sicherheit, Authentifizierungssicherheit, Netzwerksicherheit und Schulung bzw. Sensibilisierung der Humanressourcen sind nur einige davon.

Der Zugriff auf schützenswerte Daten hat im Rahmen einer Sicherheitsvereinbarung oder -verordnung zu erfolgen. Allgemeine Sicherheitsvereinbarungen – wie die Portalverbundvereinbarung (siehe *3.5.3.2.2 Portalverbundvereinbarung*) – können durch anwendungsspezifische Sicherheitsvereinbarungen ergänzt werden. Die Prüfung der Sicherheitsvereinbarungen soll zum Zeitpunkt des Zugriffs automatisch erfolgen und einfach zu verwalten sein. Dazu sind die Erfordernisse in Sicherheitsklassen zu kategorisieren, welche mit Maßnahmen im Benutzer-, Anwendungs- und Kommunikationsbereich zu erfüllen sind. Die Sicherheitsklassen im Portalverbund werden nach der Spezifikation *SecClass 2.1* [BMI, 2007-5] in vier Kategorien von 0-3 unterschieden. Die Vereinbarung von Sicherheitsklassen gewährleistet eine adäquate Sicherheit für die Anwendungen. Die Sicherheitsklassen sind auf einer allgemeinen Ebene spezifiziert und müssen von

den jeweiligen Organisationen im Detail spezifiziert werden. Damit sollen unterschiedliche Sicherheitsnormen (z. B.: ISO 27001, IT-Grundschutzhandbuch) (siehe *1.8.4.1 Standardisierte Informationssicherheitsmanagement-Systeme*) umgesetzt und zertifiziert werden können [BMI, 2007-2, S 3].

In diesem Kontext werden die Anforderungen der Pseudonymität (siehe *2.2.2 Pseudonymität*) oder Anonymität (*2.2.3 Anonymität*) von Benutzern nicht betrachtet, da die Nachvollziehbarkeit des Zugriffs auf personenbezogene Daten wichtiger ist.

Die Sicherheitsklasse ist aus Benutzersicht von folgenden Faktoren abhängig [BMI, 2007-2, S 8f]:

- Client (z. B.: Arbeitsplatzrechner),
- Ort (Außendienst, Telearbeitsplatz, Amtsgebäude mit Zutrittskontrolle),
- Netzwerkanbindung (Intra- versus Internet),
- Autorisierungsprozess,
- Authentifizierungsfaktoren (z. B.: Wissen und Besitz).

Die folgende Tabelle definiert, in welchen Bereichen von der jeweiligen Organisation des Benutzers detaillierte Informationssicherheitsanforderungen definiert werden müssen: „X“ bedeutet erforderlich, „E“ empfohlen.

Client-Authentifizierung	**0**	**1**	**2**	**3**
Anonym	X			
Authentifiziert durch Wissen (Benutzerkennung/Passwort)		X		
Authentifiziert durch Wissen und Besitz (SW-Zertifikat, HW-Token, Bürgerkarte, Einmalpasswort) oder Authentifiziert durch Wissen an in einem geschützten Bereich betriebenen Gerät oder Authentifiziert durch Wissen und biometrisches Merkmal			X X X	
Authentifiziert durch Wissen und biometrisches Merkmal an in einem geschützten Bereich betriebenen Gerät oder Authentifiziert durch Wissen und Besitz an in einem geschützten Bereich betriebenen Gerät oder Authentifiziert durch Wissen und Besitz an einem mobilen Endgerät mit erhöhtem Grundschutz				X X X
IT-Grundschutz	**0**	**1**	**2**	**3**
Passwortsicherheit		X	X	
Session Timeout		X	X	X
Keine (Zwischen-) Speicherung von Anwendungsdaten am Client		X	X	X

Schutz vor Schadprogrammen		X	X	X
Physische Sicherheit			X	X
Netzwerkidentifikation (IP-Netzwerk- oder Gerätezertifikat)				E
Restriktives Gerätemanagement (beschränkte Benutzerrechte)			X	X
Datenschutz	**0**	**1**	**2**	**3**
Integrität (MAC/Hashwert im SSL)	X	X	X	X
Authentizität (über Protokolle)		X	X	X
Verbindlichkeit (über Protokolle oder Signatur)		X	X	X
Verschlüsselung (SSL, symmetrischer Schlüssel mind. 100 Bit)			X	X
Personelle Maßnahmen	**0**	**1**	**2**	**3**
Identifikation (Registrierung) mit amtlichem Lichtbildausweis oder durch persönliche Bekanntschaft			X	
Identifikation (Registrierung) mit amtlichem Lichtbildausweis entsprechend den Erfordernissen für qualifizierte Zertifikate[788]				X
Regelungen für Mitarbeiter		X	X	X

Abbildung 49: Datenklassifizierung aus Benutzersicht

Für die Klassifikation von Anwendungen ist der Schutzbedarf für Informationssysteme ausschlaggebend. Bei der Schutzbedarfskategorie „niedrig bis mittel“ wird auf eine detaillierte Risikoanalyse verzichtet und auf die Klassifizierung nach dem Datenschutzgesetz bzw. Grundschutzansatz zurückgegriffen. Dies erlaubt eine schnelle und effektive Auswahl von grundlegenden Sicherheitsmaßnahmen bei gleichzeitiger Gewährleistung eines angemessenen Schutzniveaus. Informationssysteme der Schutzbedarfskategorie „hoch bis sehr hoch“ sind einer detaillierten Risikoanalyse zu unterziehen (siehe *1.8.2.3 Risikoanalyse*). Die Sicherheitsklasse wird als Maximum der beiden Klassifizierungen ermittelt.

Klassifizierung der Daten nach DSG 2000 und Grundschutzansatz	**0**	**1**	**2**	**3**
Frei verfügbare Informationen	X			
Abfrage von personenbezogenen Daten, die für jedermann zugänglich sind		X		
Transaktion personenbezogener Daten (§4 Abs 1 DSG 2000)			X	
Transaktion sensibler Daten (§4 Abs 2 und §18 Abs 2 DSG 2000)				X

Abbildung 50: Datenklassifizierung nach DSG/Grundschutzansatz

Die Schutzbedarfsklassen werden situationsabhängig (Gesetzesverstoß, Beeinträchtigung der persönlichen Unversehrtheit, Vertraulichkeit, Dauer der Verzichtbarkeit, negative Außenwirkung,

[788] Anm.: §8 Abs 1 SigG verlangt, dass „die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines amtlichen Lichtbildausweises zuverlässig festzustellen ist.“ Der Nachweis darüber ist durch die Ablage einer Ausweiskopie oder die Niederschrift der Ausweisdaten zu erbringen.

finanzielle Auswirkungen etc.) abgeleitet[789]. Weiterführende Erläuterungen dazu siehe in BMI, 2007-2, S 6f.

Aus Anwendungssicht ergeben sich folgende Anforderungen:

Server-Authentifizierung	**0**	**1**	**2**	**3**
Server-Authentifizierung durch Zertifikat (für HTTPS)	X	X	X	X
Signatur von aktivem Content	X	X	X	X
Datensicherheit	**0**	**1**	**2**	**3**
Authentizität (über Protokolle)		X	X	X
Bestätigung von Transaktionen durch die Anwendung			X	X
Integrität (MAC/Hashwert im SSL)	X	X	X	X
Verbindlichkeit (über Protokolle oder Signatur)		X	X	X
Verschlüsselung (SSL, symmetrischer Schlüssel mind. 100 Bit)			X	X

Abbildung 51: Datenklassifizierung aus Anwendungssicht

Für die Kommunikation zwischen Anwendungs- und Stammportal wird eine Authentifizierung in Form eines Zertifikats (für HTTPS) verlangt. Datensicherheit wird je nach Sicherheitsklasse über Protokolle, Signatur, Verschlüsselung oder Transaktionsbestätigungen erreicht.

Peer[790]-Authentifizierung	**0**	**1**	**2**	**3**
Wahlweise: Client-Zertifikat (über SSL-Verbindung oder VPN) oder Shared Secret (VPN) oder Überprüfung der statisch zugeordneten IP-Adresse		X	X	X
Datensicherheit	**0**	**1**	**2**	**3**
Integrität (MAC/Hashwert im SSL)	X	X	X	X
Verschlüsselung (SSL, symmetrischer Schlüssel mind. 100 Bit)			X	X

Abbildung 52: Datenklassifizierung aus Kommunikationssicht

Eine effektive Realisierung dieser Maßnahmen erfordert ein funktionierendes Informationssicherheitsmanagement. An dieser Stelle ist auf die diesbezüglichen Ausführungen in *1.2.2 Anforderungen an die Informationssicherheit, 1.3 Taxonomie von Angriffen auf den Wert Information, 1.7.2.1 Kryptologie, 1.7.2.3 Biometrie, 1.7.2.4 Perimetersicherheit, 1.7.2.6 Neue und alternative Ansätze des Schutzes vor Malicious Code, 1.8.2.4.3 IT-Sicherheitsplan, 1.8.2.5.1*

[789] Vgl. http://www.ag.bka.gv.at/index.php/Portalverbund:Sicherheitsklassen [7. August 2007]
[790] Peer ist die Bezeichnung für einen gleichberechtigten Knoten in einem Computernetzwerk.

Implementierung von Maßnahmen, 2.2.1 Digitale Identität, 2.2.6 Autorisierung, Authentifizierung und Authentizität zu verweisen.

3.5.3.2.4 Techniken und Technologien für Portalverbund

Für die Implementierung eines Portalverbundes sind verschiedene Techniken und Technologien erforderlich. An dieser Stelle ist an die Ausführungen in einem vorigen Kapitel (siehe *3.4 Komponenten und Funktionen eines Identitätsmanagementsystems*) zu verweisen. Ergänzend sollen hier nur die Spezifika hinsichtlich Portalverbund erläutert werden.

Ein Portal wird im diesem Verbund im Allgemeinen als Reverse Proxy (siehe *1.7.2.4.3 Proxy)* im Sinne der HTTP-Spezifikation[791] implementiert. Aus HTTP-Client-Sicht ist ein Gateway keine Zwischenstation, sondern der endgültige Kommunikationspartner. Dem entsprechend sind Namensraum und Adressierung auf das Portal bezogen. Ein PV-Portal unterscheidet sich von einem gewöhnlichen Reverse Proxy durch zwei Merkmale: Die Funktion als Autorisierungs- und Authentifizierungsproxy einerseits und das Mapping von URLs auf mehrere Anwendungsportale andererseits. URL-Mapping bedeutet, dass der Pfadteil des URLs entscheidet, zu welchem Server ein Request weiter geleitet wird. Dadurch entsteht am Reverse Proxy ein gemeinsamer Namensraum der Anwendungen.

Wird das Domain-Attribut im Cookie-Header (siehe *2.3.3.2.3 Cookies*) nicht gesetzt, dann braucht es vom Reverse Proxy nicht umgeschrieben werden. Andernfalls müssen Cookie-Domains bei Responses so editiert werden, dass sie bei einem darauf folgenden Request einerseits vom Browser an das Portal übergeben werden und andererseits das Stammportal die Domäne wieder korrekt zurücksetzen kann [BMI, 2004-2, S 1ff].

Einer der Gründe, warum sich Service Oriented Architecture (kurz: SOA) (siehe *3.4.4.2.8 SOA*) auf Basis von Web Services durchsetzt, ist, dass SOAP (siehe *3.4.4.2.3 SOAP*) erlaubt, das Web als universelle Middleware[792] einzusetzen, ohne auf teure und proprietäre Lösungen angewiesen zu sein. SOAP muss besonders geschützt werden, da es Daten in einer allgemein verständlichen Form (als sogenannter *tagged text*) transportiert, die leicht abgehört und von einem ungewollten Empfänger missbraucht werden können. Erweiterungen von SOAP um Sicherheitsaspekte finden sich in Form der WS-Security-Spezifikation (siehe *3.4.4.2.5 WS-Security*) wieder [BMI, 2005, S 8ff].

---

[791] http://www.ietf.org/rfc/rfc2616.txt [23. November 2007]

[792] Middleware ist eine Verteilungsinfrastruktur, über die verschiedene Anwendungen auf unterschiedliche Ressourcen zugreifen können. Sie dient dem Aufbau von verteilten Systemen, in denen Anwendungen entfernte wie lokale Ressourcen nutzen können. Middleware ist zwischen Applikation und Betriebssystem angesiedelt und vermittelt zwischen diesen. Technisch stellt sie Software-Schnittstellen und/oder Dienste bereit. Eine Software A, die die Middleware-Schicht benutzen möchte, um mit einer Software B zu kommunizieren, kann diese Schnittstellen benutzen. Die entsprechenden Aufrufe werden von der Middleware-Softwarekomponente über ein Netzwerk weitergereicht (z. B.: TCP/IP, darauf aufbauend HTTP, darauf aufbauend SOAP, Web Services verwendet). Auf der Empfängerseite setzt die Middleware die Anforderung in einen Funktionsaufruf an die Software B um. Gegebenenfalls leitet sie die Antwort von B an A auf demselben Weg zurück.

3.5.3.2.5 Autorisierung und Authentifizierung

Der erste Schritt ist die Autorisierung beim Stammportalbetreiber. Dabei wird festgestellt, welchen Mitarbeitern welche Applikationen mit welchen Rechten zustehen. Für jede Anwendung existiert eine Reihe von Berechtigungsparametern. Der Applikationsverantwortliche in der Dienststelle ist für die Zuordnung verantwortlich. Dem Mitarbeiter werden ein Benutzername und ein Kennwort zugewiesen. Jede organisatorische Änderung (Jobwechsel, Ausscheiden des Mitarbeiters etc.) ist vom Zuständigen nachzuvollziehen.

Die Authentifizierung erfolgt durch das Stammportal. Das Anwendungsportal erhält die Benutzerinformationen über PVP. Übertragen werden Meta-, Chaining-, Autorisierungs-, Authentifizierungs- und Verrechnungsinformationen (siehe *3.5.3.2.1 Portalverbundprotokoll*). Der Benutzer wird durch Organisations-ID (VKZ und OrgId), Benutzer-ID (gvOrgPerson/uid), Name des Benutzers (gvOrgPerson/cn), Globaler Identifier des Benutzers (gvOrgPerson/gvGid), Sicherheitsklasse (Default Klasse 1), Funktion des Benutzers (gvPersonFunction/gvFunction), Anwendungsrechte bzw. Rollen (gvApplicationRight/cn) eindeutig identifiziert. Bei erfolgreicher Prüfung der Parameter wird der HTTP-Request an die jeweilige PV-Anwendung weitergeschickt. Danach wird die Applikation zur Verfügung gestellt. Die Kommunikation zwischen den Portalbetreibern ist in Form eines SSL/TLS-Zertifikats (siehe *1.3.4.2.5 SSL/TLS-Sicherheit, 1.7.2.1.6 Digitale Zertifikate, 3.5.3.2.1 Portalverbundprotokoll*) abgesichert.

In Zusammenhang mit SOA (siehe *3.4.4.2.8 SOA*) tauchen neue Anforderungen an die Verwaltung von Benutzern und Berechtigungen auf: Nicht mehr einzelne Systeme, auf denen ein Benutzerprofil existiert und eine persönliche Anmeldung genügt, sondern Services, die von unterschiedlichen unabhängigen Systemen angeboten werden, sind die Dienstanbieter. Um nicht mit jedem dieser Services einzeln verhandeln zu müssen (Anmeldung, Rechteüberprüfung, Anwendung, Abmeldung), ist eine Vermittlungsschicht für die Benutzerverwaltung und Rechteerteilung notwendig geworden. Dabei ergeben sich Besonderheiten für die Verwaltungsaufgaben um Benutzer und Rechte in einem Netzwerk von Services [BMI, 2005-2, S 9]:

- Es muss eine Vertrauensbasis zwischen den Systemen bestehen, an denen die Benutzer angemeldet sind und den Systemen, auf denen die Services angeboten werden.
- Die Anwendungen müssen eine Übereinkunft über die Vermittlung von Identitätsinformationen und Berechtigungen haben, um die Benutzerinformationen von einem System auf einem anderen gültig werden zu lassen.
- Die Vermittlung dieser Berechtigungen muss auf eine sichere Weise nicht nur auf Netzwerk- sondern auf Anwendungsebene erfolgen.

3.5.3.2.6 Verzeichnisdienst LDAP-gv.at

Die E-Government-Strategie der Österreichischen Bundesregierung strebt eine vollständige Darstellung der Verfahren der öffentlichen Verwaltung in elektronischer Form an. Diese Verfahren umfassen sowohl die Abläufe zwischen Behörde (engl. *Government*), Bürgern (engl. *Citizen*) (kurz: *G2C*), als auch die internen Abläufe zwischen Behörden (kurz: *G2G*).

In diesen Verfahren sind die Zuständigkeiten und Rechte von Personen und Organisationseinheiten wichtige Parameter. Der Verzeichnisdienst bildet diese Informationen in einer standardisierten Form ab und ermöglicht es Applikationen, über definierte Schnittstellen auf die Informationen zuzugreifen. Für den Abruf besteht eine verwaltungsinterne Sicht, die über das Intranet beziehungsweise den Portalverbund erreichbar ist. Weiters besteht eine auf den notwendigen Informationsumfang reduzierte, öffentlich zugängliche Sicht im Internet.

Der Verzeichnisdienst bietet die Plattform für die sichere Bereitstellung von Informationen über Rechte und Attribute, die zu Einrichtung und Betrieb der internen Sicherheit von Organisationen erforderlich sind. Diese Informationen erstrecken sich von der Integration der internen Benutzerverwaltung von Betriebssystemen über die ressortübergreifenden Rechte an Portalen bis zur Verwaltung von Zertifikaten[793].

LDAP-gv.at ist die Spezifikation des LDAP-Schemas (siehe *3.4.1.1.2 LDAP*) für den zentralen Verzeichnisdienst der Verwaltung in Österreich[794]. Darin werden die Objektklassen (Organisation, Organisationseinheit, Mitarbeiter, Benutzerrechte) der Benutzerverwaltungssysteme beschrieben. Die aktuelle Version 2.3.0 [BMI, 2006-2] ist mit den Schemaerweiterungen für die Berechtigung und Rechtedelegation im Rahmen der PVP-Implementierung abgestimmt.

Der LDAP-Verzeichnisdienst besteht aus einem zentralen und verschiedenen lokalen Verzeichnissen, die ein einheitliches Grundschema haben und optional mit lokalen Erweiterungen. Bezeichner und Listenwerte sind in englischer Sprache definiert, um einen internationalen Austausch zu ermöglichen.

Objekte werden im *Directory Information Tree* (kurz: *DIT*) positioniert. Mit *domain* erfolgt die Abbildung der Domain-Struktur oberhalb von Verwaltungseinheiten, um die Internet-Domänen wie gv.at, or.at etc. abzubilden. Mit *gvOrganisation* werden Verwaltungseinheiten (Gemeinden, Länder, Ministerien, Selbstverwaltungskörper etc.) dargestellt. Ihre Geschäftseinteilung wird mit Objekten der Klasse *gvOrgUnit* abgebildet. Parallel zur Domain-Hierarchie soll die Org-ID (siehe *3.5.3.2.7 Verwaltungskennzeichen*) als Alternative verwendet werden. Besonders in der Bundesverwaltung, wo Domänen oft kurzlebig sind, ist diese zusätzliche Adressierung sinnvoll. Die Personeneinträge der Klasse *gvOrgPerson* entsprechen Mitarbeitern. Eine natürliche Person kann in mehreren Organisationen geführt werden. Die Zusammenführung mehrerer Einträge einer Person (*gvOrgPerson*) erfolgt durch einen Global Identifier (*Gid* bzw. *gvbPK*). Besitzt eine Person in einer

[793] Vgl. http://www.digitales.oesterreich.gv.at/site/cob__21727/5289/default.aspx [6. September 2007]

Organisation unterschiedliche Funktionen mit unterschiedlichen Rechten, werden die Rechte zusätzlich an die Funktionen der Person (*gvPersonFunction*) gebunden[795].

3.5.3.2.7 Verwaltungskennzeichen

Für eine Reihe von E-Government-Anwendungen ist ein eindeutiges Kennzeichen für Behörden und sonstige Verwaltungsstellen erforderlich. Ein solches stellt das Verwaltungskennzeichen (kurz: VKZ) dar. Verwendung findet das VKZ beispielsweise im Portalverbund.
Das Schema des VKZ hat folgendes Aussehen [BMI, 2007-1, S 2]:

E	BER	-	SCHL

Legende:
„E“ steht für Ebene (Länge: 1 Zeichen)
B=Bund, L=Land, G=Gemeinde, S=Sozialversicherungsträger, K=Kammer, X=Privatrechtlicher Bereich

„BER“ steht für Bereichskennung (Länge: bis zu 3 Zeichen)
BH=Bezirkshauptmannschaft, FA=Finanzamt, BG=Bezirksgericht etc.
(Anm.: Für L wird die erste Stelle der Bereichskennung von der Länderkennung gebildet: 1=Burgenland, 2=Kärnten bis 9=Wien. Diese Länderkennung entspricht der ersten Stelle des Gemeindekennzeichens.)

„SCHL“: Lokaler Schlüssel im jeweiligen Bereich

Beispiele für VKZ sind:
BMF: Bundesministerium für Finanzen
BBG-011: Bezirksgericht Wien Favoriten
L5SB-507: Umweltamt Salzburg
SST-WGKK: Wiener Gebietskrankenkasse
KAE: Ärztekammer
FN-nnnnnnn: Unternehmen mit Firmenbuchnummer nnnnnnn

Die maximale Länge des Verwaltungskennzeichens beträgt 32 Zeichen. Die Verwaltung von beliebigen Teilbereichen des Schlüssels kann an einzelne Stellen der Verwaltung delegiert werden.

[794] Vgl. http://ldap.gv.at/ [5. September 2007]
[795] Vgl. http://www.ag.bka.gv.at/index.php/VerzD:LDAP_gv_at [5. September 2007]

3.5.3.2.8 Funktionsprinzip

Das Portalverbundsystem ermöglicht es den teilnehmenden Organisationen, wechselseitig auf Anwendungen zuzugreifen und dabei ihre lokale Benutzerverwaltung auch für externe Anwendungen zu verwenden.

Betreiber von Anwendungen, die externe Benutzer zulassen, brauchen nur noch Organisationen zu administrieren und reduzieren damit gegenüber einer Benutzerverwaltung den Aufwand um eine Größenordnung.

Voraussetzung für die Delegation der Benutzerverwaltung durch den Anwendungsbetreiber ist, dass eine geeignete Vertrauensstellung hergestellt wird. Das wird organisatorisch durch den Beitritt zur Portalverbundvereinbarung (siehe *3.5.3.2.2 Portalverbundvereinbarung*) erreicht. Die am Portalverbund teilnehmenden Organisationen betreiben für ihre lokalen Netzwerk-Domänen Portale, die über das Internet vernetzt sind. Die Anwendungen sind Webapplikationen, die Request-Response-Protokolle wie HTTP oder SOAP (siehe *3.4.4.2.3 SOAP*) verwenden.

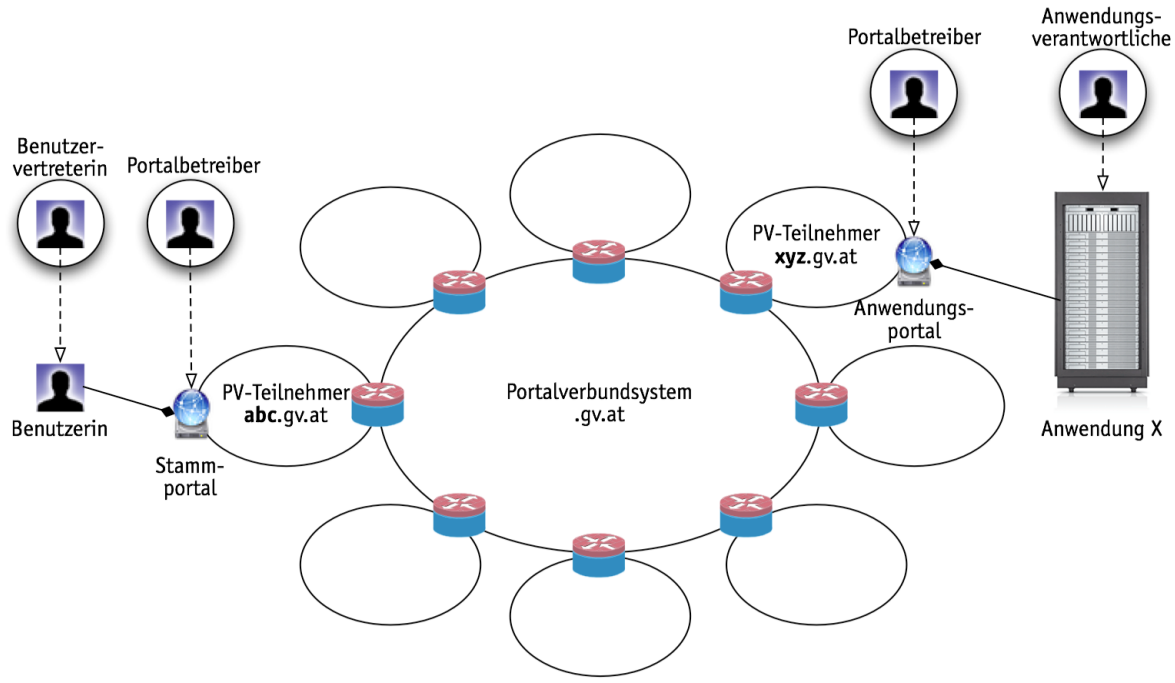


Abbildung 53: Portalverbund – Funktionsweise allgemein

In obiger Abbildung verwenden Benutzer aus der Domain abc.gv.at die Anwendung X der Domain xyz.gv.at. Der Anwendungsverantwortliche der Anwendung X (Anm.: eine Datenanwendung im Sinne des §7 (4) DSG 2000) delegiert die Funktionen Autorisierung und Authentifizierung an den Betreiber des Portals der Domäne *xyz.gv.at*. In diesem Zusammenhang wird die Summe der für die Anwendung X möglichen Rechte und Einschränkungen definiert. Der Anwendungsverantwortliche hat mit der Organisation *abc.gv.at* eine Anwendungsvereinbarung (siehe *Abbildung 48: Portalverbundvereinbarungen*) für die Anwendung X geschlossen. In der Folge beauftragt der

Anwendungsverantwortliche den Betreiber des Portals *xyz.gv.at*, dem Portal *abc.gv.at* die in der Nutzungsvereinbarung definierten Rechte einzuräumen. Der Portalbetreiber von *abc.gv.at* definiert, welchen Benutzern der Organisation *abc.gv.at* der Zugriff auf die Anwendung eingeräumt wird [BMI, 2005-2, S 2]. Der Benutzer authentifiziert sich am Stammportal, das ihn über das Portalverbundprotokoll am Anwendungsportal autorisiert und authentifiziert. Der Benutzer greift via Internet-Browser auf die gewünschten Applikationen zu. Durch Eingabe von Benutzername und Kennwort erfolgt die Anmeldung am Authentifizierungsserver. Die einmalige Eingabe (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) genügt, dem Mitarbeiter stehen damit sämtliche ihm zugedachten Applikationen zur Verfügung. Der Ablauf ist graphisch in *Abbildung 55: PV-Umsetzung* dargestellt.

- Der Mitarbeiter baut durch das Auswählen einer Behördenapplikation über das am Stammportal befindliche Zertifikat eine SSL-Kommunikation auf.
- Der Authentifizierungsserver befüllt den HTTP-Header mit den vorgesehenen Daten nach PVP. Der Server verwendet SSL nach außen, im geschützten Bereich wird auf HTTP umgestellt.
- Das Inbound-Servlet prüft den HTTP-Header nach dem PVP-Protokoll und protokolliert diese.
- Bei erfolgreicher Prüfung der Parameter wird der HTTP-Request an die jeweilige PVP-Anwendung weitergeschickt und die Applikation zur Verfügung gestellt.

3.5.3.2.9 Revision

Laut §4 (8) PVV ist für ein Stammportal eine Schnittstelle für die Revision zu spezifizieren. Diese Funktion wird als Anwendung an den Anwendungsportalen[796] der Stammportalbetreiber implementiert. Den Revisionsberechtigten der Anwendungsverantwortlichen sind die notwendigen Zugriffsrechte einzurichten, damit alle Berechtigungen der betreffenden Anwendung gelesen werden können. Laut PVV sind in der Revisionsabfrage den Anwendungsverantwortlichen für alle Benutzer, die auf deren jeweiligen Anwendungen Zugriff haben, folgende Attribute auszugeben: Familien-, Vorname, UserID, Global Identifier, Organisationseinheit des Benutzers und Rechte [BMI, 2007-3, S 3f, BMI, 2007-4].

[796] Organisationen ohne eigenes Anwendungsportal können die Funktionalität des Anwendungsportals auch in der Revisionsabfrage implementieren. Dazu ist im Wesentlichen nur das Zertifikatsmanagement erforderlich.

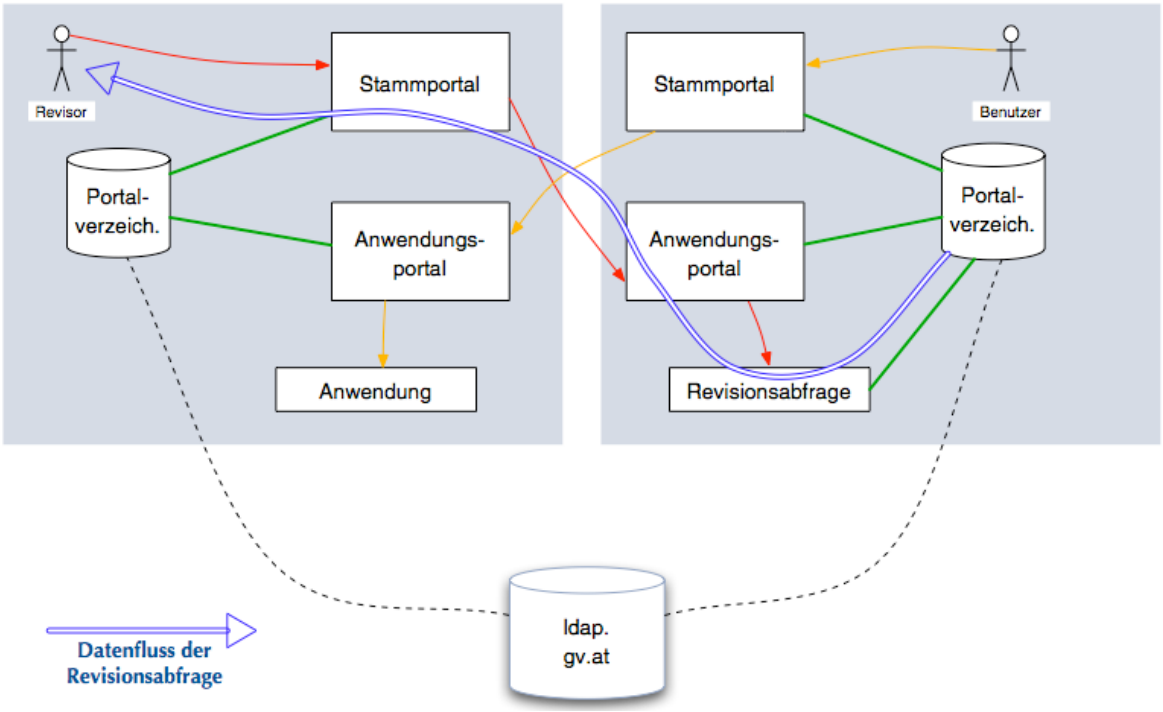


Abbildung 54: Revision

3.5.4 UMSETZUNG EINES IDENTITÄTSMANAGEMENTSYSTEMS

Die Neunziger Jahre waren in den Unternehmen geprägt von der Automatisierung der Geschäftsprozesse durch die Einführung komplexer Anwendungen (Kundenmanagement, Supply Chain Management, Wissensmanagement etc.). Jeweils für sich betrachtet sind damit durchaus Vorteile nutzbar geworden. In Summe können sich durch diese Entwicklungen Negativ-Effekte einstellen, wie keine aufgabengerechte Berechtigungsverwaltung, personell nicht-zuordenbare Accounts oder fehlende Differenzierung zwischen den Rechten interner und externer User. Die Folgen sind aufwändig zu erstellende, ungenaue Reports, die kaum Möglichkeiten für eine sachgerechte Rezertifizierung bieten (siehe *1.8.4.1 Standardisierte Informationssicherheitsmanagement-Systeme*). Diese Situation führt zu Bestrebungen der Zentralisierung der User- und Berechtigungsverwaltung. Zunächst für die Berechtigungen von Anwendungen einer Systemplattform (z. B.: alle Windows-Anwendungen über Active Directory), dann für plattformunabhängige Directories (z. B.: LDAP). Obwohl diese Implementierungen bald an ihre Grenzen stoßen, erfolgt hier bereits die Initialisierung eines Identitätsmanagement-Projektes. Schnell stellt sich die Frage nach der *organisatorischen Reife* eines Unternehmens für ein IMS-Projekt. Aus der Reife eines Unternehmens kann auf die Risiken und den Implementierungsaufwand geschlossen werden. Dabei tauchen spezielle Problembereiche auf, wie etwa die Qualität der Benutzerdaten, rollenbasierte Berechtigungen versus direkt zugewiesene Berechtigungen bis hin zu der Diskussion, welches das beste Rollenmodell sei. Gesicherte Erkenntnis

ist inzwischen, dass ein rollenbasiertes Prozessmanagement für eine Rationalisierung und einen Gewinn an Informationssicherheit sorgen kann[797].

In die folgenden Ausführungen fließen die praktischen Erfahrungen aus der Umsetzung des Portalverbund-Projektes ein. Identitätsmanagement stellt demnach eine übergreifende, unternehmensweite Aufgabe für Unternehmensführung, IT-Führung und Informationssicherheit dar. Solche Systeme müssen in der Form geplant und etabliert werden, dass sie im Kontext von Informationssicherheit (siehe *1.8 Unternehmenssicherheit*) bzw. Datenschutz (*2.3.2.1 Informationelle Selbstbestimmung*, *2.3.2.2 Zusammenhang von Identitätsmanagement und Datenschutz*) die geschäftlichen Aktivitäten eines Unternehmens optimal unterstützen.

Schon bei der Planung ist zu beachten, dass die Umsetzung eines Identitätmanagementsystems für eine große Anzahl von Benutzern in mehreren Phasen abläuft und je nach Intensität und zumindest ein Jahr lang dauern kann. Gartner ergänzt[798]: „*While identity projects may be complicated and costly, organizations can be successful by taking small steps and limiting the scope to key applications - at least initially. They don't believe that all of those legacy applications will ever be fully integrated.* "

Die Bedingung für die Realisierung ist das Vorhandensein einer entsprechenden Lobby im Unternehmensmanagement. Eine Schlüsselanforderung stellt die solide Definition von Identität dar, die sich auf die unterschiedlichen Prozesse, Programme und die bestehende IT-Infrastruktur einstellt. Im Rahmen einer Bedarfsanalyse sind die Anforderungen und Verantwortungen zu ermitteln, die aus den Geschäftsprozessen resultieren. Dies stellt die Basis für die Modellierung von Rollen- und Berechtigungskonzepten sowie für das Design der Prozesse dar. Weiters muss das Schutzniveau der Daten bestimmt werden, um geeignete Prozesse festlegen und angemessene Authentifizierungsverfahren auswählen zu können (siehe *1.8.2 Umsetzung von Informationssicherheitsmanagement*). Zudem sind im Rahmen der technischen Sollfestlegung Anforderungen an die IT-Architektur gemeinsam mit den verantwortlichen Administratoren zu definieren (siehe *3.5.3.2.3 Sicherheitsklassen*). Dabei gilt es zu überlegen, inwieweit vorhandene Komponenten genutzt werden können. Aus technischer Sicht konkurrieren verschiedene Architekturansätze. Es geht einerseits um die Datenhaltung – relationale Datenbank versus LDAP – und um die Frage, entweder ein modulares System mit zentraler und komponentenübergreifender Modellierung oder eine lose Kopplung einzelner Produkte mit einer Synchronisation der User- und Strukturdaten zwischen den Produkten einzuführen. Zu beachten ist, dass Rahmenlösungen von vielen Herstellern zur Verfügung stehen, jedoch Anpassungen erfordern. Je komplexer und unübersichtlicher die bisherigen Applikationen und die IT sind, desto teurer kommt die Implementierung[799]: „[…] *spent*

[797] Vgl. http://www.digitalidworld.de/agenda.php [8. Dezember 2007]
[798] Vgl. http://www.computerworlduk.com/technology/security-products/authentication/in-depth/index.cfm?articleid=139 [8. Dezember 2007]
[799] Vgl. http://www.computerworlduk.com/technology/security-products/authentication/in-depth/index.cfm?articleid=139 [8. Dezember 2007]

more than a year mapping data between repositories and changing all user IDs to a common naming convention. But then they found that the versions of the CRM and other software they had deployed – both key repositories of user identity data – wouldn't connect with IMS without substantial integration work."

Bei der Festlegung der Prozesse ist zu definieren, ob die Administration zentral und/oder dezentral erfolgen soll oder ob Möglichkeiten für Self-Service (siehe *3.4.2.5 Self Service*) gewünscht sind. Das Soll wird außerdem von gesetzlichen Bestimmungen und internen Richtlinien wie beispielsweise Sicherheitsvorgaben (siehe *1.8.2.4.2 IT-Systemsicherheitspolitik*) beeinflusst. Der nächste Schritt ist, im Rahmen einer Soll-Ist-Analyse zu prüfen, inwieweit die definierten Anforderungen im Unternehmen bereits umgesetzt sind. Erst auf Basis dieses Ergebnisses ist es möglich, den Inhalt, den zeitlichen Rahmen und die Kosten des umzusetzenden Projekts genauer zu planen. In der Umsetzungsphase haben die Projektverantwortlichen die Aufgabe, Möglichkeiten für die fachlichen, technischen und administrativen Anforderungen zu evaluieren. Dazu gehört, die entsprechenden Architekturkonzepte zu erstellen, Berechtigungskonzepte zu entwickeln sowie Prozesse und Workflows zu gestalten und geeignete Systeme zur Identitätsverwaltung auszuwählen. Im Rahmen eines *Proof-of-Concept*[800] ist die Machbarkeit zu überprüfen, bevor der *Rollout* beginnen kann. Für den Betrieb von IMS sind strukturierte Prozesse wesentlich. Die Bedeutung von Prozessen wird durch eine Umsetzung eines IMS von Novell (siehe *3.3.1.1 Novell Identity Manager*) von *Health First*[801] untermauert: „[…] *Like most vendors, Novell offers connectors for commonly used directories such as LDAP, popular applications such as PeopleSoft, and databases such as SQL Server and Oracle, which some applications use as back-end repositories for identity information. For other applications, Health First needed to write new connectors. But customization wasn't what slowed the project. On average, we spend two or three months dealing with the business processes and two to three weeks writing the connector for any given application*." Mit der Einführung von Identitätsmanagementsystemen gehen daher in der Regel Eingriffe in die Ablauforganisation einher.

Wesentlich ist die Identifizierung der *Stakeholder*[802] und ihr Einbinden in den gesamten Entscheidungs- und Umsetzungsprozess.

[800] Als Proof-of-Concept (deutsch: Machbarkeits-Studie) wird der Nachweis verstanden, an dem die prinzipielle Durchführbarkeit eines Vorhabens belegt ist. Meist ist mit dem Proof-of-Concept die Entwicklung eines Prototyps verbunden, der die benötigte Kernfunktionalität aufweist. Mittels eines Proof-of-Concept können Risiken in der Entscheidung minimiert werden.

[801] http://www.health-first.org/ [8. Dezember 2007]

[802] Als Stakeholder wird eine Person oder Gruppierung bezeichnet, die ihre (berechtigten) Interessen wahrnimmt.

3.5.4.1 Erfolgsfaktoren

Gartner [Gartner, 2006, S 2] hat in einer Untersuchung die *Do's* and *Don'ts* eines IMS-Projekts identifiziert. Fakt ist, dass „*there are no hard-and-fast rules for successful IM implementation – all enterprises must evaluate their own ability to follow specific practices*".

Wesentliche Faktoren für die erfolgreiche Einführung eines unternehmensweiten Identity Managements bilden unter anderem[803] [Gartner, 2006, S 2ff]

- das Committment des Managements,
- die Erstellung einer detaillierten Anforderungsanalyse mit Fachabteilungen und der IT-Abteilung,
- die Entwicklung eines einfachen, aber flexiblen rollenbasierten Berechtigungskonzeptes,
- ein schrittweises Vorgehen, das in einem ersten Schritt die wichtigsten Anwendungen in das IM integriert,
- die Auswahl von Produkten mit Standardschnittstellen,
- das Design einfacher und sicherer Prozesse in Verbindung mit einem hohen Automatisierungsgrad,
- die Verwendung von starker Authentifizierung,
- das primäre Ziel soll vorderhand nicht ein unternehmensweites Directory sein,
- das Versorgen von Usern mit Rollen nur nach Bedarf,
- SSO soll nicht für alle Applikationen funktionieren,
- Federation wird erst bei wirklichem Bedarf realisiert.

Die Einführung eines IMS muss als unternehmensweite Aufgabe gesehen werden, um einen wirtschaftlichen und sicheren Betrieb gewährleisten zu können.

Laut einer Analyse[804] von Gartner und *Völcker Informatik*[805] laufen viele Identitätsmanagement-Projekte zeitlich und finanziell aus dem Ruder, weil deren Komplexität unterschätzt wird. Einer der wichtigsten Aspekte in diesem Zusammenhang ist die unzureichende Qualität der vorhandenen Daten. Aus dem Abschlussbericht zur Analyse geht weiters hervor, dass sich ein Betrieb bei der Verbesserung der Datenqualität neben der Technik auf zwei weitere wesentliche Eckpfeiler konzentrieren muss. Zum einen sind dies die Mitarbeiter, damit die Notwendigkeit einer hohen Datenqualität zur Selbstverständlichkeit wird. Zum anderen geht es um die Prozesse. Entsprechende Regeln, Workflows und Audits sollen fester Bestandteil der Unternehmenskultur sein und von den Angestellten gelebt werden. Da es kein allgemein gültiges Patentrezept – unabhängig von Branche und

[803] Vgl. http://www.lanline.de/themen/security/article.html?thes=8001,9779&art=/articles/20070S2/31071420_ha_LL.html [14. August 2007]
[804] Vgl. http://www.securitymanager.de/magazin/news_h26521.html [8. März 2008]
[805] http://www.voelcker.com/ [8. Dezember 2007]

Größe gibt – muss eine Lösung zudem flexibel und individuell auf die Bedürfnisse des jeweiligen Betriebes zugeschnitten sein. Der Anspruch an die Tools der Benutzerverwaltung ist es, einer bestimmten Person unternehmensweit nicht nur eine eindeutige Identität zuzuordnen, vielmehr soll sichergestellt werden, dass jeder Account der relevanten IT-Systeme dieser *unique* ID zugeordnet wird. "*Wichtig ist, dass die Einordnung von Personen in Organisationsstrukturen und funktionale Einheiten klar und widerspruchsfrei ist*", so Eckhard Völcker. "*In Organisationen mit wenigen hundert oder wenigen tausend IT-Benutzern lässt sich die Zuordnung vielleicht noch manuell durchführen. Je größer die Anzahl ist, desto schwieriger wird dieses Vorhaben*."

3.5.4.2 Organisatorische Aspekte

Um das Spektrum der Funktionalitäten richtig abzubilden, muss vor der Umsetzung einiges überdacht werden (siehe *3.6.3.3 Erarbeitung eines Rollenkonzepts*): Welche Bereiche soll Identitätsmanagement umfassen? Wer darf zu welchen Daten/Informationen Zugriff haben? Was muss von einer Organisation bekannt sein? Wer muss mit eingebunden sein? Stellvertreterregelung? Schulungsmaßnahmen? Sanktionen bei Nichteinhalten von Fristen, Erfüllen von Eingaben? Wie wird mit neuen Applikationen umgegangen?
Bei einigen Punkten kann Anleihe bei der Informationssicherheit genommen werden: Mindsetting, Überzeugungsarbeit, Schulungen (siehe *1.8.2.5.2 Sensibilisierung und Schulung*) bzw. Revision und Auditing (siehe *1.7.1.1.3 Audits und Revision*). Anknüpfungspunkt zwischen Informationssicherheit und Identitätsmanagement sind im organisatorischen Bereich Sicherheitspolicies (siehe *1.8.2.4.2 IT-Systemsicherheitspolitik*).

3.5.4.2.1 Stakeholder

Ein wesentlicher Faktor für die Umsetzung eines IM-Projekts ist das Finden und Einbinden von Stakeholdern (siehe *3.5.1 Anforderungen und Nutzen aus Mitarbeitersicht*). Grundsätzlich können in drei Gruppen unterschieden werden[806]:

- IT-Verantwortliche,
- Non-IT-Management,
- Endanwender.

Diese Gruppen lassen sich weiter differenzieren. Innerhalb der IT sind Identity Management-Themen für die Verantwortlichen von Informationssicherheit und Helpdesk, den Anwendungsarchitekten oder den zuständigen Personen für Unternehmensportale von Interesse.

[806] Vgl. http://www.kuppingercole.de/articles/treiber_260607 [17. August 2007]

Beim Non-IT-Management gibt es etwa die Revision oder den Finanzbereich, der Compliance-Anforderungen umsetzen muss, das Top-Management mit dem Ziel der Corporate Governance oder die Fachabteilungen bzw. den Vertrieb, der mit seinen CRM-Systemen einen der größten Identitätsspeicher des Unternehmens betreibt. Der Betriebsrat bzw. die Personalvertretung sind schon allein aufgrund der Tatsache, dass Systeme zur Kontrolle der Mitarbeiter von Gesetzes wegen zustimmungspflichtig sind, einzubinden (siehe *1.7.3.2.1 Mitwirkung des Betriebsrates*, *1.7.3.2.2 Personalinformationssysteme*).

Aus Sicht von Endbenutzern ist vor allem die eigene Identität interessant – sei es im Unternehmen, wo meist mehr als eine solche Identität für die Authentifizierung benötigt oder sei es im Internet, wo ebenfalls mit vielen Identitäten agiert wird. Niemand ist für den Erfolg eines Identitätsmanagementsystems von größerer Bedeutung als der Benutzer selbst.

3.5.4.2.2 Ablauforganisation

„*Es gibt zwei Betrachtungsweisen der IT: als Funktion und als inhärenten Bestandteil von Prozessen, Produkten oder Services. Die IT muss zeigen, dass sie die Funktion beherrscht und die Kernprozesse effizienter machen kann*."[807]. Unternehmen müssen heute flexibler denn je auf Änderungen reagieren können. Es ist deshalb oberste Aufgabe der IT, diese Flexibilität zu unterstützen. Neue und veränderte Geschäftsprozesse müssen schnell und sicher umgesetzt werden (siehe *3.4.4.2.8 SOA*).

Generell wird zwischen wertschöpfenden (auch: primären oder Kernprozessen oder Geschäftsprozessen) und unterstützenden (auch: sekundären) Prozessen unterschieden. Wertschöpfende Prozesse sind jene, die an der Erstellung des Produkts, dessen Vermarktung, Distribution und dessen Service beteiligt sind. Die sekundären Prozesse dienen dazu, die primären Prozesse zu unterstützen und gewährleisten eine funktionierende Infrastruktur, damit die primären Aktivitäten durchgeführt werden können. Neben Beschaffung, Personalwirtschaft, Produkt- und Technologieentwicklung ist nach Porter eine der vier sekundären Kategorien die Unternehmensinfrastruktur [Wojda, 2005, Prozessorientierte Ansätze, S 10]. Dazugehörig ist die IT, wo über den Ansatz des *Information Engineering* das Ziel der Abbildung von Geschäftsprozessen in Informationssystemen verfolgt wird. Mezler-Andelberg [Mezler-Andelberg, S 19ff] unterteilt die unterstützenden IT-Prozesse im Rahmen von Identity Management in drei Gruppen: Die *operativen Prozesse* (auch: *Workflow*) sind Tätigkeiten, die tagtäglich durchgeführt werden. Dazu gehört etwa, dass Benutzer angelegt oder mit den entsprechenden Berechtigungen ausgestattet werden. Durch die *administrativen Prozesse* werden Funktionen eines IMS innerhalb eines vorab definierten Rahmens erweitert. Sie ermöglichen es, auf Situationen zu reagieren, für die es keinen passenden operativen Prozess gibt. Im Wesentlichen kann darunter die Pflege des IMS an sich bzw. die Kontrolle der

[807] Aussagen von Adrian Bult, seines Zeichens CEO von Swisscom Mobile, in http://www.computerwelt.at/detailArticle.asp?a=108237&n=6 [20. August 2007]

Datenqualität verstanden werden. Die *gestaltenden Prozesse* passen die Art, wie Ergebnisse erzielt werden, an die Anforderungen an. Dazu gehören etwa die Definition der Schlüsselfelder einer Datenquelle oder die Rollendefinitionen. Sowohl operative als auch administrative Prozesse werden von den gestaltenden beeinflusst. Insgesamt sind diese Prozesse von den Geschäftsprozessen, den gesetzlichen Anforderungen und der Fluktuation der User (Statusänderung eines Mitarbeiters, Outsourcing, Firmenübernahme etc.) abhängig.

GenericIAM[808] ist eine Bemühung verschiedener Unternehmen[809] aus Industrie, Dienstleistung und Produktion, die Prozesse des Identity Managements allgemeingültig, generisch und branchenübergreifend zu definieren, zu beschreiben und zu standardisieren. Ziel der Arbeitsgruppe ist es, immer wieder vorkommende Unternehmensabläufe mit standardisierten Notationen so zu beschreiben, dass sie zur Lösung von Identity Management-Aufgaben verwendet werden können[810]. Im Folgenden wird in dieser Reihenfolge jeweils ein Beispiel für generische Prozesse, Funktionen und Objekte aufgezählt:

- *Onboarding* ist ein generischer Prozess, der die Abläufe, die beim Neueinstieg eines Mitarbeiters in ein Unternehmen involviert sind, beschreibt. Beim Identity Management ist dies das Erfassen von Mitarbeiterdaten und das Gewähren von Zugriffsberechtigungen. Dabei sind typischerweise mehrere Abteilungen (z. B.: Personalabteilung, IT) involviert. Dieser Prozess ist oft abstimmungsintensiv und wenig automatisiert. Verantwortlich für diesen Prozess zeichnet die Personalabteilung.
- Self Service (siehe *3.4.2.5 Self Service*) meint eine generische Funktion, welche die Pflege und Aktualisierung der eigenen Daten ermöglicht. Die Daten sind in der Regel nur dem Benutzer persönlich bekannt. Dazu zählen Geburtstage, Adressen, Rechnungsdaten und Daten rund um den Arbeitsplatz.
- Eine Rolle (siehe *3.6.3 Von der Identität zur Rolle*) wird als generisches Objekt verstanden.

Die Integration von Systemen kann aus informationssicherheitstechnischer Betrachtung nur dann erreicht werden, wenn der Zugriff von Benutzern in jedem der in einem Prozess genutzten Systeme differenziert gesteuert werden kann. Sichere Identitäten sind daher eine fundamentale Voraussetzung für sichere und flexible Geschäftsprozesse.

Bei Identitätsmanagement können neben der Speicherung von digitalen Identitäten in Verzeichnissen oder Chipcards zwei Ebenen unterschieden werden. Das technische Identitätsmanagement umfasst funktionsorientierte Aufgaben wie Passwortmanagement. Das prozessorientierte Identitätsmanagement wird über den Geschäftsprozess gesteuert. Als Beispiel ist Provisioning (siehe

[808] http://www.genericiam.org/ [20. Dezember 2007]
[809] http://www.genericiam.org/aktuelle-mitglieder-3.html [20. Dezember 2007]
[810] Vgl. http://www.iam-wiki.org/Prozessorientiertes_Identity_Management [20. Dezember 2007]

3.4.2.4 Provisioning und Reporting) zu nennen, mit dem der gesamte Lebenszyklus-Prozess von Benutzern abgebildet wird. In der Praxis unterliegt die Userverwaltung normalerweise keinem Kreislauf. Meist liegen verschiedene Attribute der Benutzerdaten isoliert in verschiedenen Verzeichnissen.

Jede Anwendung basiert in irgendeiner Form auf Identitäten. Das gilt insbesondere für die zentralen Geschäftsanwendungen, bei denen alleine die Zugriffsberechtigungen und Geschäftsregeln ohne die Verbindung mit digitalen Identitäten nicht umsetzbar sind. Interne wie externe Geschäftsprozesse funktionieren nur, wenn die Identitäten der Partner, Kunden/Bürger und Mitarbeiter bekannt sind und die Prozesse in Abhängigkeit davon gestaltet werden können. Geschäftsregeln, wie das Limit für Bestellungen, müssen im Kontext der Identität gesetzt werden können. Personalisierte Inhalte können nur geliefert werden, wenn ausreichend Informationen über die Identität des Benutzers vorhanden sind [KCP, 2004, S 1ff].

3.5.4.2.3 Aufbauorganisation

Bedingung für das Funktionieren einer granulierten Rechtevergabe ist eine eindeutige Beschreibung einer Organisation bzw. ihrer Abteilungen und Stellen (siehe *3.5.3.2.7 Verwaltungskennzeichen*). Eine Herausforderung besteht darin, wie der krankheits- bzw. urlaubsbedingte Ausfall eines Mitarbeiters gehandhabt wird, eine andere, wie mit spezifischen Situationen (abteilungsübergreifende Projektteams, temporäre Arbeitskräfte, mobile Mitarbeiter) umgegangen wird.

Zur Abwicklung eines IM-Projekts bedarf es eines Projektteams. Wie in *1.8.3.1.3 Sicherheitsfaktor Mitarbeiter* beschrieben, sollte sich das Team mindestens aus einem Mitglied der Unternehmensleitung, dem Informationssicherheitsverantwortlichen und einem Vertreter der IT-Anwender zusammensetzen.

3.5.4.2.4 Unternehmenskultur

Die bereits erwähnte organisatorische Reife steht in Zusammenhang mit der gelebten Unternehmenskultur. An dieser Stelle ist auf die Ausführungen in *1.8.3.1.2 Exkurs: Unternehmenskultur*, im Speziellen auf die veränderungsfördernden Kräfte, zu verweisen.

Informationssicherheits-Maßnahmen und damit einem Identitätsmanagementsystem wird ambivalent begegnet: Einerseits helfen sie Administratoren und Informationssicherheitsbeauftragten durch ihre administrative Präsenz, die Arbeitsverfassung des Einzelnen im gewünschten Rahmen zu halten. Andererseits werden sie als Exekutive des Systemzwanges im Unternehmen erlebt. In dieser Verkehrung werden sie als Kontrollinstanz verstanden und es wird ihnen misstrauisch bis ablehnend begegnet. Die IT-Abteilung hat damit zugleich eine sichernde und eine entsichernde Seite.

Informationssicherheit nutzt ihr Potential zur produktiven Gestaltung der Unternehmenskultur bislang zu wenig, hat aber die Chance, eine „sinnliche Belebung in oft sachliche Zwänge zu bringen“ und so regulierend auf die Gesamtverfassung des Unternehmens einzuwirken[811].

3.5.4.2.5 IM und Outsourcing

Identitätsmanagement und Compliance sind Aufgaben, die außerhalb der Kernkompetenz der Unternehmen liegen. Ein vertrauenswürdiger Outsourcing-Anbieter, der die Verwaltung von Identitäten übernimmt, schafft den Freiraum, um sich auf die eigentlichen Stärken konzentrieren zu können. Das Outsourcing von Informationssicherheit und das damit verbundene Identitätsmanagement erfordert vom Management eines Unternehmens grundsätzliche Überlegungen bezüglich der Verantwortlichkeit gegenüber den *Shareholdern*, Stakeholdern sowie den Inhabern von Daten. Die Kontrolle der vorgegebenen Informationssicherheitsmaßnahmen stellt hohe Anforderungen an das Management. Ein weiterer wesentlicher Aspekt besteht in der Gewährleistung der Kompatibilität der im Outsourcing der Informationssicherheit verankerten Prozesse mit nationalem bzw. internationalem Recht[812].

Identitätsmanagement kann im Zusammenhang mit Outsourcing eine zweite Bedeutung haben und als Bindeglied zwischen Unternehmen und Outsourcing-Partner dienen. *Verknüpftes Identity Management* ist gleichbedeutend mit der problemlosen Portierbarkeit von Komponenten der Nutzeridentität über traditionelle Grenzen hinaus [Sun, 2006, S 3].

3.5.4.2.6 Portalverbund

Für den Portalverbund gibt es darüber hinaus spezielle Erfordernisse in der Umsetzung.

Für den Anwendungsbetreiber ergeben sich folgende organisatorische Aufgaben [BMI-3, 2006, S 13]:

- Festlegung der Sicherheitsklassen (siehe *3.5.3.2.3 Sicherheitsklassen*).
- Publikationen beim Depositar: Rechte, Sicherheitsklassen, zugriffsberechtigte Stellen, SLA und Kontakte (siehe *3.5.3.2 Definition Portalverbund*).
- Definition zusätzlicher Sicherheitsauflagen (siehe *1.8 Unternehmenssicherheit*).
- Betriebshandbuch und Deployment-Dokumentation.
- Revisionsregeln definieren (siehe *3.5.3.2.9 Revision*).

Für die zugriffsberechtigte Stelle gibt es folgende organisatorische Hürden zu meistern [BMI-3, 2006, S 17]:

- Verwaltung der Benutzer und ihrer Rechte an eigenen und fremden Anwendungen mit der gebotenen Sorgfalt.

[811] Vgl. http://www.securitymanager.de/magazin/artikel_1524.html [8. Dezember 2007]

- Verpflichtung der Benutzer zur Einhaltung der Informationssicherheitsmaßnahmen und Datenschutzbestimmungen (siehe *1.8 Unternehmenssicherheit*).
- Einrichtung des Zugriffs auf Anwendungen (z. B.: Portalverbundvereinbarung, Zertifikatsaustausch).

3.5.4.3 Technische Maßnahmen

Für die zugrundeliegenden Technologien kann auf die Ausführungen in *3.4 Komponenten und Funktionen eines Identitätsmanagementsystems* bzw. *3.5.3.2.4 Techniken und Technologien für Portalverbund* verwiesen werden.

Bei der technischen Umsetzung des Portalverbundes gilt es, eine Reihe von Überlegungen anzustellen und diese konzertiert umzusetzen. Wie die Realisierung beim Arbeitgeber des Autors (siehe *Abbildung 55: PV-Umsetzung*) zeigt, reicht das Spektrum von Verzeichnistechnologien über Zertifikatsverwaltung bis hin zum Aufbau einer mehrteiligen Identitätsmanagement-Infrastruktur. All diese Maßnahmen müssen den Ansprüchen der Informationssicherheit gerecht werden.

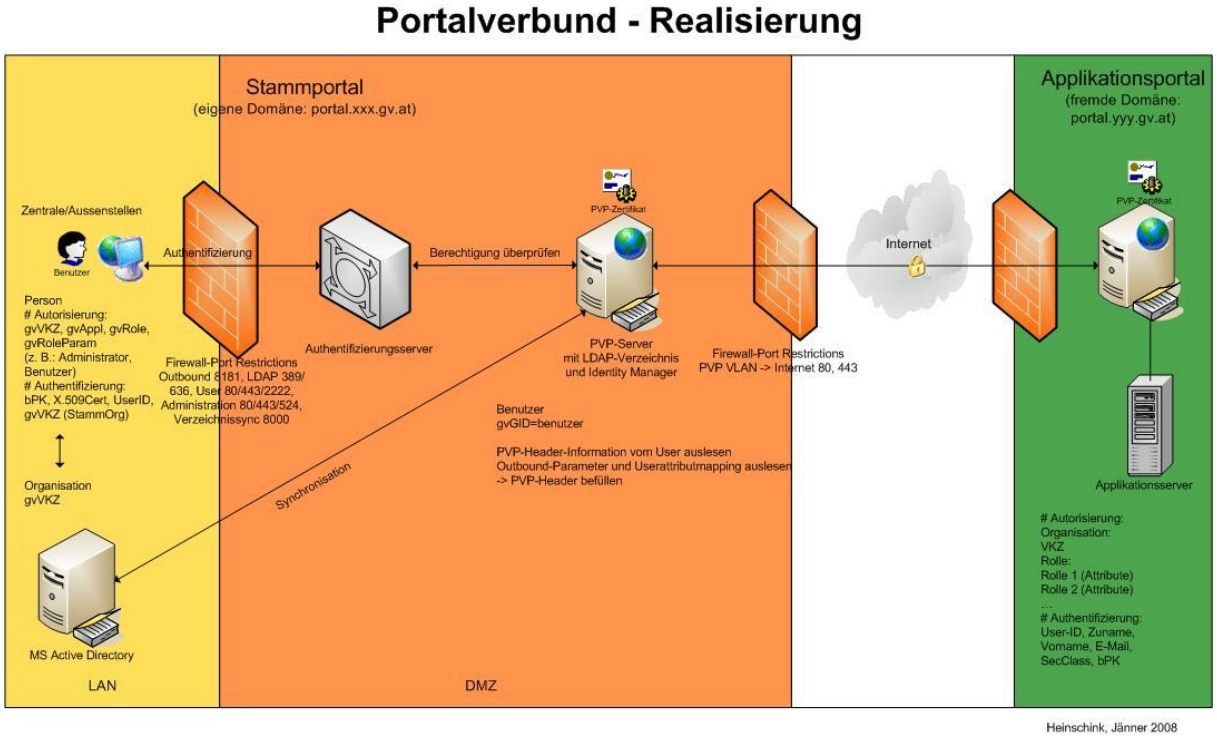


Abbildung 55: PV-Umsetzung

3.5.4.3.1 Bereitstellung und Management der Infrastruktur

Folgende (Mindest-)Komponenten und Mechanismen sind zur Realisierung des Portalverbunds im speziellen, respektive Identitätsmanagementsystems im allgemeinen, in auf einander abgestimmter Form bereitzustellen und laufend zu verwalten: Internetanbindung, Netzwerk (LAN – VLAN, WLAN)

[812] Vgl. http://www.isss.ch/events/ft1998.11/index.html [8. Dezember 2007]

(siehe *1.3.4.2.1 TCP/IP-Sicherheit*, *1.3.4.2.7 Wireless LAN-Sicherheit*), DMZ, (Web-) Server, Verzeichnis (siehe *3.4.1.1 Verzeichnisdienst*), Datenbank, Zertifikate (siehe *1.7.2.1.6 Digitale Zertifikate*), Backup (siehe *1.7 Schutzmaßnahmen und Gegenstrategien*, *3.5.4.3.4 Datensicherung und -archivierung*), remote Access (siehe *1.5 Exkurs: Mobiles Arbeiten*), Benutzerverwaltung und starke Authentifizierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*, *3.4.2 Access-Management und Technologien zur Autorisierung und Authentifizierung*, *3.4.2.3 Chipkarten*). In Abhängigkeit von den Vorgaben aus der Informationssicherheit (siehe *1.8.2.5 Umsetzung des IT-Sicherheitsplans*) ist es unerlässlich, die wesentlichen Anbindungen und Systeme redundant auszulegen.

Die Herausforderung besteht darin, dass Eingriffe (z. B.: Netzwerkaufbau, Firewall-Umstellung, Änderung im Verzeichnis, Betriebssystemwechsel, Informationssicherheitsmaßnahme) in eine Komponente dieser Infrastruktur durch die Abhängigkeiten Folgen für die restlichen Teile bedeuten können. Die Erfahrung zeigt, dass die Komplexität durch den Einsatz dedizierter Hardware zumindest für den Kernbereich (Authentifizierungsserver, PVP-Server) reduziert werden kann.

Des Weiteren sollten die Systeme so ausgelegt werden, dass sie jederzeit erweiterbar sind. Um eine Expansion respektive eine sanfte Migration zu ermöglichen, lehrt die Praxis, ein Testsystem in Analogie zur Produktivumgebung aufzubauen.

3.5.4.3.2 Datenqualität und Identitätsspeicher

Ohne ausreichende Datenqualität bleiben viele der Ziele, die von Identity Management erwartet werden, unerreichbar[813]. Eines der Ergebnisse der bereits erwähnten Analyse von Gartner und Völcker Informatik (siehe *3.5.4.1 Erfolgsfaktoren*) lautet, dass die unzureichende Qualität der vorhandenen Daten viele Identitätsmanagement-Projekte zeitlich und finanziell in Mitleidenschaft zieht. „*Üblicherweise liegt die Datenqualität bei den häufig genutzten Identitätsspeichern Active Directory oder Lotus Notes bei 80 bis 85 Prozent, in stark fragmentierten ERP-Landschaften sogar noch weit darunter. Initiale Datenqualitäten von über 95 Prozent sind dagegen nur ganz selten anzutreffen*." konkretisiert *Eckhard Völcker*, Vorstandsvorsitzender von Völcker Informatik. Außerdem machen viele Unternehmen den Fehler, die Erzielung einer möglichst hohen Qualität der Daten und die Benutzerverwaltung als rein technisches Problem einzustufen.

Es kann keine zuverlässige Autorisierung und Authentifizierung geben, wenn die User gezwungen sind, sich gegen eine unzuverlässige Datenbasis auszuweisen. Bei Identity Federation (siehe *3.2.3 Identitätsföderation und -kontrolle*) geht es darum, Vertrauen herzustellen. Das hängt einerseits vom Sicherheitsniveau des Identity Providers und der Stärke der Authentifizierung ab, andererseits von der

[813] Vgl. http://www.kuppingercole.de/articles/datenqualitaet [14. Jänner 2008]

Qualität der von ihm verwenden Identitätsdaten. Compliance-Ansprüche können ohne verlässliche Datenbasis nicht erfüllt werden.

In jedem Fall gilt, dass die Qualität von Identitätsinformationen als strategische, unternehmensübergreifende Aufgabe begriffen werden muss. Qualität setzt definierte Prozesse und Verantwortlichkeiten (siehe *3.5.4.2.2 Ablauforganisation, 3.5.4.2.3 Aufbauorganisation*) für Änderungen voraus, vom Self Service bis hin zu Stellen im Unternehmen, die die Qualität der Daten messen und bei Problemen frühzeitig gegensteuern. Qualität kann dabei nur durch eine integrierte Sicht entstehen: entweder durch die Nutzung eines Datenbestandes an verschiedenen Stellen (z. B.: Identity Federation) oder durch eine Synchronisation von Informationen, wie sie über Provisioning-Lösungen realisiert werden[814].

3.5.4.3.3 Usability

Aufgrund der Verschiedenheit der Applikationen ist bei der Umsetzung einer Portalverbundlösung bzw. eines Identitätsmanagementsystems darauf zu achten, dass die Schnittstelle zum Benutzer (siehe *3.4.4.2.9 User Interface*) möglichst einfach gestaltet wird. Durch die intuitive Verwendbarkeit akzeptiert der User die Lösung und trägt damit zum Erfolg bei (siehe *3.5.4.2.1 Stakeholder*).

3.5.4.3.4 Datensicherung und -archivierung

Eine Herausforderung für die IT-Abteilung ist die Sicherung bzw. langfristige Archivierung von Identitätsdaten. Auf der einen Seite wird den Mitarbeitern über Self Service (siehe *3.4.2.5 Self Service*) und der informationellen Selbstbestimmung (siehe *3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*) eine Handhabe über die eigenen Daten gegeben, auf der anderen Seite werden die Daten durch die IT-Administration gesichert und im Schadensfall wiederhergestellt. Besonders herausfordernd ist der Umgang mit Pseudonymen.

In diesem Zusammenhang gilt es für jedes Unternehmen zu klären, ob über die gesetzlichen Vorgaben hinaus interne Usancen und Richtlinien existieren, auf deren Basis Identitätsdaten und Berechtigungsvergaben (siehe *3.5.3.2.9 Revision*) aufzubewahren sind.

3.5.4.3.5 Künftige Anforderungen an die IT

In der Studie „Zukunft digitale Wirtschaft“ von *Roland Berger Strategy Consultants*[815] und der deutschen Bitkom [Berger, Bitkom, 2007, S 6ff] werden die wesentlichen IKT-Metatrends identifiziert:

- Konvergenz: Die technologischen Plattformen moderner IKT werden zusammenwachsen. Unternehmen wie Festnetz-, Mobilfunknetz- und Kabelnetzbetreiber, die bislang in getrennten

[814] Vgl. http://www.tecchannel.de/sicherheit/identity_access/468274/ [15. Jänner 2008]
[815] http://www.rolandberger.com/ [9. Dezember 2007]

Märkten aktiv waren, werden immer mehr zu Konkurrenten. Sie alle erschließen neue Geschäftsfelder und weichen die klare Trennung zwischen den Produktbereichen auf.

- Flexibilität: Unternehmen werden zunehmend verschiedene Prozesse und Funktionen wie Forschung, Einkauf, Produktion und Vertrieb entkoppeln und neu miteinander kombinieren bzw. parallelisieren. IT unterstützt dabei die Entwicklung flexibler Geschäftsprozesse sowie die Einbindung von Lieferanten (siehe *3.2.3 Identitätsföderation und -kontrolle*).
- Ubiquität (siehe *1.5.2 Ubiquitäres Computing*): Die Studie sieht die weitgehende und beschleunigte Durchdringung unserer Umwelt mit IK-Technologien. In Zukunft werden sich einzelne Geräte zu Systemen zusammenschließen und miteinander kommunizieren. Dazu kommt, dass sich die Dateneingabe revolutionieren wird: Statt mit Maus und Tastatur werden Computer und elektronische Geräte mittels Touchscreen oder durch Sprache bedient werden.
- Datennutzbarkeit: Die Datenmenge, die weltweit gespeichert wird, wächst exponentiell. IKT sind nicht nur Treiber dieser Entwicklung, sondern es ist auch Aufgabe moderner IT, diese Daten effizient zu verwalten und besser nutzbar zu machen.

Ausgehend von diesen Metatrends wurden für die Studie über 300 Informations- und Kommunikationstechnologien und -dienste untersucht und dabei folgende Wachstumsfelder herausgearbeitet:

- Eingebettete Systeme (engl. *embedded systems*) finden sich in Waschmaschinen, Herzschrittmachern oder Computertomografen.
- Serviceorientierte Software-Architekturen (siehe *3.4.4.2.8 SOA*) werden in Unternehmen eingesetzt, um Software-Applikationen in einzelne Services zu zerlegen. Diese werden damit zu eigenständigen, wieder verwendbaren Softwaremodulen.
- Ein weiteres Wachstumsfeld sind IT Utility-Services. Dazu zählen beispielsweise E-Mail-Provider, Software- und Speicherplatzanbieter und andere Dienstleister, die es möglich machen, weltweit auf Applikationen oder Daten zuzugreifen. IT Utility-Services erlauben den flexiblen Zugriff auf Rechenleistung, Programme und Speicherplatz, ohne dass Unternehmen oder Organisationen dafür selbst IT-Kapazitäten aufbauen müssen.
- Ein verhältnismäßig kleiner Markt mit allerdings ausgesprochen hohen Wachstumschancen ist die Biometrie (siehe *1.7.2.3 Biometrie*). Haupteinsatzgebiet bildet branchenübergreifend die Informationssicherheit.
- Digitales Rechtemanagement (siehe *2.3.3.5 Digital Rights Management*) umfasst alle Verfahren zum Schutz von Urheber- und Vermarktungsrechten an digitalen medialen Inhalten und ermöglicht die individuelle Verwertung und Abrechnung. DRM ist nicht nur bei Fragen der Softwarepiraterie relevant, sondern hilft Unternehmen auch beim Schutz vor Missbrauch ihrer Daten (siehe *3.4.2.2 DRM-Funktion*).

Darüber hinaus sieht die Studie interessante Wachstumsfelder vor allem in verschiedenen Breitbandtechnologien, RFID (siehe *2.3.3.3 RFID*), Telematik sowie Informationssicherheit (siehe *1 Informationssicherheit im privaten und betrieblichen Umfeld*).

Für Unternehmen bedeutet die rasante technische Entwicklung, dass sich die Lebenszyklen von technischen Geräten, Applikationen und Produkten weiter verkürzen werden. Unternehmen und ihre (IT-)Mitarbeiter müssen permanent Know-how aufbauen, um die Anforderungen abdecken zu können.

Bei näherer Betrachtung der aktuellen Marktentwicklungen und -anforderungen werden die erläuterten Trends noch um einige Herausforderungen für die Unternehmen ergänzt:

- Virtualisierung (siehe *1.3.2.2 Gegenmaßnahmen*: *Virtualisierung*).
- *Green-IT*: Aktivitäten, die die Nutzung von Informationstechnologie über ihren gesamten Lebenszyklus hinweg umwelt- und ressourcenschonend gestalten. Im Vordergrund stehen dabei zum einen der Energieeinsatz bei der Nutzung von Hardware und zum anderen die verwendeten Materialien und Produktionsmittel.
- Web 2.0 (siehe *1.1 Problemstellung und Herausforderung: Web 2.0*): Die Transformation zum „Unternehmen 2.0“, unterstützt durch eine partizipative Unternehmenskultur, Web 2.0-Lösungen und SOA, wird immer mehr als unternehmensstrategische Aufgabe gesehen. Die weiter fortschreitende Öffnung der Unternehmen und die damit verbundenen neuen Technologien bringen neue Informationssicherheitsgefahren mit sich.
- Wissensmanagement und Collaboration: Mit dem Einzug von Web 2.0 in Unternehmen entwickelt sich eine neue Form von Wissensmanagement und damit eng verknüpfter Konzepte wie Collaboration. In Verbindung mit Social Software wie Wikis, Blogs und Social Bookmarking werden die Inhalte durch den Mitarbeiter erstellt. Über die Kommentierung und Bewertung wird die Qualität gesichert. Wissensmanagement wird somit zu einem zentralen Unternehmens- und IT-Thema. Durch diese Anwendungen verändern sich Geschäftsprozesse, neue Vertriebswege werden etabliert und die Benutzer wissen in ihrer Gesamtheit als „kollektive Intelligenz“ mehr als die Experten, weil sie sich in Communities miteinander austauschen und lose, bedarfsorientierte Beziehungen knüpfen [Bitkom-2007, S 7].
- Corporate Governance (siehe *2.2.1 Digitale Identität*: *Corporate Governance*), IT-Governance (siehe *1.8.1 Ziele und Aufgaben des Informationssicherheitsmanagements*: *IT-Governance*).
- *Corporate Social Responsibility*: umschreibt den freiwilligen Beitrag der Unternehmen zu einer nachhaltigen Entwicklung, der über die gesetzlichen Forderungen hinausgeht. Es steht für verantwortungsvolles, unternehmerisches Handeln in der eigentlichen Geschäftstätigkeit, in ökologisch relevanten Aspekten, in der Beziehung mit Mitarbeitern und im Austausch mit den Stakeholdern.

- EU-DL-Richtlinie: Die Herstellung eines gemeinsamen Marktes beinhaltet auch die freie grenzüberschreitende Erbringung von Dienstleistungen. Die Dienstleistungsrichtlinie der EU soll den grenzüberschreitenden Handel mit Dienstleistungen fördern. Besonderes Gewicht kommt dabei dem Abbau von bürokratischen Hindernissen zu, die den grenzüberschreitenden Dienstleistungsverkehr behindern. Die Richtlinie ist Ende Dezember 2006 in Kraft getreten und gibt den Mitgliedsstaaten bis Ende 2009 Zeit für die Umsetzung in nationales Recht. Eine große Herausforderung für die öffentliche Verwaltung ist die Vorgabe eines „einheitlichen Ansprechpartners". Dieser muss als One-Stop-Shop im Bereich des E-Government in der Lage sein, alle Verfahren und Formalitäten elektronisch abzuwickeln, unterschiedliche Zuständigkeiten müssen abgedeckt werden.

3.6 INFORMATIONELLE SELBSTBESTIMMUNG IM BETRIEBLICHEN UMFELD

An dieser Stelle sollen Überlegungen beschrieben werden, wie auf Basis der Portalverbund-Umsetzung ein umfassenderes Identitätsmanagementsystem entstehen kann. Obwohl viele Technik-Elemente und Prozesse durch die Realisierung einer Portalverbund-Lösung bereits existieren, sind sowohl technische als auch organisatorische Änderungen und Ergänzungen erforderlich.
Der Fokus der Ausführungen liegt weniger bei den bereits ausführlich behandelten Techniken und Technologien als bei der Rollenkonzeption und den organisatorischen Veränderungen.
Die Bestrebung ist, ein System zu schaffen, dass – unter Berücksichtigung der Informationssicherheit – neben dem Nutzen für Mitarbeiter und Unternehmen vor allem den Aspekt der informationellen Selbstbestimmung für den Anwender unterstützt.

3.6.1 FUNKTIONSERWEITERUNG DES PORTALVERBUNDS IN RICHTUNG IDENTITÄTSMANAGEMENTSYSTEM

Die erforderlichen technischen Komponenten wurden unter *3.4 Komponenten und Funktionen eines Identitätsmanagementsystems, 3.5.3.2.4 Techniken und Technologien für Portalverbund und 3.5.4.3 Technische Maßnahmen* vorgestellt. Die wesentlichen Bestandteile sind aus *Abbildung 55: PV-Umsetzung* zu ersehen. Auf dieser Basis sind – abhängig vom Bestehenden bzw. der Zieldefinition – Investitionen in den Auf- bzw. Ausbau einer Verzeichnisstruktur, eines Portals und Schnittstellen (auch: Konnektoren) zu Identitätsspeichern bei gleichzeitiger Berücksichtigung der Anforderungen der Informationssicherheit (z. B.: Verfügbarkeit, Vertraulichkeit) zu tätigen. Um dem Benutzer die Hoheit über seine Daten zu geben, sind diesem Arrangement Werkzeuge zur Pseudonymisierung und Anonymisierung beizufügen. Diesbezügliche Ausführungen sind unter *2.2.2 Pseudonymität, 2.2.3 Anonymität, 2.4.3 Säule 3: Datenschutz durch Technik, 2.4.4 Anonym Surfen, 2.4.5 Anonym Mailen, 2.4.6 Pseudonym Surfen und Mailen* zu finden.

Die folgende Abbildung zeigt ein erweitertes Identitätsmanagementsystem mit der Integration von zusätzlichen Identitätsspeichern (Personalinformationssystem, Gleitzeit etc.), wie es im Umfeld des Autors dieser Arbeit im Entstehen ist.

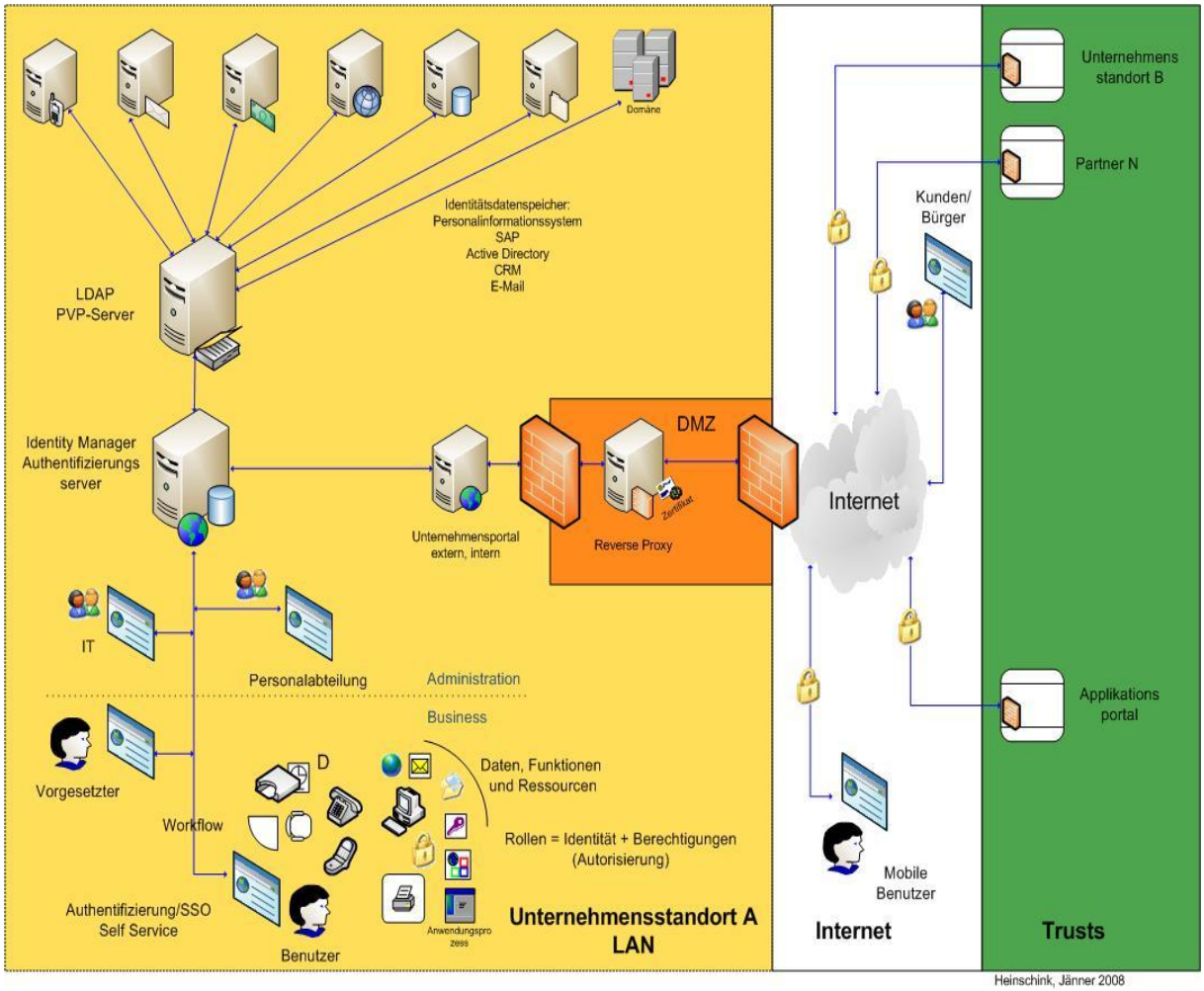


Abbildung 56: Identitätsmanagement auf Basis von PV

3.6.2 AUFTEILUNG DER VERWALTUNG DER BENUTZERDATEN

Mithilfe eines Identitätsmanagementsystems soll die Verwaltung der Benutzerdaten – im Sinne der Idee des bereichsspezifischen Personenkennzeichens (siehe *2.4.7 Bereichsspezifisches Personenkennzeichen und Bürgerkarte im E-Government*) zur Verhinderung der Gesamtsicht auf die Daten eines Einzelnen – aufgeteilt werden. Bislang wird diese Tätigkeit ausschließlich vom EDV-Administrator erledigt. Organisatorisch ist eine Arbeitsteilung hinsichtlich Identitätsverwaltung auf IT-Abteilung, Personalabteilung und Mitarbeiter selbst (siehe *3.4.2.5 Self Service*) vorstellbar. Diese Dreiteilung bringt mit sich, dass die Gesamtsicht des Verwaltungspersonals auf die Daten des einzelnen Mitarbeiters eingeschränkt wird.

Ein mögliches Szenario könnte sich wie folgt darstellen: Bei Neueintritt eines Mitarbeiters erstellt die Personalabteilung in Übereinstimmung mit dem zuständigen Vorgesetzten die digitale Identität. Dabei

werden dem Mitarbeiter Zugriff auf Daten, Funktionen und Ressourcen gewährt. Durch Policies wird sichergestellt, dass er auf jenen Systemen Rechte erhält, die seiner Organisationsrolle entsprechen. Der Automatismus eines Identitätsmanagementsystems erlaubt somit dem Arbeitnehmer, bereits am ersten Tag seine Tätigkeit aufnehmen zu können.

Verändert sich nun der Status der Daten eines Mitarbeiters (Namensänderung durch Heirat, Geburt eines Kindes, Änderung des Wohnorts, Bankverbindung, Jobrochade, Bürowechsel etc.), ist dieser in der Pflicht bzw. ist es in seinem Eigeninteresse (z. B.: Erhalt des Mehrkinderzuschlages), die Werte zu aktualisieren. Für den Vorgesetzten gibt es lediglich eine limitierte Sicht auf die Daten des Mitarbeiters. Er hat – ebenso wie die Personalabteilung – kontrollierende Funktion hinsichtlich des Ergebnisses des Mitarbeitergesprächs, der Gehaltsdaten, der Entwicklung auf der Kostenstelle etc.

Bei Ausscheiden des Mitarbeiters ist wieder die Personalabteilung am Zug, somit gewährleistet, dass keine Karteileichen im System bleiben, der Identitätslebenszyklus ordnungsgemäß beendet wird.

Die technischen Arbeiten obliegen weiterhin der IT-Abteilung: mobiles Arbeiten (siehe *1.5 Exkurs: Mobiles Arbeiten*), Sicherheitstechniken (siehe *1.7.2 Technische Gegenmaßnahmen*) und die Bereitstellung der Identitätsinfrastruktur (siehe *3.5.4.3.1 Bereitstellung und Management der Infrastruktur*). Der IT-Mitarbeiter erstellt die in diesem Kontext erforderlichen Regeln und Policies, der Informationssicherheitsverantwortliche (siehe *1.8.2.6 Management von Informationssicherheit, 1.8.3.1.3 Sicherheitsfaktor Mitarbeiter*) muss dazu die Freigabe erteilen („Vieraugenprinzip“).

Damit werden Ressourcen in der Unternehmens-IT frei für andere notwendige Arbeiten, der User gewinnt Hoheit über seine Daten, hat aber eine Bringschuld und trägt auch mehr Verantwortung. Die Kontrolle liegt entsprechend den Anforderungen an Identitätsmanagementsysteme (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz*) beim Benutzer.

Identitätsmanagementsysteme sollen im betrieblichen Umfeld dem Benutzer die größtmögliche Freiheit über seine Daten geben. Durch das Splitten der Benutzerverwaltung auf Personalabteilung, IT-Administration und Benutzer erhöht sich zudem die Benutzerproduktivität bei gleichzeitiger Reduktion der Administrationskosten auf IT-Seite (siehe *3.5.1 Anforderungen und Nutzen aus Mitarbeitersicht, 3.5.2.2 Produktivität und Kosten*).

3.6.3 VON DER IDENTITÄT ZUR ROLLE

In Kapitel *2.2.1 Digitale Identität* wurde bereits der Zweck von Digitalen Identitäten und die Bedeutung von Benutzerprofilen und Rollen erläutert. Die einen Benutzer charakterisierenden Eigenschaften werden demnach als Benutzerprofil verstanden. Dabei entsteht der Kontext zu den Geschäftsprozessen. Identitäten können in den Formen leere Identität (=Anonymität), Pseudo-/Teilidentität (=Pseudonymität), und vollständige Identität auftreten.

Die Zuweisung von Berechtigungen zu einer Identität, sprich die Autorisierung (siehe *2.2.6 Autorisierung, Authentifizierung und Authentizität*), wird durch Rollen abgebildet. Berechtigungen

stehen für den Zugriff auf Daten, Funktionen und Ressourcen. Die Zugriffsbedingungen werden formal im Rahmen eines Informationssicherheitskonzepts in Policies (siehe *1.8.2.4 Erstellung eines Informationssicherheitskonzepts*) festgehalten.

Rollen gruppieren Berechtigungen, die Benutzer auf Systemen haben. Sie vereinfachen die Administration dadurch, dass nicht jedem Benutzer eine Vielzahl von Einzelberechtigungen zugeordnet werden muss, sondern diese ihre Berechtigungen über Gruppenzugehörigkeiten oder zugewiesene Rollen erhalten. Rollen entsprechen einer logischen Tätigkeit, für die verschiedene Einzelrechte benötigt werden. So können Rollen beispielsweise ein Aufgabengebiet, eine Stellenbeschreibung oder eine Organisationseinheit repräsentieren. Rollen dienen dazu, Berechtigungskonzepte verständlich zu halten[816].

3.6.3.1 Rollenkonzepte

Die meisten Benutzerverwaltungen decken einen zu kleinen Ausschnitt aus den relevanten Rollenkonzepten ab. Genügt häufig im ersten Schritt ein gruppenorientierter Ansatz, so ist spätestens bei der Integration des nächsten Zulieferers oder bei der Anbindung der nächsten Anwendung ein Modell erforderlich, welches ein aufgabenorientiertes Rollenkonzept erfordert. Für eine zentrale Benutzerverwaltung ist deshalb eine flexible Abbildung von allen in der Praxis vorkommenden Rollenkonzepten unabdingbar [Doubleslash, 2006, S 8f]:

- Aufgabenorientiertes Rollenkonzept (Abbildung der Tätigkeiten, Aufgaben, Stellenbeschreibungen): In der traditionellen Organisationslehre wird mit dem Begriff der Rolle die Position eines Benutzers innerhalb einer Organisation bestimmt. Rollen dienen hierbei dazu, Organisationsstrukturen zu veranschaulichen, Hierarchien abzubilden, Vertretungsregeln festzulegen und Aufgaben zu verteilen. Für diesen Zweck wird in Rollenkonzepten der Begriff Organisationseinheit verwendet.
- Gruppenorientiertes Rollenkonzept (Typen von Benutzern, Gruppierung von Benutzern, Verantwortlichkeiten): Im Rahmen kompetenzorientierter Rollenbildung beschreibt eine Rolle eine Grundmenge von Qualifikationsanforderungen, die eine Person erfüllen muss, um bestimmte Tätigkeiten ausführen zu können. Die Anforderungen, die organisationsneutral formuliert werden, umfassen zunächst die Fachkompetenz, also fachbezogene und fachübergreifende Kenntnisse, Fähigkeiten und Fertigkeiten, die Mitarbeitergruppen dazu befähigen, in beruflichen Situationen sach- und fachgerecht zu handeln.
- Organisationsorientiertes Rollenkonzept (Abbildung der Unternehmensstruktur, Gliederung, Abteilungen): Während die kompetenz- und aufgabenorientierte Rollenansätze ihren Schwerpunkt auf die Ablauforganisation legen, richtet sich der organisationsorientierte Ansatz an der

[816] Vgl. http://www.iam-wiki.org/Rollen [9. Dezember 2007]

Aufbauorganisation eines Unternehmens aus. Dazu werden Stellen mit ähnlichen organisatorischen Charakteristika gruppiert. Der Vorteil dieses Rollenkonzepts liegt darin, dass sich Prozess- und Organisationsdefinition voneinander trennen lassen. Im funktionalen Kontext stellt eine Rolle das Aufgabenpaket eines Mitarbeiters dar, wobei sowohl mehrere Mitarbeiter eine Rolle wahrnehmen können als auch eine Person verschiedene Rollen innehaben kann. Die Aufgaben können im Rahmen einer Baumstruktur betrachtet werden, deren Wurzel die Gesamtaufgabe darstellt, die in mehreren Ebenen in Elemente zerlegt wird. Stellen werden dadurch gebildet, indem Elementaraufgaben zusammengefasst werden. Dazu wird die Gesamtaufgabe des Unternehmens im Markt schrittweise zerlegt und bildet so hierarchisch strukturierte Aufgaben mit einem hohen Detaillierungsgrad. Um die Rollen erstmalig zu erstellen, werden die formalen Geschäftsprozesse analysiert und widerspruchsfrei abgebildet. Im nächsten Schritt werden ähnliche Aufgaben oder solche, die gemeinsam ausgeführt werden müssen, zu Rollen zusammengefasst. An der Verwendung von Adjektiven im Namen der Rollen lässt sich die Tätigkeit erkennen.

Die wesentlichen Komponenten von Datenzugriffsmodellen sind [Mezler-Andelberg, 2007, S 42 ff]:

- Benutzer: ist die physische Person, die mit einem System arbeitet.
- Session: wird durch das Anmelden und Arbeiten eines Benutzers erzeugt.
- Subjekt: das Arbeiten mit Systemen bedingt Prozesse, diese werden als Subjekt bezeichnet.
- Objekt: steht für jede Form von Ressourcen (z. B.: Datei, Drucker, Datenbank).
- Operation: ist eine Aktion, die von einem Subjekt auf einem Objekt angewendet wird (z. B.: lesen, schreiben).
- Berechtigung: ist die Erlaubnis für die Kombination von Objekt und Operation.

Rund um diese Komponenten entstanden verschiedene Datenzugriffsmodelle, wie *Discretionary Access Control-Model* (kurz: *DAC*) oder *Mandatory Access Control-Model* (kurz: *MAC*), um die Vertraulichkeit und Integrität (siehe *1.2.2 Anforderungen an die Informationssicherheit: Vertraulichkeit, Integrität*) von Daten zu wahren. MAC wird beispielsweise in Windows Vista in Form des *Biba*-Modells[817] eingesetzt. Aus einer Weiterentwicklung der Modelle durch das *National Institut of Standards and Technology* (kurz: *NIST*)[818] entstand *Role-Based Access Control* (kurz: *RBAC*)[819].

[817] Hier werden Informationen nicht vor dem Lesen, sondern vor Manipulation durch Unbefugte geschützt. Das Biba-Modell zielt auf die Datenintegrität ab und wird beispielsweise als Schutzmaßnahme für sicherheitsrelevante Systeme wie Firewalls verwendet.
[818] http://www.nist.gov/ [10. Dezember 2007]
[819] http://csrc.nist.gov/groups/SNS/rbac/standards.html [10. Dezember 2007]

3.6.3.2 Role-Based Access Control und Authority Model

RBAC ist ein Berechtigungskonzept in Mehrbenutzersystemen. Die Zugriffskontrolle auf Daten, Funktionen oder Ressourcen erfolgt dabei über Rollen. Dabei werden den Benutzern Rollen zugeordnet. Ein Benutzer kann mehrere Rollen inne haben und einer Rolle können mehrere Benutzer zugeordnet sein (n:m-Beziehung). Die Berechtigungen eines Benutzers definieren sich aus der Rolle, in der er beim Zugriff auf den Computer agiert. Einer Rolle können mehrere Rechte zugeordnet werden und vice versa (n:m-Beziehung). In einer Rolle werden also eine Menge einzelner, fein granulierter Rechte zusammengefasst. Eine Rolle stellt damit ein Rechtebündel dar, das zur Erfüllung einer bestimmten Aufgabe benötigt wird[820].

Für die Verwaltung dieser Zuordnungen werden in der Regel Identitätsmanagementsysteme verwendet. Diese ermöglichen die Zuordnung von Benutzern in 1:n Computersystemen über die Bindung an zumindest eine Rolle. Der Einsatz eines Rollenmodells beim Provisioning (siehe *3.4.2.4 Provisioning und Reporting*) verringert die Mengenproblematik beim Benutzermanagement und führt zu einem konsistenten Berechtigungskonzept.

Mithilfe des *Authority Models*, entwickelt von der *Stanford University*[821], können Rollen anschaulich erläutert werden [Mezler-Andelberg, 2007, S 51f]. Die Gliederung unterteilt sich in eine System- und eine Businesssicht. In der Systemsicht werden die individuellen Berechtigungen aus einer oder mehreren Applikationen zu neutralen Berechtigungen zusammengefasst. Diese Berechtigungen werden zu Aufgaben gruppiert. Unter Aufgaben werden einzelne Tätigkeiten verstanden, die ein Mitarbeiter zu erledigen hat. Die nächste Ebene sind Funktionen in den Geschäftsprozessen. Diese bestehen aus einer Reihe von Aufgaben. Eine oder mehrere Funktionen bilden nun eine Rolle, die einem Benutzer zuordenbar ist.

An einem *Use Case* soll anhand des Authority Models ein Teilbereich der Jugendwohlfahrt aus dem betrieblichen Umfeld des Autors illustriert (siehe *Abbildung 57: Jugendwohlfahrt - Authority Model*) werden.

[820] Vgl. http://www.iam-wiki.org/Role_Based_Access_Control_%28RBAC%29 [10. Dezember 2007]
[821] http://www.stanford.edu/ [10. Dezember 2007]

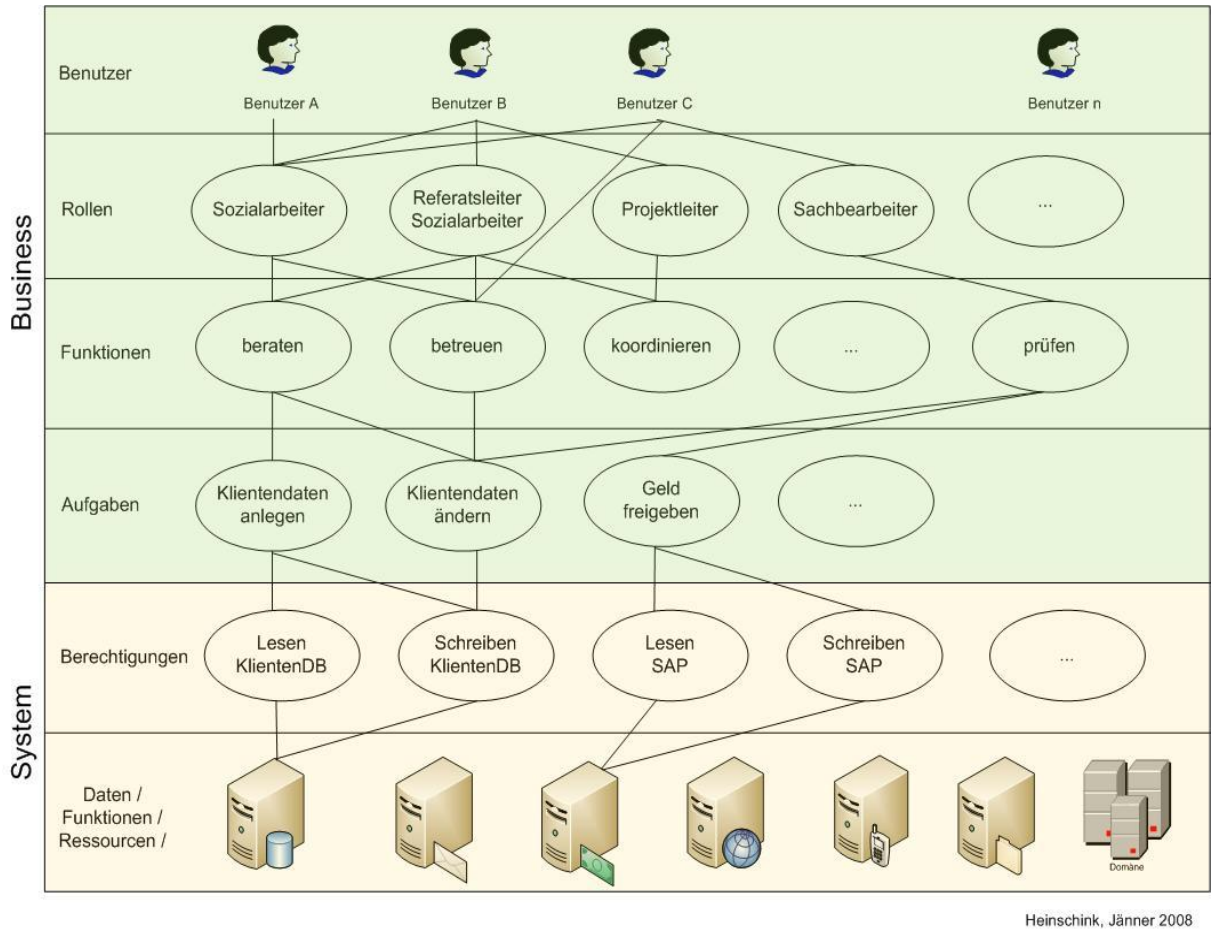


Abbildung 57: Jugendwohlfahrt - Authority Model

3.6.3.3 Erarbeitung eines Rollenkonzepts

Die Erarbeitung eines Rollenkonzepts stellt eine große Herausforderung bei der Einführung eines Identitätsmanagementsystems dar. Das liegt unter anderem daran, dass es bei den meisten Unternehmen nicht möglich ist, alle Anforderungen in einem Rollenmodell abzudecken. Obwohl sich in den letzten Jahren sowohl die theoretischen Ansätze als auch die Werkzeuge weiterentwickelt haben, ist es eher die Regel, dass Projekte in diesem Umfeld abgebrochen werden bzw. nur ein Teil der Ziele erreicht wird. Zwei Beispiele[822] zeigen, wo die Herausforderungen liegen können: „*Role definition also can be tricky when several business units are involved. Montvale, N.J.-based Ingersoll Rand Co. supports different Web portals for dealers of each of the company's three construction equipment lines: Bobcat, Club Car and Ingersoll Rand. A dealer that carries all three brands had seven different log-ins to access all required applications. Jim McDonald, manager of IT, says he used Oracle Corp.'s Identity Manager and other Oracle tools to create a single identity and single sign-on for each user. Now he's working on assigning users roles so each user inherits role-based rights and*

[822] Vgl. http://www.computerworlduk.com/technology/security-products/authentication/in-depth/index.cfm?articleid=139 [8. Dezember 2007]

attributes automatically. The problem is that different groups define the same role names differently. For example, a parts manager at one dealership may be able to see prices and costs, while at another, management may not want the parts manager to see what the company pays for a part. Different constituencies will never agree on a single set of role definitions, says McDonald, and you have to work around that. We let each brand define their own roles. We're not trying to dictate the business requirements, he says."

Das zweite Beispiel veranschaulicht die Grenzen eines Rollenkonzepts: „*After mapping all of your accounts, the second most challenging task is defining roles, says Jim Shattuck, lead systems analyst at Children's Hospital Boston. The teaching hospital has been consolidating identity repositories and uses Microsoft Identity Information Server to link 14 applications to perform automated user provisioning. As part of that effort, the hospital defined about 90 minor roles. The roles help us provision about 80 percent of the users, but there are 20 percent that are too disparate, Shattuck says. Those do not justify the effort involved in defining and maintaining them, he says, so they are handled as one-off requests. The number of applications included in the project is also limited. For the most part, the roles affect applications and permissions that are integrated tightly with Active Directory and not beyond, Shattuck says. The rest of the more than 100 applications, including the hospital's primary clinical application, aren't yet integrated. As far as roles go, we're maybe 20 percent of the way there, he says. Shattuck cites both technical and management challenges. For example, to provision the clinical application, the hospital needed to define key roles and add new "departmental" and "manager" fields in PeopleSoft, the authoritative repository of identity data for provisioning users in the clinical application.*"

Mit *Bottom-up* und *Top-down* gibt es zwei Möglichkeiten, sich der Entwicklung von Rollen zu nähern. Der Status quo ist, dass die Benutzer Berechtigungen in diversen Applikationen haben. Um diese Berechtigungen festzustellen, müssen diese ausgelesen und in einem Repository gesammelt werden. Mit Methoden des Data Mining (siehe *2.2.5 Data Mining*) werde diese Daten analysiert, indem die Berechtigungen von Personen mit gleichen Aufgabenbereichen verglichen werden. Aus dem Resultat lassen sich Basisrollen ableiten. Dabei lässt sich feststellen, wenn zwei Benutzer mit denselben Aufgaben andere Berechtigungen haben. Ebenso werden die Berechtigungen analysiert und gruppiert, um herauszufinden, ob es unterschiedliche oder redundante Arten gibt, wie Benutzer bestimmte Berechtigungen erhalten. Der Bottom-up-Ansatz führt relativ schnell zu Ergebnissen, inkludiert aber wesentliche Nachteile. Zunächst müssen entsprechende Werkzeuge zur Verfügung stehen. Dann gilt es, die große Menge an gesammelten Daten zu analysieren. Dazu braucht es viel Erfahrung und ein profundes Wissen über die bestehenden Prozesse respektive Aufgaben der Mitarbeiter. Zudem ist unsicher, ob die gefundenen Rollen dem Soll entsprechen, da sie aus dem Ist-Stand abgeleitet wurden. Es ist daher ein weiterer Schritt notwendig, um zu prüfen, ob die Anforderungen der Geschäftsprozesse und Compliance (siehe *3.5.2.1 Gesetze, Regulative, Compliance*) erfüllt werden.

Gelöst werden kann das dadurch, dass von den Geschäftsprozessen und den davon abgeleiteten Rollen ausgegangen wird. Ein Top-down-Ansatz erfolgt in der Regel über eine Analyse der Geschäftsprozesse, die sehr aufwändig ist und detailliert genug sein muss, um daraus die notwendigen Berechtigungen für die einzelnen Mitarbeiter ableiten zu können.

Der beste Ansatz scheint eine Kombination aus beiden Vorgehensweisen zu sein. Dabei werden bestimmte Teilbereiche abgegrenzt und für diese geprüft, ob und inwieweit die definierten Rollen den gefundenen Berechtigungsgruppen entsprechen. Voraussetzung dafür ist die Möglichkeit, das Rollenmodell im IMS beliebig und mit wenig Aufwand zu erweitern.

Laut Mezler-Andelberg [Mezler-Andelberg, 2007, S 50f], ergänzt um die Erfahrungen des Autors, bleiben einige Entscheidungen offen, die jedes Unternehmen für sich treffen muss (siehe *3.5.4.2.3 Aufbauorganisation*):

- Gibt es Ausnahmen, die nicht in Standardrollen abgebildet werden können?
- Darf eine Vertretung alles, das die vertretene Person darf?
- Was passiert im Krisenfall? Hier steht Informationssicherheit gegen Ausfallszeit. Ist es besser, wenn die Mitarbeiter weiterarbeiten können, auch wenn ein entsprechender Sicherheitslevel nicht mehr gewährleistet ist?
- Wie sind die Daten zu klassifizieren? Werden die Daten, die nicht klassifiziert sind, geschützt oder wird der Zugriff gestattet?
- Was passiert mit Rollen, die nur im Rahmen eines Projekts benötigt werden? Wer hat nach Abschluss des Projekts noch Zugriff auf die Daten und mit welcher Rolle?

3.6.4 AUSPRÄGUNGEN VON ROLLEN

An dieser Stelle soll neben der Aufteilung der Verwaltung der Benutzerdaten (siehe *3.6.2 Aufteilung der Verwaltung der Benutzerdaten*) eine weitere Idee zur Stärkung der informationellen Selbstbestimmung eingebracht werden. Entgegen dem Charakters von Identitätsmanagementsystemen soll nicht mehr für alle Bereiche Transparenz und Nachvollziehbarkeit (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz: Transparenzziele*) herrschen. Für den Mitarbeiter soll ein *geschützter Raum* geschaffen werden, in dem er ohne Überwachungsmöglichkeit private Tätigkeiten durchführen kann (siehe *2.4.2.4 Integration von Datenschutzmechanismen in IT-Komponenten, 2.4.3 Säule 3: Datenschutz durch Technik*). Hinsichtlich der Zulässigkeit von Betriebsmitteln für private Zwecke bzw. von Überwachungsmöglichkeiten am Arbeitsplatz darf auf *1.7.3.2 Arbeitsrechtliche Grundlagen der Informationssicherheit in Unternehmen* und *2.3.4 Exkurs: Privacyaspekte für den betrieblichen User* verwiesen werden.

Während der Mitarbeiter eine einfache, intransparente Möglichkeit zum Durchführen privater Tätigkeiten bekommt, werden aus Unternehmenssicht informationssicherheitstechnische Gefahren (z. B.: Download von verseuchten Attachments in Abteilungsverzeichnisse, Installation von Programmen,

die die Informationssicherheitsvorkehrungen unterminieren) unterbunden. Zudem fördern Maßnahmen, die zum Vorteil der Mitarbeiter gedacht sind, deren Motivation.

An Kapitel 3.6.3 Von der Identität zur Rolle anschließend wird dem Begriff „Rolle“ eine zweite Bedeutung verliehen. Zur klassischen, dienstlichen Rolle soll eine private Rolle entwickelt und angeboten werden. Während unter der dienstlichen Rolle – wie in den vorigen Kapiteln beschrieben – der Zugang der Mitarbeiter zu ihren betrieblichen Ressourcen verstanden wird, ermöglicht die private Rolle dem Mitarbeiter persönliche Tätigkeiten (E-Banking, privater Besuch von Webseiten, Datenspeicher etc.) unbeobachtet durchzuführen.

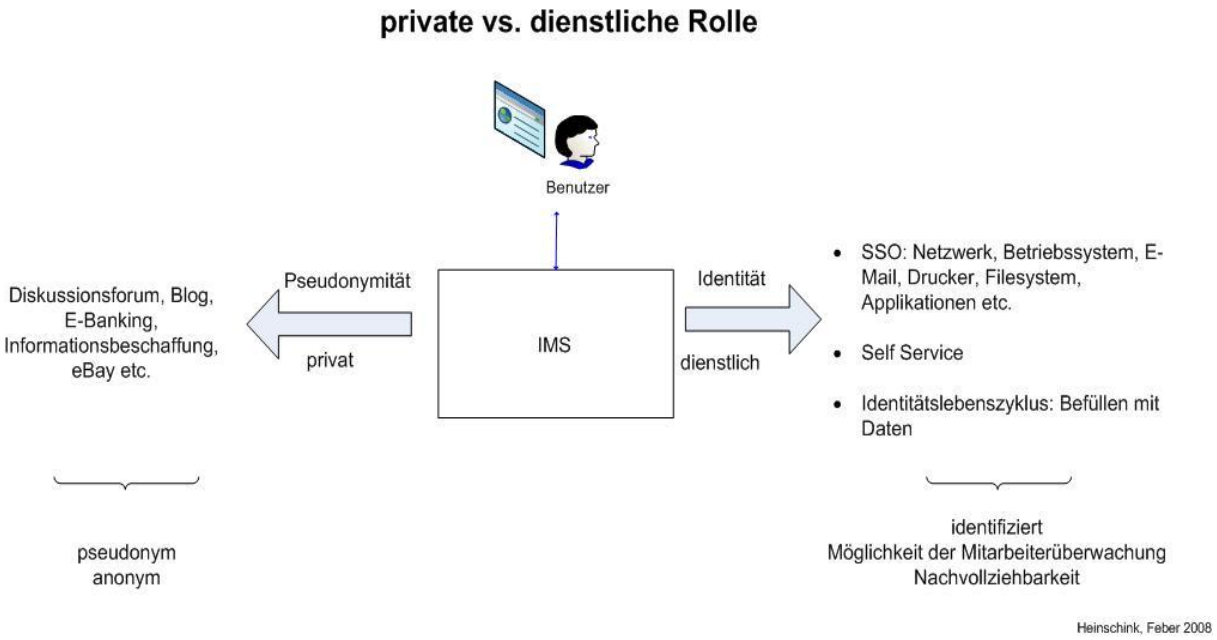


Abbildung 58: private vs. dienstliche Rolle

Beim Start des PCs wird mit dem Betriebssystem das Identitätsmanagementsystem gestartet. Wie in *Abbildung 59: Login private/dienstliche Rolle* symbolisch dargestellt, gibt es beim Login die Wahlmöglichkeit zwischen privater und dienstlicher Nutzung. Für beide Bereiche sind Username und Passwort erforderlich, wobei der Unterschied darin liegt, dass die Credentials für den privaten Gebrauch lokal und verschlüsselt auf dem PC gespeichert werden. Die Zugangsdaten für die dienstliche Verwendung hingegen werden im unternehmensweiten Verzeichnis abgelegt.

Zu den Funktionen eines Identitätsmanagementsystems (siehe *3.4 Komponenten und Funktionen eines Identitätsmanagementsystems*) sollen Ansätze und Technologien, wie in *2.4.3 Säule 3: Datenschutz durch Technik* (anonym und pseudonym Surfen bzw. anonym und pseudonym Mailen) beschrieben, zur Anwendung kommen, im speziellen der Security Chip (siehe *1.7.2.8 Trusted Computing*) für die lokale Verschlüsselung oder die Biometrie (siehe *1.7.2.3 Biometrie*) zur Authentifizierung.

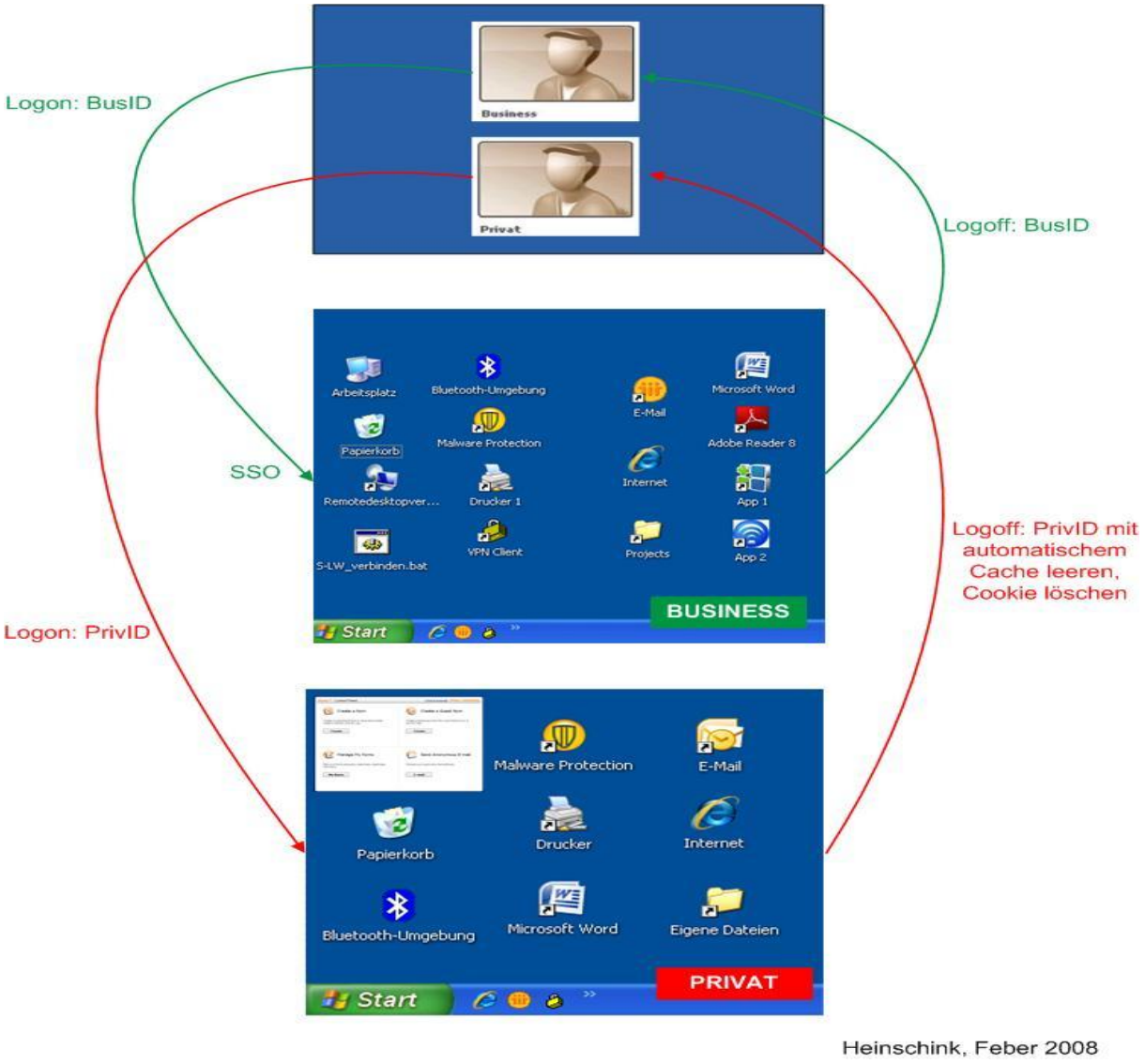


Abbildung 59: Login private/dienstliche Rolle

3.6.4.1 Dienstliche Rolle

Die dienstliche Rolle entspricht der vollständigen Identität (siehe *2.2.1 Digitale Identität*: *Vollständige Identität*) und erfüllt drei Funktionen (siehe *3.5.1 Anforderungen und Nutzen aus Mitarbeitersicht*). Die erste erlaubt dem Mitarbeiter mittels SSO (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*) einen singulären Zugang zu seinen Ressourcen (Netzwerk, Betriebssystem, E-Mail, Drucker, Filesystem, Applikationen etc.). Die zweite befähigt ihn, gewisse administrative Aufgaben selbstständig, ohne Abhängigkeit von Dritten, durchzuführen (siehe *3.4.2.5 Self Service*). Mit der dritten kann er seinen Part für die Aufrechterhaltung des Identitätslebenszyklus erfüllen, indem er seinen Datenbestand wartet (siehe *2.2.1.1 Lebenszyklus einer Identität, 3.6.2 Aufteilung der Verwaltung der Benutzerdaten*).

Der Mitarbeiter ist vollständig identifiziert, daraus ergeben sich einerseits der Nachteil der Mitarbeiterüberwachung (siehe *2.3.4 Exkurs: Privacyaspekte für den betrieblichen User*), andererseits

die Vorteile der Personalisierung (siehe *2.2.4 Personalisierung*) und der Nachvollziehbarkeit (siehe *3.5.2.1 Gesetze, Regulative, Compliance*).
Durch die Aufteilung der Identitätsverwaltung (siehe *3.6.2 Aufteilung der Verwaltung der Benutzerdaten*) wird die Sicht des Verwaltungsangestellten bzw. Vorgesetzten auf die Daten des Mitarbeiters eingeschränkt und damit die informationelle Freiheit des Einzelnen gestärkt.

3.6.4.2 Private Rolle

Mit der privaten Rolle wird dem Mitarbeiter die Möglichkeit eingeräumt, persönliche Angelegenheiten (E-Banking, privater Besuch von Webseiten, Datenspeicher etc.) ohne Überwachungs- und Eingriffsmöglichkeit der IT bzw. sonstiger Zugriffsberechtigter (z. B.: Personalabteilung, vorgesetzte Instanz) zu erledigen.
Der Einstieg erfolgt unter einer Identität ohne Attribute (*PrivID*, siehe *Abbildung 59: Login private/dienstliche Rolle* bzw. *2.2.2 Pseudonymität*: *Pseudo-/Teilidentität 2.2.3 Anonymität*: *Leere Identität*), deren Credentials lokal am PC des Benutzers verschlüsselt gespeichert werden. Damit wird organisatorisch und technisch eine klare Abgrenzung zur geschäftlichen Tätigkeit geschaffen. Für die Erledigung privater Angelegenheiten sind im Wesentlichen ein Internet-Browser, eine Textverarbeitung, eine Tabellenkalkulation und diverse kleinere Programme (z. B.: zur Bildbearbeitung) ausreichend. Zum möglichst anonymen Besuch des Internets steht dem Mitarbeiter, wie in *Abbildung 42: Pseudonym-Funktion von Anonymizer* dargestellt, ein Verwaltungstool für Pseudonyme zur Verfügung. Damit ist es möglich, Pseudonyme selbst zu wählen oder per Zufallsgenerator erzeugen zu lassen. Die Pseudonyme können in Kategorien eingeteilt (z. B.: Einkauf, Informationsmaterial etc.) und beschrieben (bei welcher URL verwendet, bis wann gültig) werden. Zur Verhinderung der Verkettbarkeit eignen sich besonders Beziehungs- oder Transaktions-Pseudonyme (siehe *2.2.2 Pseudonymität: Beziehungs-Pseudonyme, Transaktions-Pseudonym*). Da das Anonymisieren von E-Mails über den Unternehmensmailserver aufwändig ist, ist der Gebrauch eines Webmaildienstes ratsam. Die Arbeit erfolgt lokal am Benutzergerät ohne Zugriff von und auf die Unternehmensdomäne. Die Daten werden in einem eigenen Bereich auf der lokalen Festplatte verschlüsselt gespeichert. Bei der Abmeldung wird sichergestellt, dass sämtliche historische Daten (Cookies, Application Traces etc.) gelöscht werden.
Der Benutzer trägt die Verantwortung für den Inhalt der Daten und die Administration des persönlichen Bereichs (z. B.: Installation von Programmen, Datensicherung). Die Aufgabe der IT bzw. des Helpdesks besteht lediglich im einmaligen Anlegen, nicht jedoch in der laufenden Unterstützung.
Das IMS darf für den Privatbereich keine Protokollierung durchführen. Dem Verwaltungsmitarbeiter stehen somit keine Daten über den Mitarbeiter zur Verfügung.

3.6.5 PROJEKTREALISIERUNG

Die Arbeit liefert eine umfassende Beschreibung der Themen Informationssicherheit, Privacy und Identitätsmanagement und erklärt deren Zusammenhänge und Abhängigkeiten. Der Schwerpunkt liegt auf der betrieblichen Sichtweise. Dieser wurde um spezifische Aspekte aus dem behördlichen Umfeld ergänzt. Die theoretischen Ausführungen wurden mit Beispielen aus der Praxis untermauert. An dieser Stelle werden Projektumsetzungspläne aus dem Arbeitsumfeld des Autors vorgestellt, die auf den bisher vorgestellten Theorien und Konzepten aufbauen.
Die Ausführungen werden auf einem relativ hohen Abstraktionsniveau gehalten, da einerseits eine Detailtiefe nur bedingt notwendig ist, zum anderen, um vertrauliche Daten wie Konfigurationen oder Sicherheitseinstellungen des Arbeitgebers des Autors nicht preiszugeben.

3.6.5.1 Problemstellung und Herausforderung

Das Unternehmen, in dem der Autor arbeitet, ist als IT-Dienstleister für den öffentlichen Bereich tätig. Der Kunde im gegenständlichen Fall ist eine Landesverwaltung. Dort hat der Autor die Mitverantwortung in der Aufgabenstellung eines Informationssicherheitsbeauftragten. Im Zuge dieser Funktion wurde im Jahr 2004 ein Informationssicherheitsmanagementsystem eingeführt, welches den Rahmen für alle Maßnahmen im Umgang mit Information absteckt. Das bei diesem Kunden anstehende Projekt ist die Umsetzung eines Identitätsmanagementsystems. Die Realisierung soll in zwei Schritten erfolgen: Auf Basis des in der Fertigstellung befindlichen Portalverbundsystems (siehe *3.5.3 Praxisbeispiel: Identitätsmanagement für Behörden in Form des Portalverbunds*) soll durch organisatorische und technische Erweiterungen ein umfassendes Identitätsmanagementsystem (siehe *3.6.1 Funktionserweiterung des Portalverbunds in Richtung Identitätsmanagementsystem*) entstehen. Bestrebung ist, ein System zu schaffen, das neben dem Nutzen für Mitarbeiter und Behörde den Aspekt der informationellen Selbstbestimmung für die Anwender in den Vordergrund stellt (siehe *3.6 Informationelle Selbstbestimmung im betrieblichen Umfeld*).
Die Landesverwaltung ist in folgenden zwei Aufgabenbereichen tätig:

- Hoheitsverwaltung: Hier handelt das Land *als Behörde*, also mit staatlicher „Befehls- und Zwangsgewalt“. Das ist überall dort, wo Bewilligungen zu erteilen, Verbote auszusprechen und Strafen zu verhängen sind.
- Privatwirtschaftsverwaltung: Hier agiert das Land wie ein Privater, wenn es etwa kulturelle Aktivitäten setzt bzw. eine Schule oder ein Krankenhaus betreibt. Diese Aufgaben entspringen dem leistungsstaatlichen Gedanken.

Angelegenheiten der Hoheitsverwaltung darf nur das Land selbst wahrnehmen, jene der Privatwirtschaftsverwaltung können auch von Privaten wahrgenommen werden. An der Spitze der Landesverwaltung steht die Landesregierung, ein mehrköpfiges, vom Landtag gewähltes Kollegium

unter dem Vorsitz des Landeshauptmannes. Die Landesregierung bedient sich bei der Erledigung ihrer Aufgaben eines Geschäftsapparates, des Amtes der Landesregierung. Für dessen Funktionsfähigkeit hat der Landeshauptmann und als höchster Beamter der Landesamtsdirektor (kurz: LAD) zu sorgen.
Die Bezirkshauptmannschaften (kurz: BH) sind hauptsächlich mit hoheitlichen Aufgaben befasst, haben daher den meisten Bürgerkontakt.
In *Abbildung 60: Übersicht Organisationsstruktur* sind die ausführenden Organe der Verwaltung in Übersichtsform angeführt. Die zentrale Stelle bildet die Landesamtsdirektion. Ihr sind alle Abteilungen, Bauämter (kurz: BA) und Bezirkshauptmannschaften unterstellt. Für die interne Infrastruktur des gesamten Verwaltungsapparates zeichnen die LAD-Stabsstellen „Organisation“ und „IT“ verantwortlich. Aus Gründen der Übersichtlichkeit wird auf Querverbindungen zwischen den Abteilungen und der Regierung, das Anführen von Landesbeteiligungen und einer vollständigen Darstellung aller Abteilungen und Referate verzichtet.

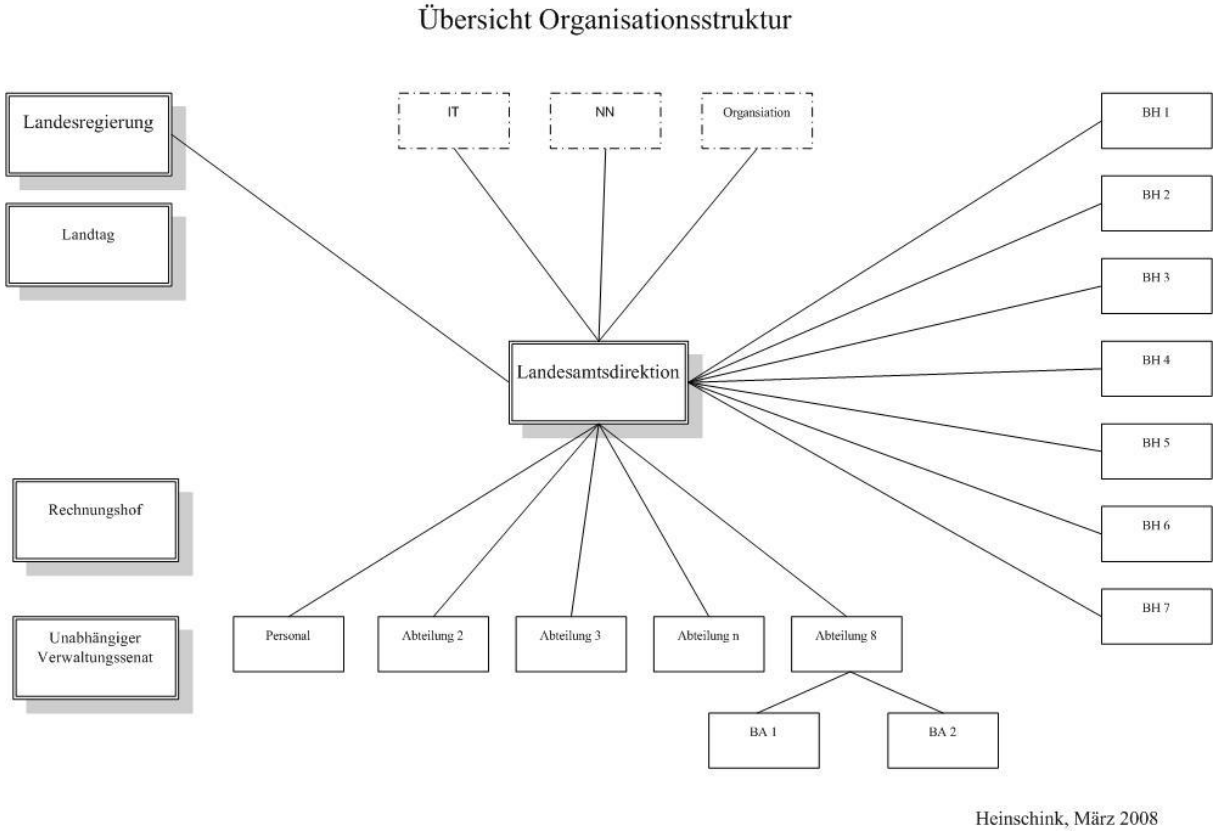


Abbildung 60: Übersicht Organisationsstruktur

Die IT hat mehr als tausend Benutzer in rund 15 Lokationen zu administrieren. Die Bürgeridentitäten sind in dieser Zahl nicht inkludiert. Die Standorte sind über eine Windows-Domäne ausfallssicher vernetzt, zudem gibt es *befreundete Netze* wie beispielsweise das der Gemeinden. Die Infrastruktur wird aus einem homogenen Umfeld (Windows, Host) mit redundanter Auslegung gebildet.

Um eine Übersicht über die verarbeiteten (Identitäts-) Daten zu erhalten, sollen diese kategorisiert werden. Zunächst soll eine Unterscheidung in Analogie zum TKG 2003 in *Stammdaten* und *Inhaltsdaten* erfolgen. Die Klassifizierung nach Dateneigentümer soll auf drei Bereiche beschränkt werden. Der Landtag, der Rechnungshof und der Unabhängige Verwaltungssenat befinden sich zwar im Umfeld der Landesregierung, sind aber aus IT-technischer Sicht vom Landesnetz unabhängig. Für eine spätere Wiederverwendbarkeit sollen die Gruppen mit Kurznamen versehen werden.

- [Bürger] Bei den *Bürgerdaten* ist zwischen jenen für die Einzelperson und jenen von Unternehmen zu unterscheiden. Bei ersteren geht es um persönliche Angaben (Name, Geburtsdaten, Familienstand etc.), oft in Kombination mit finanziellen Angelegenheiten (z. B.: Förderung). Es kann sich aber auch um sensible Daten handeln, wie Straf-, Konkursverfahren oder Aufzeichnungen über Familiensituationen (Kindesabnahmen, sexuelle Übergriffe etc.). Unternehmensdaten ergeben sich etwa bei gewerberechtlichen Angelegenheiten. Der Bürger soll vor der Willkür des Datenzugriffs durch die Verwaltungsmitarbeiter geschützt werden (siehe *2.4.7 Bereichsspezifisches Personenkennzeichen und Bürgerkarte im E-Government*).
- [Politiker] Den Regierungsmitgliedern steht eine eigene Infrastruktur zur Verfügung. In den sogenannten *politischen Büros* arbeiten neben dem Regierungsmitglied seine politischen Berater und Büroangestellten. Es muss sichergestellt werden, dass es zu keinen Vermischungen der Daten zwischen den politischen Büros kommt. Der Aktenlauf aus den Fachabteilungen (Stichwort: *Elektronischer Akt*) zur Ansicht und Unterschrift muss ungehindert der Schutzmaßnahmen laufen. Da die Regierungsmitglieder wie deren Büromitarbeiter im Personalstand des Landes stehen, sind sowohl Stamm- als auch Inhaltsdaten zu verwalten.
- [Mitarbeiter] Für die Verwaltungsmitarbeiter sind ebenfalls die Stamm- und Inhaltsdaten zu verwalten. Hier gibt es ein Spannungsfeld: Zum einen muss aus rechtlichen bzw. ökonomischen Gründen absolute Transparenz herrschen. So sollen beispielsweise willkürliche Abfragen im Zentralen Melderegister verhindert werden. Zum anderen soll dem Mitarbeiter das Recht auf Hoheit über seine eigenen Daten gewährt werden.

  [Administratoren] Gehören zur Gruppe der Mitarbeiter, sind aufgrund ihrer Tätigkeit in der IT oder Personalabteilung mit dem Umgang von Daten konfrontiert. Administratoren haben kraft ihrer Tätigkeit Zugang auf die Stamm- und/oder Inhaltsdaten der Mitarbeiter.

  [Vorgesetzte] Gehören ebenfalls zur Gruppe der Mitarbeiter, brauchen jedoch zur Ausübung ihrer Führungsrolle Zugriff auf die Daten ihrer Mitarbeiter. Dem Erforderlichkeitsprinzip und dem Grundsatz der Datenvermeidung folgend soll dem Administrator und dem Vorgesetzten nur noch das jeweils notwendige Mindestmaß an Daten zur Verfügung gestellt werden.

Vor einiger Zeit wurde ein Konsolidierungsvorhaben im Infrastrukturbereich begonnen. Dieses hat zum Ziel, aus einem heterogenen, aufwändig zu administrierenden Umfeld ein homogenes zu machen.

Aus einer Vielzahl von Applikationen und Systemen wird durch Einführung unternehmensweiter Software wie SAP und Ressourcenvirtualisierung auf einige wenige reduziert. Die Folge ist eine besser überschaubare, strukturiertere Systemlandschaft, die leichter zu verwalten und damit wirtschaftlicher ist. Der Administrationsaufwand der vom Personalstand reduzierten IT wird weniger. Ein Nebeneffekt ist, dass mit diesem Vorhaben auch die Daten zusammengeführt werden. Die verbesserten Reportingfunktionen der Systeme erlauben umfangreichere und detailliertere Auswertungen zu generieren.

Die Bestrebung der öffentlichen Hand ist, alle sogenannten Behördenapplikationen (Zentrales Melderegister, Zentrales Vereinsregister, Führerscheinregister etc.) von diversen proprietären Plattformen auf Webbasis zu portieren, um eine effiziente, behördenübergreifende Zusammenarbeit via Portal zu ermöglichen. Den internen Mitarbeitern sollen über ein zentrales Webinterface die unterschiedlichen Anwendungen der verschiedenen Institutionen zugänglich gemacht werden. Da es sich dabei vielfach um personenbezogene Daten handelt, ist eine entsprechende Informationssicherheitsinfrastruktur erforderlich. Dazu gehört eine Berechtigungsstruktur, welche sowohl den hausinternen als auch den externen Anforderungen entsprechen muss. Für jede Applikation gibt es verschiedene Berechtigungsparameter, die für Mitarbeiter mit unterschiedlichen Rollen zu vergeben sind. Zudem ist es erforderlich, dass alle vom Benutzer getätigten Aktivitäten in einer Applikation nachvollziehbar dokumentiert werden.

Hervorgerufen durch (nicht beabsichtigte) Geschehnisse in der Vergangenheit und durch subjektive Eindrücke mit negativen Gefühlsfolgen bei gleichzeitig hoher Sensibilität (z. B.: sensible Bürgerdaten) respektive Exklusivität (z. B.: politische Rede) der Daten steht der Vorwurf der Überwachung im Raum. Die EDV-Abteilung sieht sich mit Misstrauen konfrontiert, ohne entsprechende Gegenargumente in der Hand zu haben. Die diesbezüglichen Überlegungen und Diskussionen haben zu Selbstschutzmaßnahmen der IT geführt. Zwischenzeitlich behilft sich die Administration beim Arbeiten mit personenbezogenen Daten mit manuellen Mitteln (z. B.: Löschen von Logdateien nach Fehleranalyse) und einem selbstauferlegten Vieraugenprinzip.

Zusammenfassend lässt sich die Situation ohne Identitätsmanagement so beschreiben, dass eine große Anzahl an isolierten Applikationen auf unterschiedlichen, teilweise proprietären Servertypen existiert. Dies hat zur Folge, dass die Benutzer mit einer Vielzahl an Kennungen und die IT-Mitarbeiter mit einem entsprechend hohen Supportaufwand konfrontiert sind. Zudem hat der User mit unterschiedlichen Zugängen zu den Anwendungen zu kämpfen: *3270-Emulation*[823], Softwareclient und Weblösung. Die Verbindung zu den Fremdapplikationen erfolgt über ein eigenes, teuer zu mietendes Behördenintranet. Durch die dezentrale Rechtevergabe fehlt es an der nötigen Transparenz,

[823] Unter 3270-Emulation wird ein Vorgang verstanden, der Funktionen eines IBM-Mainframerechners auf einen PC zur Verfügung stellt.

die durch isoliertes Logging noch erschwert wird. Organisatorisch besteht eine Abhängigkeit zu externen Stellen, weil die Userverwaltung beim Anwendungsbetreiber erfolgt.
Die IT ist allein verantwortlich für das Verwalten der Userdaten: vom Lebenszyklus einer ID (siehe *2.2.1.1 Lebenszyklus einer Identität*), über die Rechtevergabe bis hin zum Management der Stamm- und Inhaltsdaten. Eine Kontrolle der Berechtigungen ist ob der vielen Systeme schwierig und aufwändig, dementsprechend existieren Karteileichen und sicherheitstechnische Schwachstellen. Die verwendete achtstellige ID ergibt sich aus einer Abkürzung des Familiennamens und dem Anfangsbuchstaben des Vornamens (z. B.: für den Autor *heinschj*), ist also durchaus sprechend.

3.6.5.2 Zielsetzungen

Die Ziele ergeben sich aus den beschriebenen Anforderungen. Prämisse und Bedingung für die Umsetzung ist, dass die zu setzenden Aktivitäten mit dem in der Landesverwaltung laufenden Informationssicherheitsmanagementsystem abgestimmt sein müssen.

- *Strukturierung der Zugriffsrechte und Stärkung der informationellen Selbstbestimmung*. Es muss sichergestellt werden, dass die Daten nur von Zugriffsberechtigten eingesehen werden dürfen. Deren Rechte müssen transparent und nachvollziehbar sein. Als Kontrollmöglichkeit ist eine granulierbare Protokollierung einzuführen. Für die Politiker und Mitarbeiter soll das Maß an informationeller Selbstbestimmung erhöht werden.
- *Etablierung eines Self Service-Dienstes* (siehe *3.4.2.5 Self Service*). Durch die Zugriffsmöglichkeit der Politiker und Mitarbeiter auf die eigenen Daten und entsprechende Prozesse (z. B.: Aufteilung der Administrationsaufgaben, Vertreterregelung) der Personal- bzw. IT-Abteilung werden Abläufe der Administration vereinfacht, beschleunigt und vereinheitlicht. Hierunter fällt beispielsweise das Rücksetzen und Ändern eigener Passwörter oder die Pflege bestimmter Identitätsattribute wie Adresse oder Telefonnummer. Damit verwalten Mitarbeiter einen Teil ihrer Personaldaten selbst und entlasten die Personal- bzw. IT-Abteilung von Routineaufgaben.
- *Öffnung der Verwaltung*. Die Verwaltung soll sich zum einen gegenüber dem Bürger, zum anderen behördenintern in der Zusammenarbeit mit anderen Institutionen (Bund, Städte, Gemeinden etc.) öffnen. Die Funktion des Self Service soll längerfristig auch dem Bürger zur Verfügung stehen. Über ein personalisiertes Portal sollen Eingaben gemacht, Bescheide eingesehen, Kontenstände abgefragt sowie Zahlungen veranlasst werden können.
- *Erhöhung der Usability* (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*). Durch den stetig steigenden Grad an Vernetzung zwischen Organisationen und die Steuerung der Kernprozesse über IT-Systeme erhöht sich trotz der Konsolidierungstendenzen die Anzahl der IDs. Das belastet zum einen den Anwender, zum anderen bedeutet das für die IT-Abteilung einen steigenden administrativen Aufwand in der Benutzerverwaltung, weil nicht nur Benutzer und Berechtigungen für Mitarbeiter, sondern auch für Bürger, Partner und Lieferanten verwaltet

werden müssen. Wir haben festgestellt, dass die Benutzer daher – sofern es die Systeme zulassen – keine oder einfachste Passwörter verwenden. Der Benutzer muss sich mit einer Single-Sign-On-Lösung (kurz: SSO) nur einmal für alle ihm zustehenden Applikationen authentifizieren. Gerade im Hinblick auf Portale ist diese Möglichkeit aus Anwender- und Landessicht wünschenswert.

- *Einführung einer starken Authentifizierung und Verschlüsselung*. Ausschlaggebend für den geforderten Sicherheitsgrad sind die Daten, die verarbeitet werden. Dazu sind die Erfordernisse in Sicherheitsklassen zu kategorisieren, welche mit Maßnahmen im Benutzer-, Anwendungs- und Kommunikationsbereich zu erfüllen sind. Die Vereinbarung von Sicherheitsklassen im Portalverbund gewährleistet eine adäquate Sicherheit für die Anwendungen. Die Sicherheitsklasse 3 bedingt eine Authentifizierung durch Wissen und Besitz bzw. biometrisches Merkmal an in einem geschützten Bereich betriebenen Gerät oder an einem mobilen Endgerät mit erhöhtem Grundschutz. Es ist daher naheliegend, die Umsetzung in Form einer Chipkarte zu gestalten.
- *Erhöhung der Mobilität*. Den Politikern und Mitarbeitern soll orts- und zeitungebunden Zugriff zu den Daten unter einem Höchstmaß an Sicherheit gewährleistet werden.

3.6.5.3 Umsetzung und Vorgehensweise

Die Realisierung der Zielsetzungen soll in zwei Schritten erfolgen: Als Basis dient ein derzeit im Aufbau befindliches Portalverbundsystem, das den sicheren Austausch von Daten und Berechtigungen zwischen zwei oder mehreren Organisationen ermöglicht. Auf dieser Grundlage soll durch organisatorische und technische Erweiterungen ein holistisches Identitätsmanagementsystem entstehen. Bei der Planung ist berücksichtigt, dass die Umsetzung eines solchen Vorhabens für mehr als tausend Benutzer nur in mehreren Phasen ablaufen und je nach Intensität mehr als ein Jahr lang dauern kann. Bestrebung ist, ein System zu schaffen, das neben dem Nutzen für Politiker, Mitarbeiter und Behörde den Aspekt der informationellen Selbstbestimmung für den Anwender in den Vordergrund stellt. Identitätsmanagement stellt eine übergreifende, unternehmensweite Aufgabe für Landesamtsdirektion, IT-Führung und Informationssicherheit dar.

Die Initialzündung im konkreten Projekt war die Vorgabe von externen Stellen, ein Portalverbundsystem einzuführen. Die Bedingung für eine Erweiterung ist das Vorhandensein einer entsprechenden Lobby in der politischen und administrativen Führung. Dazu muss bei den verantwortlichen Personen laufend Überzeugungsarbeit geleistet und ein für sie verständlicher, quantifizierbarer Mehrwert gefunden und dargestellt werden. Gleichzeitig muss auf die langfristigen Auswirkungen hingewiesen werden, da die Investitionskosten auch beim modularen Vorgehen beträchtlich sind. Die wesentlichen Argumente für die Entscheidungsträger in der Landesverwaltung sind in diesem Zusammenhang die Reduzierung der Passwörter und der Nutzen eines Portals. Unterstützend wirkt dabei die allgemeine Unzufriedenheit mit der im Einsatz befindlichen Intranet-Lösung. Da für den Betrieb eines Identitätmanagementsystems strukturierte Prozesse erforderlich sind,

ist oft ein Eingriff in die Ablauforganisation notwendig. Aus diesem Grund sind die Identifizierung der Stakeholder und ihr Einbinden in den Entscheidungs- und Umsetzungsprozess wesentlich. Wie in *Abbildung 60: Übersicht Organisationsstruktur* hervorgehoben, sind dies im Besonderen die Stabsstelle Organisation und die Personalabteilung. Dazu ist es – wie sich bei anderen übergreifenden Projekte gezeigt hat – empfehlenswert, je einen Vertreter der Fachabteilungen und der Bezirkshauptleute einzubinden. Damit die Lösung angenommen wird, bedarf die Auswahl der Testpersonen quer durch die Organisation besonderer Aufmerksamkeit.

Bei einigen Aufgaben (z. B.: Mindsetting, Überzeugungsarbeit, Schulungen) wurde gewonnene Erfahrung aus der Umsetzung des Informationssicherheitsmanagementsystems (siehe *1.8 Unternehmenssicherheit*) herangezogen. Anknüpfungspunkt zwischen Informationssicherheit und Identitätsmanagement sind im organisatorischen Bereich die IT-Sicherheitspolicies. Darunter werden Dokumente verstanden, in denen grundlegende Vorgaben und Richtlinien zur Sicherheit von IT-Systemen definiert werden. Weiters beinhalten sie Details über die ausgewählten Sicherheitsmaßnahmen.

Dem best practise-Ansatz folgend wurden Informationen und Fakten zusammengetragen, die zu einer erfolgreichen Einführung eines unternehmensweiten Identity Managements führen:

- die Erstellung einer detaillierten Anforderungsanalyse mit Fachabteilungen, Bezirkshauptmannschaften und IT-Abteilung,
- das Design einfacher und sicherer Prozesse in Verbindung mit einem hohen Automatisierungsgrad,
- die Entwicklung eines einfachen, aber flexiblen rollenbasierten Berechtigungskonzeptes,
- die Auswahl von Produkten mit Standardschnittstellen,
- die Verwendung von starker Authentifizierung,
- ein schrittweises Vorgehen, das in einem ersten Schritt die wichtigsten Anwendungen in das IM integriert,
- das primäre Ziel soll vorderhand nicht ein unternehmensweites Directory sein,
- das Versorgen von Usern mit Rollen nur nach Bedarf,
- SSO soll nicht für alle Applikationen funktionieren,
- Federation wird erst bei wirklichem Bedarf realisiert.

Wie festgestellt wurde, liegt das wesentliche Erfolgsmoment in einem schrittweisen Vorgehen und in der Reduzierung des Umfangs bzw. Funktionalität bei gleichzeitigem Verfolgen des Gesamtziels.

Um das Spektrum der Funktionalitäten richtig abzubilden, muss vor der Umsetzung einiges überdacht werden: Welche Bereiche soll Identitätsmanagement umfassen? Wer darf zu welchen Daten/Informationen Zugriff haben? Was muss von einer Organisation bekannt sein? Wer muss mit

eingebunden sein? Stellvertreterregelung? Schulungsmaßnahmen? Sanktionen bei Nichteinhalten von Fristen, Erfüllen von Eingaben? Wie wird mit neuen Applikationen umgegangen? Datenschutz?

Um zu einem strukturierten Vorgehen bei der Projektumsetzung zu kommen, kann das sogenannte Ebenenmodell [Mezler-Andelberg, 2007] herangezogen werden. Das Modell setzt sich aus vier Ebenen zusammen: Die erste Ebene bilden die Personendaten, die zweite die Ressourcen, in der dritten und vierten werden Autorisierung und Authentifizierung behandelt. Durch die Aufteilung in Ebenen kann jeder Teilbereich isoliert betrachtet werden, dadurch wird die gewünschte Reduktion der Komplexität erreicht. Jede Ebene kann wieder in mehrere Bereiche unterteilt werden. Die erste Ebene kann in Bürger, Partner, Politiker und Mitarbeiter geteilt werden. In der zweiten Ebene, der Ressourcen-Ebene, werden die Systeme und Daten (z. B.: Dateien, Daten, Webinhalte) behandelt, für die Berechtigungen zu verwalten sind. In der dritten Ebene geht es um die Berechtigungen in Form von Rollen und Rechten, in der vierten um den Zugriff. Die Stärke der Authentifizierung hängt von der Risikoklassifizierung (LAN – „normal“; Partnernetz – „hoch“; Internet „sehr hoch“) ab. Wie bereits an anderen Stellen ausgeführt bedarf ein Identitätsmanagement Policies (siehe *1.8.2.4.2 IT-Systemsicherheitspolitik*), Prozesse (siehe *3.5.4.2.2 Ablauforganisation*) und Techniken (siehe *3.5.4.3 Technische Maßnahmen*). Der Zusammenhang der einzelnen Ebenen wird im Modell durch sogenannte Verbindungsschichten (kurz: VS) hergestellt. Diese stellen die Art und Weise dar, wie die Ebenen untereinander Daten austauschen. Die Verbindungsschichten sind nicht festgelegt, können nach Funktionalität und Grad des Automatismus ausgewählt werden. Beispiele für solche verbindenden Elemente sind User Provisioning (siehe *3.4.2.4 Provisioning und Reporting*) oder Single-Sign-On (siehe *3.4.2.1 Passwort-Management und Single-Sign-On*). *Abbildung 61: Ebenenmodell* dient dazu, einen Überblick über das gesamte Modell an einem Beispiel mit Daten der Landesverwaltung zu geben. In der praktischen Arbeit ist es sinnvoll, nur Teilbereiche darzustellen. Das Modell eignet sich gut zur Visualisierung der einzelnen Ebenen, Bereiche oder Prozesse.

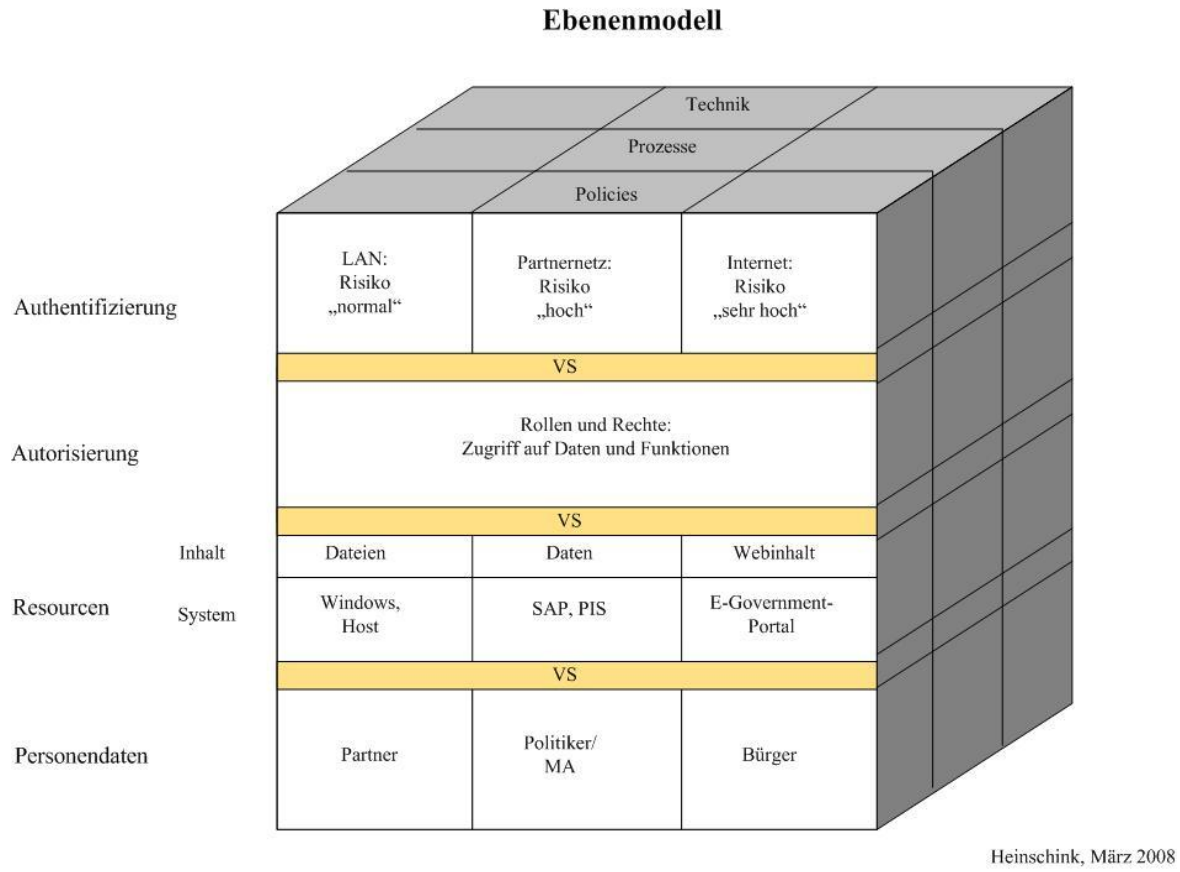


Abbildung 61: Ebenenmodell

Die Etablierung eines Identitätsmanagementsystems führt durch die Vielzahl an Funktionalitäten und begleitenden Maßnahmen zu einer Strukturierung in den Abläufen und der Verwaltung von Benutzeridentitäten und -rechten, in weiterer Folge zum „gläsernen Mitarbeiter“. Eine umfassende Protokollierung wird durch die zentrale Auslegung eines IMS erheblich erleichtert. Der Autor beobachtet diese Entwicklungen seit geraumer Zeit, als Mitarbeitender in der Informationssicherheit und in infrastrukturtechnischen Projekten ist er auch aus Selbstschutzgründen (siehe *3.5.1 Anforderungen und Nutzen aus Mitarbeitersicht*) an gegensteuernden Maßnahmen interessiert. Welche Voraussetzungen müssen vorhanden sein, welche Grundsätze beachtet werden und welche Möglichkeiten gibt es, um diesen Tendenzen zu völliger Transparenz im Sinne der informationellen Selbstbestimmung entgegen zu wirken? In der vorliegenden Arbeit wurde ein Bündel an zu beachtenden Grundsätzen, einzuhaltenden Richtlinien und umzusetzenden Maßnahmen bei der Schaffung und beim Betrieb eines Identitätsmanagementsystems herausgearbeitet. Diese sind unabhängig des sich im Einsatz befindlichen technischen Systems umzusetzen, dafür maßgebend ist der Gestaltungswille des Betreibers:

- die Beachtung des Erforderlichkeitsprinzips und des Grundsatzes der Datenvermeidung (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz, 3.2.2 Benutzer-zentrierte Identität*),

- ein zweckmäßiger Umgang mit Protokolldaten (siehe *3.4.2.4 Provisioning und Reporting, 3.4.3 Auditing*),
- die Verwendung pseudonymisierter oder anonymisierter Daten (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz*),
- die Beachtung des Vieraugenprinzips beim Management von Identitäten, der Rechtevergabe und bei Arbeiten an Systemen mit personenbezogenen Daten (siehe *3.5.1 Anforderungen und Nutzen aus Mitarbeitersicht*),
- ein hoher Grad an Automatismus (siehe *3.4.2.4 Provisioning und Reporting, 3.4.4 Portale und Web Services*),
- die Aufteilung der Benutzerverwaltung (siehe *3.6.2 Aufteilung der Verwaltung der Benutzerdaten, 3.6.4.1 Dienstliche Rolle*),
- die Einschränkung der Sicht der Administration und des Vorgesetzten (siehe *3.6.4.1 Dienstliche Rolle*),
- die Schaffung von Privatsphäre im virtuellen Raum (siehe *3.6.4.2 Private Rolle*).

Identitätsmanagementsysteme basieren auf einer Bündelung von verschiedenen Techniken und Technologien. Viele dieser Komponenten (z. B.: Verzeichnisdienst, Webserver, Passwortmanagement) finden in der Regel in Organisationen ihren Einsatz. Diese meist isoliert agierenden Systeme gilt es im Hinblick auf ein unternehmensweites IMS zu adaptieren, zu ergänzen und in diesem Kontext zusammenzuführen. Die erforderlichen technischen Komponenten wurden unter *3.4 Komponenten und Funktionen eines Identitätsmanagementsystems, 3.5.3.2.4 Techniken und Technologien für Portalverbund und 3.5.4.3 Technische Maßnahmen* vorgestellt.

Eine weitere Maßnahme, dem Benutzer die Hoheit über seine Daten zu geben, ist, diesem Arrangement Werkzeuge zur Pseudonymisierung beizufügen. Die Grundlagen dafür wurden bereits unter *2.2.2 Pseudonymität, 2.2.3 Anonymität, 2.4.3 Säule 3: Datenschutz durch Technik, 2.4.4 Anonym Surfen, 2.4.5 Anonym Mailen, 2.4.6 Pseudonym Surfen und Mailen* dargestellt. Im Kontext der Landesverwaltung sollen die Einsatzmöglichkeiten von Pseudonymen für Politiker und Mitarbeiter überlegt werden.

Grundsätzlich werden Pseudonyme zum Schutz von Personen vergeben, deren Identität Dritten nicht bekannt werden darf, deren Identität über das Pseudonym jedoch einem bestimmten Personenkreis bekannt sein muss. Pseudonyme stellen eine unidirektionale Zuordnung von Identität und Pseudonym her.

Bei Pseudonymen sind folgende Eigenschaften von Bedeutung [ULD, 2007]:

- Zuordnung/Zurechenbarkeit: Wie wird ein Pseudonym einer Person zugeordnet? Kann das Pseudonym frei gewählt werden? Ist es auf eine andere Person übertragbar?

- Verkettbarkeit: Ist es ersichtlich, ob mehrere Transaktionen vom gleichen Benutzer getätigt wurden? (Anm.: Ist keine Verkettung möglich, spricht man von Anonymität.)
- Aufdeckbarkeit: Wer kann wie die Zuordnung eines Pseudonyms zu einer Person aufdecken?

Es gibt eine Reihe von Abstufungen bei Pseudonymen. Auf der einen Seite steht die Anonymität und auf der anderen Seite die vollständige Identifizierung der Identität des Mitarbeiters. Hinsichtlich des Datenschutzes ist die Verkettbarkeit relevant:

- Preisgabe der Identität.
- Personen-Pseudonym: z. B.: Nickname, Personalnummer.
- Rollen-Pseudonym: z. B.: eine Rolle in einem Unternehmen.
- Beziehungs-Pseudonym: ein Pseudonym pro Kommunikationspartner.
- Transaktions-Pseudonym: ein neues Pseudonym für jede Transaktion.

Grundsätzlich gilt: Je mehr Attribute einer Identität preisgegeben werden, umso besser wird der Komfort für den Benutzer und umso schwächer der Schutz seiner Daten. Die Anonymität des Pseudonyminhabers hängt davon ab, wieviel unmittelbar über die Zuordnung des Pseudonyms zur Person bekannt ist und inwieweit sich ein Personenbezug durch Beobachtung der Pseudonymverwendung, d. h. die Verkettung einzelner Aktionen, erschließen lässt. Generell bieten sowohl Rollen- als auch Beziehungs-Pseudonyme stärkere Anonymität als Personen-Pseudonyme. Die stärkste Anonymität lässt sich mit Transaktions-Pseudonymen erreichen.

Status quo

Die Sachlage stellt sich aktuell so dar, dass Politiker und Mitarbeiter mit einer vollständigen Identität arbeiten. Die BenutzerID ergibt sich aus einer – sprechenden – achtstelligen Kombination aus Familien- und Vorname. *Abbildung 62: Beispiel Benutzeraccount/Profil* Landesverwaltung zeigt die Vielzahl an Attributen, die über einen Benutzer am Beispiel von Testuser „Karl Mitarbeiter“ (ID: *mitarbek*) gespeichert und bei jeder Anmeldung mitgeschickt werden. Die Palette der Attributdaten reicht vom Namen über die Bezeichnung der Abteilung bis hin zu privaten Rufnummern. Durch das Arbeiten mit Profilen[824] entsteht eine beträchtliche Ansammlung von Einstellungen[825] (z. B.: für Eigene Dateien, Windows Explorer, Netzwerk, Drucker) und History- bzw. Verbindungsdaten[826] (z.

[824] Auf Computern unter Windows-Betriebssystemen werden über Benutzerprofile die Einstellungen für die Arbeitsumgebung jedes Benutzers erstellt und verwaltet.
[825] Vgl. http://technet2.microsoft.com/windowsserver/de/library/b4418d02-1339-41c8-9eeb-fd72553f0bdc1031.mspx?mfr=true [15. März 2008]
[826] Vgl. http://technet2.microsoft.com/windowsserver/de/library/b4418d02-1339-41c8-9eeb-fd72553f0bdc1031.mspx?mfr=true [15. März 2008]

B.: Cookies, zuletzt verwendete Dateien, Favoriten, Anwendungsdaten wie benutzerdefiniertes Wörterbuch, Verlaufsdaten und temporäre Dateien) – siehe *Abbildung 63: Daten in einem Profil*.

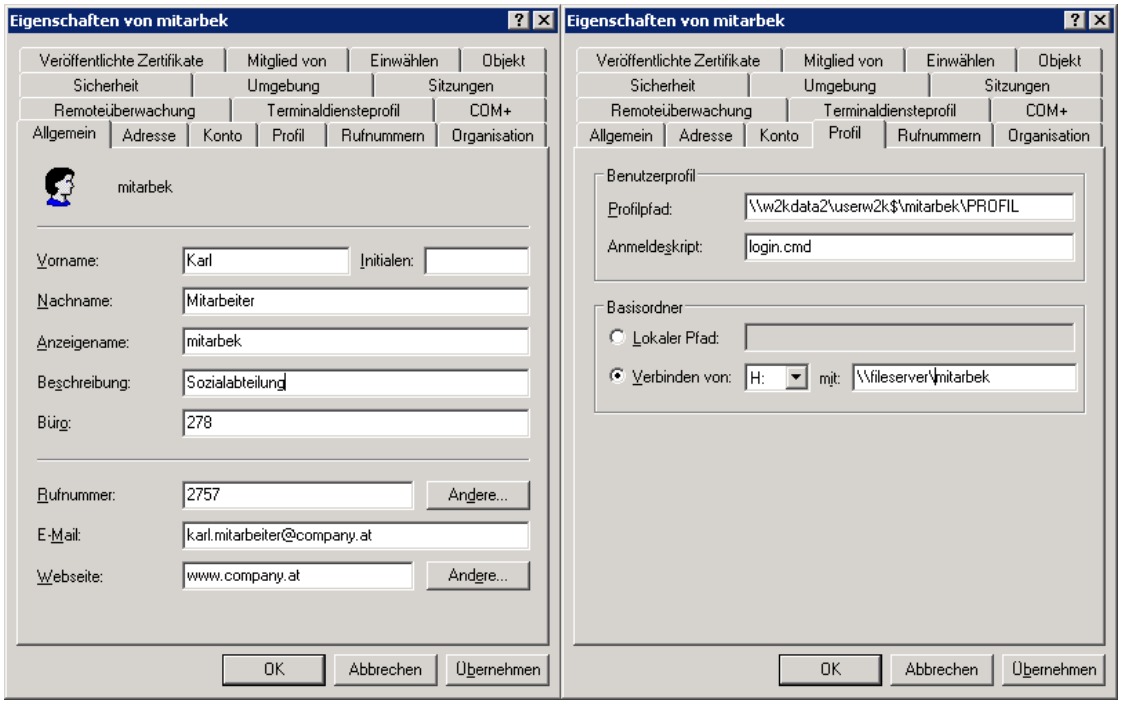


Abbildung 62: Beispiel Benutzeraccount/Profil Landesverwaltung

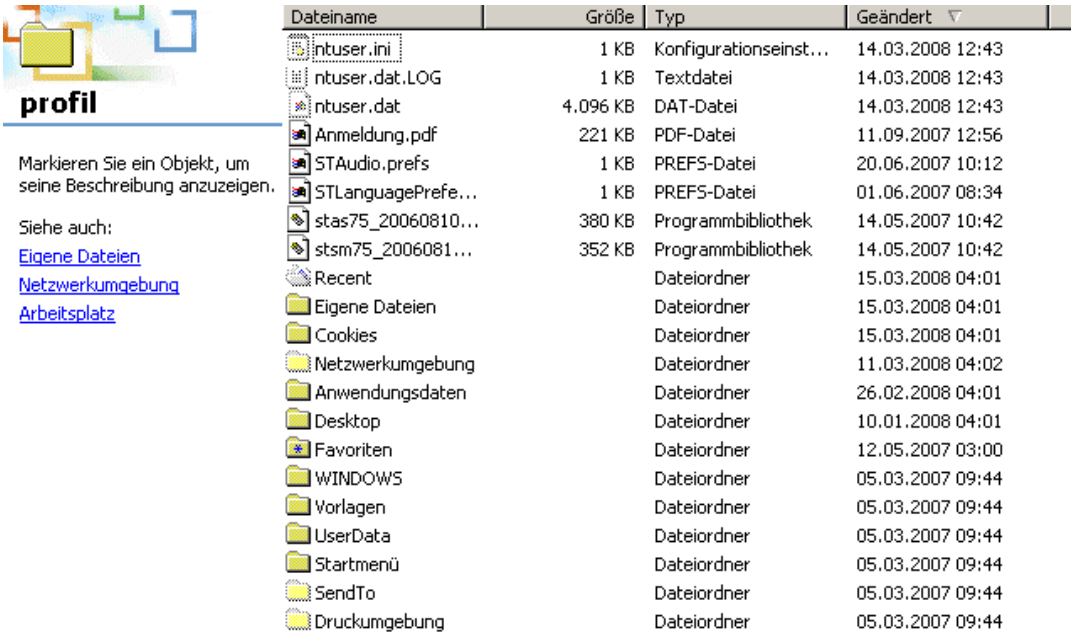


Abbildung 63: Daten in einem Profil

Bei allen anderen Systemen (Mailingsystem, Mobile Services etc.) wird bei der Verwaltung von Identitäten in Analogie dazu vorgegangen. Es ist somit für all jene Mitarbeiter (IT, Personalabteilung, Organisation etc.), die mit den Systemen, Verzeichnissen, Datenstrukturen und Abläufen in

irgendeiner Form in Berührung kommen, erkennbar, um welchen Benutzer es sich handelt. Durch die Zentralisierungs- und Konsolidierungstendenzen, im Konkreten der Einführung des Portalverbund- bzw. Identitätmanagementsystems, wird diese Transparenz noch weiter verstärkt.

Ziele

Die Ziele sollten eine möglichst hohe Unverkettbarkeit, eingeschränkte Aufdeckbarkeit und die Einhaltung der Absicherungs-, Identitäts-, Transparenz- und Vertraulichkeitsziele (siehe *3.2.1 Anforderungen an Identitätsmanagementsysteme und Datenschutz*) sein.

Der Zweck digitaler Identitäten besteht darin, bestimmte Attribute für bestimmte Situationen bereit zu stellen. Es ist wichtig, nicht automatisch alle Attribute einer Identität preis zu geben, sondern immer nur jene, die das Gegenüber (z. B.: Service, Applikation, Kommunikationspartner) verlangt (siehe *2.4.2.2 Datensparsamkeit*). Informationstechnik kann hier unterstützen, indem je nach Situation und Kontext unterschiedliche Pseudonyme (auch: Teil-Identitäten) statt der vollständigen Identität verwendet werden.

Wie kann ein Pseudonymisierungsansatz in der Landesverwaltung aussehen?

Der erste Schritt wäre die Änderung der *sprechenden* ID-Bezeichnungen. Hier bietet sich die Verwendung von Personen-Pseudonymen in Form einer Variante der Personalnummer an. Eine Variante deshalb, um den Effekt der Unidirektionalität von Identität und Pseudonym herstellzustellen. Um beim Beispiel von Karl Mitarbeiter zu bleiben, könnte seine pseudonymisierte ID „L0120822“ lauten. Das „L“ steht für die Landesverwaltung, „0“ als Platzhalter, die sechs Ziffern sind ein Ausschnitt seiner mehrstelligen Personalnummer. Da die Personalnummern entgegen den Gepflogenheiten in vielen anderen Unternehmen nicht öffentlich (z. B.: Intranet) aufscheinen, somit nur einem eingeschränkten Personenkreis bekannt sind, stellen sie für diesen Zweck die passende Grundlage dar. Für die Politiker und Mitarbeiter bedeutet die Änderung, dass sie sich einen neuen Benutzernamen merken müssen. Der Kontext zu bekannten Daten ist aus Gründen der leichteren Merkbarkeit wichtig. Damit soll verhindert werden, dass die Kennung nicht unter die Tastatur oder auf den Bildschirm geklebt wird (siehe *1.8.2.5.2 Sensibilisierung und Schulung, 1.8.3 Der Faktor Mensch*). Für die Administration hingegen bedeutet diese auf den ersten Blick triviale Maßnahme einen erheblichen organisatorischen und technischen Aufwand. Nach der Fixierung des Aussehens des Pseudonyms und der Festlegung des Gültigkeitsbereichs (z. B.: Landesverwaltung und alle nachgelagerten Organisationen) wäre eine naheliegende Vorgehensweise zur Ausbringung die, alle neu eintretenden Mitarbeiter gleich mit der pseudonymisierten ID auszustatten. Bei den bestehenden Usern könnte das abteilungsweise mit anschließender Kurzschulung erledigt werden. Im Vorfeld der Änderung sind in einer umfangreichen, genauen Analyse vor allem die Berechtigungen im Zusammenhang mit den diversen Systemen und Applikationen zu überprüfen. Es muss sichergestellt sein, dass sich die Mitarbeiter nach der Umstellung ohne Qualitätsverlust wieder überall

authentifizieren können, weil beispielsweise viele Systeme den Benutzernamen *hardcoded*[827] eintragen.

Das Ergebnis dieser Maßnahme sind pseudonymisierte Personen- und Protokolldaten.

Ein weiterer Schritt wäre das Weglassen respektive Reduzieren von servergespeicherten Profilen. Das würde einen großen Komfortverlust für die Politiker und Mitarbeiter bedeuten. Die Vorteile der Verwendung von Profilen liegen in der Personalisierung (siehe *2.2.4 Personalisierung*), der Mehrfachbenutzung eines PCs durch verschiedene Mitarbeiter und in der Wiederverwendbarkeit (*Roaming Profile*) an anderen Clients im selben Netzwerk. Damit wird es den Benutzern erlaubt, das Arbeitsumfeld (Netzwerklaufwerke, Desktop-Einstellungen etc.) an ihre Bedürfnisse anzupassen und diese persönliche Umgebung bei einer Anmeldung in derselben Domäne geräteunabhängig wieder vorzufinden. Nachdem aufgrund von *Desktop Sharing*-Modellen und wechselnden Arbeitsplätzen einzelner Mitarbeiter die Notwendigkeit für die Verwendung von solchen Profilen besteht, sollte unter Beibehaltung eines gewissen Komforts daher zumindest eine Reduzierung der Profilinhalte angestrebt werden. Dabei sollte für jedes Objekt hinterfragt werden, ob dessen Nutzen den verminderten Datenschutz übersteigt.

Ohne die Ergebnisse dieses Diskussionsprozesses vorwegnehmen zu wollen, zeigt die Empirie dem Autor, dass gewisse gesammelte Daten im Sinne eines Nutzen/Datenschutz-Verhältnisses vermeidbar sind. *Abbildung 64: Datenreduktion durch Profil-Redesign* zeigt in Fortführung des Beispiels (siehe zum Vergleich *Abbildung 63: Daten in einem Profil*) einen Vorschlag des Autors, in dem die Folder „Cookies“, „Recent“ und „Google Search History“ (Anwendungsdaten) aus dem Profil entfernt wurden.

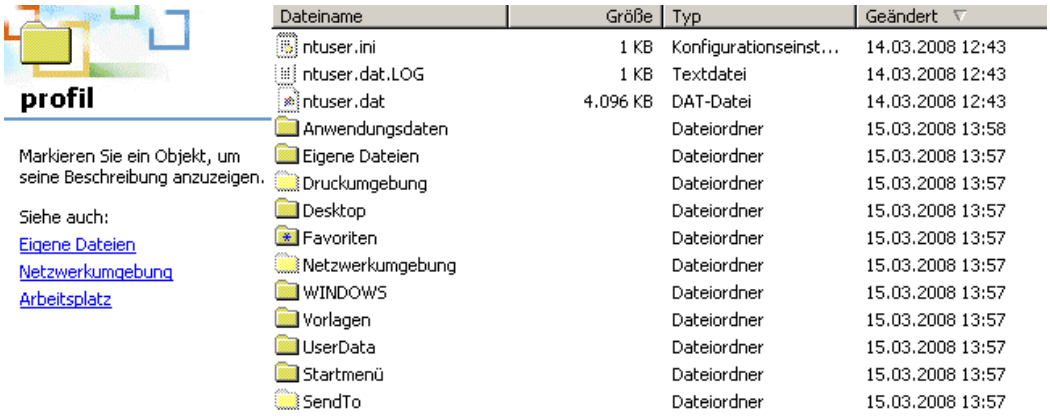


Abbildung 64: Datenreduktion durch Profil-Redesign

Die vorgestellte Maßnahme zielt im Sinne der Datensparsamkeit auf die Reduzierung von Inhaltsdaten. Zusammen mit der Verwendung von pseudonymisierten IDs wird ein Rückschluss auf einen Benutzer wesentlich erschwert.

[827] Beim Hardcodieren wird anstelle einer Variablen der absolute Wert im Source Code fixiert.

Durch die Verwendung von Personen-Pseudonymen sammeln sich Informationen an, sodass nach einer gewissen Zeit dessen Inhaber de-anonymisiert werden kann. Dieser Nachteil wird durch den Einsatz von Rollen-Pseudonymen vermieden. Eine Person kann in einem Unternehmen unterschiedliche Rollen (siehe *3.6.3 Von der Identität zur Rolle*) ausfüllen und somit mehrere (Teil-) Identitäten gleichzeitig annehmen. Der Benutzer wählt für jede seiner Rollen ein eigenes Pseudonym, in Fortsetzung des Beispiels eines für die Rolle als Sozialarbeiter (kurz: SA), ein zweites als Referatsverantwortlicher (kurz: RL) und ein drittes als Projektleiter (kurz: PL) (siehe *Abbildung 57: Jugendwohlfahrt - Authority Model*). Bei der Umsetzung muss nach dem Erforderlichkeitsprinzip sowie dem Grundsatz der Datenvermeidung gehandelt und die Repräsentation von Pseudonymen und Rollen mit verschiedenen Eigenschaften überlegt werden. In jedem Anwendungszusammenhang ist zunächst nach dem Erforderlichkeitsprinzip eine Analyse zu machen, wer welche personenbezogenen Informationen benötigt. In Überprüfung der Verfahren unter dem Gesichtspunkt einer möglichen Datenvermeidung fällt auf, dass Informationen wie der Name oft nicht erforderlich sind. Meist reicht es aus, bestimmte, für den Anwendungskontext definierte Eigenschaften zu garantieren. Der Personenbezug ist damit zur Erfüllung der Zweckbestimmung der Daten vielfach nicht notwendig.
Abbildung 65: Rollen-Pseudonyme zeigt eine Auswahl an Attributen der vollständigen Identität „Karl Mitarbeiter“, welche in anderer Form in *Abbildung 62: Beispiel Benutzeraccount/Profil Landesverwaltung* dargestellt wurde. Karl Mitarbeiter ist Sozialarbeiter, leitet gleichzeitig das Referat und hat zudem die Aufgabe der Einführung eines Wissensmanagementprojekts für diesen Bereich (siehe *Abbildung 57: Jugendwohlfahrt - Authority Model*). Er agiert in drei unterschiedlichen Rollen mit entsprechend verschiedenen Attributen[828]:

- Rolle „SA“: Als Sozialarbeiter hat er eine beratende und betreuende Tätigkeit, für die er Klientendaten zu verwalten hat [*Berechtigung 4, Berechtigung 5*]. Er muss demnach über Lese- und Schreibrechte [*Granularität-Berechtigung 4, Granularität-Berechtigung 5*] in der Klienten-Datenbank verfügen. Zudem ist für den Anwendungskontext die Organisationseinheit [*Organisationseinheit*] erforderlich.
- Rolle „RL“: Diese Rolle entspricht der eines Sozialarbeiters. Dazu kommt eine leitende und koordinierende Komponente, für deren Ausübung zusätzliche Rechte [*Berechtigung 1, Granularität-Berechtigung 1; Berechtigung 2, Granularität-Berechtigung 2*] benötigt werden. Eine über SAP umgesetzte Unternehmensrichtlinie besagt, dass die Höhe über die eigenverantwortliche Verwendung von Geldmitteln von der Position in der Hierarchie abhängig ist. Aus diesem Grund wird das Attribut [*Position*] beigefügt.

[828] Die Attribute werden in eckigen Klammern dargestellt. Granularität-Berechtigung x beschreibt die Zugriffsrechte (z. B.: lesen, schreiben) auf eine Ressource.

- Rolle „PL“: Der Projektleiter soll ebenfalls eigenmächtig über Geldmittel verfügen können [*Position*]. Für den Zugriff auf die Projektdaten und deren Verschlüsselung werden eine Berechtigung und ein Zertifikat [*Zertifikat 1*] benötigt.

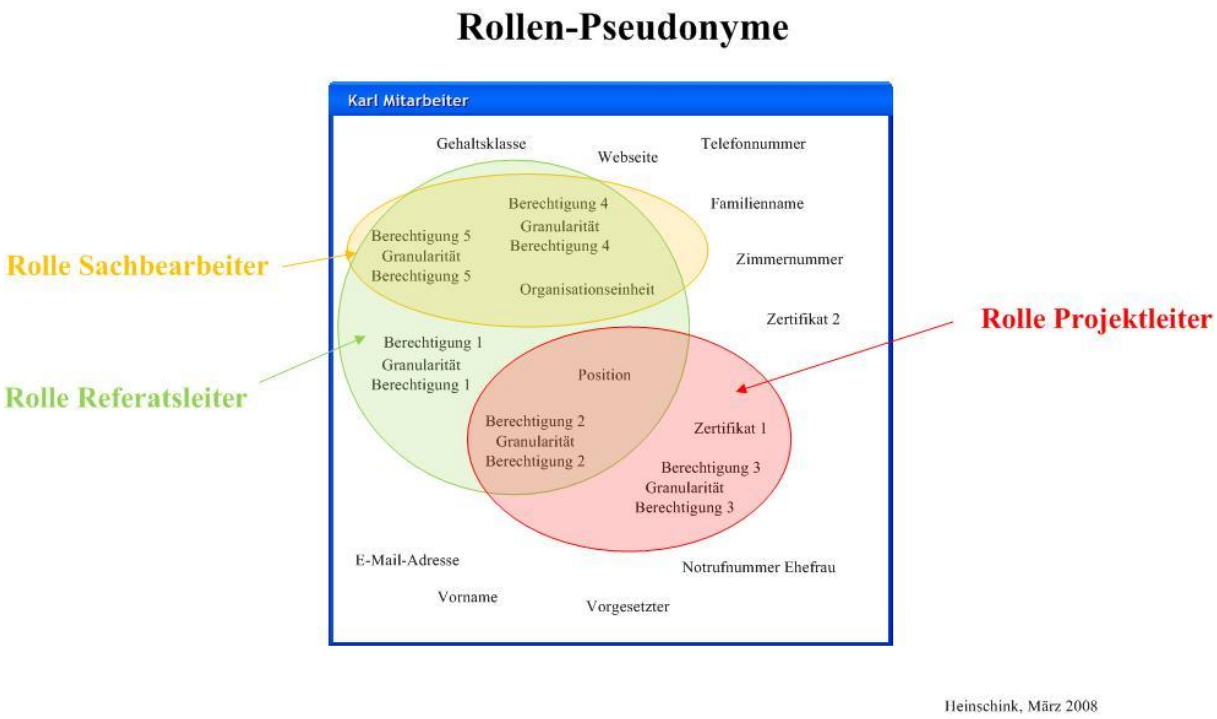


Abbildung 65: Rollen-Pseudonyme

Durch die Aufteilung einer vollständigen Identität auf mehrere Teilidentitäten bei gleichzeitig sparsamen Umgang mit Attributen (siehe am Beispiel Karl Mitarbeiter) wird eine Verminderung der Transparenz erzielt. Zudem wird die Anzahl jener, die ein Pseudonym aufdecken können, kleiner. Da eine Rolle personenunabhängig ist, kann das entsprechende Pseudonym bei einem Jobwechsel von Person A auf Person B übertragen werden.

Um es den Usern möglichst leicht zu machen, ihre verschiedenen Pseudonyme zu verwalten, ist eine komfortable Bedieneroberfläche (siehe *3.4.4.2.9 User Interface*) auf Basis eines Identitätsmanagementsystems essentiell.

Für die rechtlichen Rahmenbedingungen zur Verwendung von Pseudonymen darf auf *1.7.3.1 Datenschutz* und *2.3.2.2 Zusammenhang von Identitätsmanagement und Datenschutz* verwiesen werden.

Das Ergebnis dieser Maßnahme zielt auf eine weitere Erhöhung der Unverkettbarkeit und eine Reduktion der Aufdeckbarkeit ab.

3.6.5.4 Status der Umsetzung und Ausblick

Die erste Phase in der Etablierung eines Identitätsmanagementsystems ist mit der Einführung der Portalverbund-Lösung abgeschlossen. Die Mitarbeiter haben über eine Webseite, wo sie sich nur einmal authentifizieren müssen, Zugang zu den ihnen zustehenden Behördenapplikationen. Die Lösung funktioniert bis auf wenige technische Feinheiten einwandfrei. Die autorisierungsberechtigten Mitarbeiter vergeben nach Funktion bzw. Rolle die entsprechenden Rechte an die Sachbearbeiter. Die Verantwortungsdelegierung bewirkt, dass bei der Rechtevergabe mit der höchsten Sorgfalt vorgegangen wird. Bedarf besteht noch beim Aufbau einer redundanten Betriebsinfrastruktur und einer vollwertigen Testumgebung. Letztere ist in der Fertigstellungsphase, weil in absehbarer Zeit mit Tests eines Nachfolgeprodukts für einen obsolet werdenden technischen Baustein begonnen werden muss.

Mit der steigenden Anzahl an Applikationen wachsen auch die Anforderungen an die Sicherheit. Waren bis dato Passwörter ausreichend, bedingen immer mehr Anwendungen eine Zwei-Faktoren-Authentifizierung aus Wissen und Besitz. Die nächste Herausforderung in diesem Umfeld besteht daher in der Realisierung eines Chipkarten-Projekts. Die Anforderungen beschränken sich zunächst auf die Bedürfnisse aus dem Portalverbund. Gleichzeitig soll die Infrastruktur so ausgestaltet werden, dass sie für geplante Einsatzgebiete (z. B.: Bürgerkarte, Gleitzeit) vorbereitet ist.

Für die Erweiterung in Richtung eines umfassenderen Identitätsmanagementsystems sind bereits technische und organisatorische Maßnahmen getroffen worden (respektive in Entwicklung). Die Umsetzung soll modulartig bzw. nach Bedarf erfolgen.

Die zur Stärkung der informationellen Selbstbestimmung angedachten Maßnahmen der Einführung von pseudonymisierten Daten und Pseudonymen sind im Status der Diskussion respektive vereinzelt in Umsetzung: z. B.: die Reduzierung der Profil-Daten, die Verwendung von pseudonymen IDs bei isolierten, internen Systemen. Einen Grund für die zaghaften Fortschritte dafür stellt die fehlende Security-Governance dar. Während die technischen Maßnahmen von der IT autark durchgeführt werden können, sind die organisatorischen Aufgaben mit Abhängigkeiten zu anderen Organisationseinheiten verbunden. So ist beispielsweise die unternehmensweite Rollendefinition primär Angelegenheit der Organisationsabteilung. Der Umsetzungsplan und -zeitpunkt sind abhängig von einer umfassenden Adaptierung des Organisationsplans, dessen Finalisierung derzeit noch aussteht.

4 FAZIT UND AUSBLICK

Seit einigen Jahrzehnten befindet sich die Wirtschaft in einem weltweiten Transformationsprozess. Nur diejenigen Unternehmen, die Veränderungen frühzeitig erkennen, sich flexibel anpassen, werden dem weiter zunehmenden Konkurrenzdruck gewachsen sein und auf Dauer bestehen können. Für die Bereitstellung und Nutzung von Informationen sind Informationssysteme erforderlich, die immer komplexer werden. Fehlerhafte Informationssysteme führen schnell zu Produktionsausfällen, verzögerter Bearbeitung oder Datenverlust, folglich zu materiellem bzw. immateriellem Schaden. Ein Hauptgrund für die Ausfälle sind Sicherheitsmängel solcher Systeme. Die Herausforderung für die Unternehmen besteht daher darin, durch ihr Verhalten und ihre Organisation Prozesse und Infrastruktur nachhaltig sicherzustellen, sodass Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit der Informationen gewährleistet sind. Dem Management der Informationssicherheit kommt deshalb eine steigende strategische und operative Bedeutung zu. Informationssicherheitsmanagement dient dazu, mit diversen Bedrohungen und Risiken umzugehen. Um ein entsprechendes Sicherheitsniveau zu erreichen, genügt es nicht mehr, sich mit einzelnen technischen Maßnahmen zufrieden zu geben. Vielmehr ist ein holistischer Ansatz notwendig: Schaffung eines Rahmenwerkes, in dem einzelne technische, rechtliche oder organisatorische Maßnahmen aufeinander abgestimmt werden. Durch die Kombination der richtigen Technologien, Prozesse und Maßnahmen lässt sich eine robuste Infrastruktur aufbauen, die flexibel anpassbar ist und bei einem Höchstmaß an Informationssicherheit gleichzeitig für einen weitgehend unterbrechungsfreien Geschäftsbetrieb sorgt.

Der wachsende Umfang und die Vielfalt der Datenverarbeitungen führten zu einer starken Zunahme personenbezogener Daten mit hoher Aussagekraft. Sie erlauben, individuelles Verhalten ebenso detailliert nachzuvollziehen wie kollektive Lebensstrukturen. Treibende Faktoren sind vor allem der steigende Einsatz von Internettechnologien in allen Lebensbereichen und die allgegenwärtige Datenverarbeitung. Wenn Datenverarbeitung so funktioniert wie sie soll, kann sie immer auch als Überwachungstechnologie genutzt werden. Die technischen Konzepte sind entwickelt und es existieren eine Reihe von Services und Tools, die den Anwendern eine anonyme bzw. pseudonyme Nutzung ermöglichen oder sie vor unbemerkten Datensammlungen bewahren können. Unter der Voraussetzung eines bestmöglich geschützten Privatbereichs soll dem Benutzer die Hoheit über seine Daten gegeben werden. Dazu notwendig sind freiheitsfördernde Architekturen der Informationstechnik, die die Zusammenführung personalisierbarer Daten durch „informationelle Gewaltenteilung“ verhindern.

Identitätsmanagementsysteme stellen solche Architekturen dar. Sie zielen darauf ab, eine einheitliche, systemübergreifende Plattform für die Verwaltung von Benutzern, deren Konten und deren Berechtigungen zu schaffen. Die vorliegende Arbeit unterstreicht anhand einer praktischen Umsetzung aus dem Unternehmen des Autors die zunehmende Bedeutung des Managements digitaler Identitäten. Zum einen erfordert das Denken in übergreifenden Geschäftsprozessen eine einheitliche und offene

Infrastruktur. Zum anderen setzt der Trend zu verteilten Anwendungen und zur Ressourcenvirtualisierung – etwa in Form von Service-orientierten Architekturen – digitale Identitäten sowie automatisierte Rechteprüfungen voraus. Mit der unternehmerischen Dynamik verstärkt durch Mitarbeiterfluktuation und Personalrochaden steigt der Bedarf am Rollen- und Rechtemanagement. Die durch E-Business bzw. E-Government verschwimmenden Unternehmensgrenzen erfordern eine neue, identitätsbasierte Sicherheitsarchitektur. Neue Gesetze und Regulative aus der Finanz- oder Industriewelt setzen die Unternehmen im Sinne der Nachhaltigkeit und Auditierbarkeit unter Druck. Die unter dem Stichwort „Corporate Governance“ geführte Diskussion hat damit einen verbindlichen Rechtsrahmen erhalten, der für viele Unternehmen die Notwendigkeit mit sich bringt, Sicherheit und Zuverlässigkeit IT-gestützter Prozesse neu zu bewerten. Diese Compliance-Ansprüche sind nur durch einen hohen Grad an Automatisierung erfüllbar. Ergänzt werden diese Anforderungen durch verstärkte Diskussionen hinsichtlich des Schutzes privater Informationen und Tätigkeiten von Mitarbeitern in Unternehmen. Das Überführen von Funktionalitäten und das Konsolidieren von Applikationen in einige wenige Systeme erhöhen bei gleichzeitig verbessertem Reporting die Möglichkeiten zur Überwachung.

Identitätsmanagementsysteme sollen im betrieblichen Umfeld dem Benutzer die größtmögliche Freiheit über seine Daten geben. Dabei sind die Grundsätze der Datenvermeidung und Datensparsamkeit bei der Gestaltung der Technik und ihrer Einsatzbedingungen zu berücksichtigen. Verfahren müssen demnach so ausgestaltet werden, dass nur so viele personenbezogene Daten gesammelt und gespeichert werden, wie für die jeweilige Anwendung unbedingt notwendig sind. Die Möglichkeiten der Administration und der Vorgesetzten, Mitarbeiter überwachen zu können, sollen zumindest eingeschränkt werden. In dieser Arbeit werden die dazu erforderlichen technischen und organisatorischen Maßnahmen beschrieben. Zunächst sind den inhärenten Funktionen und Komponenten eines Identitätsmanagementsystems Werkzeuge zur Pseudonymisierung und Anonymisierung beizufügen. Dann soll die Verwaltung der Benutzerdaten und -berechtigungen aufgeteilt werden. In der Regel wird diese Tätigkeit bislang ausschließlich vom EDV-Administrator erledigt. Organisatorisch soll die Arbeitsteilung hinsichtlich Identitätsverwaltung auf IT-Abteilung, Personalabteilung und Mitarbeiter selbst erfolgen. Diese Dreiteilung bringt mit sich, dass die Gesamtsicht des Verwaltungspersonals auf die Daten des einzelnen Mitarbeiters eingeschränkt wird. Zudem sollen der vorgesetzten Instanz nur jene Daten zur Verfügung gestellt werden, die aus rechtlichen und ökonomischen Gründen zwingend bzw. notwendig sind. Als weitere Selbstbestimmungsmaßnahme soll der Benutzer eine dienstliche und eine private Rolle annehmen können. Die dienstliche Rolle entspricht der vollständigen Identität und erfüllt drei Funktionen. Die erste erlaubt dem Mitarbeiter einen singulären Zugang zu seinen Ressourcen (Netzwerk, Betriebssystem, E-Mail, Drucker, Filesystem, Applikationen etc.). Die zweite befähigt ihn, gewisse administrative Aufgaben selbstständig, ohne Abhängigkeit von Dritten, durchzuführen. Mit der dritten

kann er seinen Part für die Aufrechterhaltung des Identitätslebenszyklus erfüllen, indem er seinen Datenbestand wartet. Mit der privaten Rolle wird dem Mitarbeiter die Möglichkeit eingeräumt, persönliche Tätigkeiten wie Online-Banking, privater Besuch von Webseiten, Blogs etc. ohne Überwachungs- und Eingriffsmöglichkeit der IT bzw. sonstiger Instanzen (z. B.: Personalabteilung, Vorgesetzter) durchzuführen.

4.1 RANDBEDINGUNGEN UND GRENZEN VON IDENTITÄTSMANAGEMENT

Identitätsmanagement stellt eine übergreifende, unternehmensweite Aufgabe für Unternehmensführung, IT-Leitung und Informationssicherheit dar. Die Bedingung für die Realisierung ist das Vorhandensein einer entsprechenden Lobby im Unternehmensmanagement. Identitätsmanagementsysteme müssen in der Form geplant und etabliert werden, dass sie im Kontext von Informationssicherheit die geschäftlichen Aktivitäten eines Unternehmens optimal unterstützen. Eine Hürde stellt dabei die durchgängige Umsetzung von Policies im Bereich der Informationssicherheit bis auf Systemebene dar, die klare organisatorische Regeln verlangt. Bei der Realisierung von Identitätsmanagement stellt sich schnell die Frage nach der organisatorischen Reife eines Unternehmens für ein solches Projekt. Aus der Reife eines Unternehmens kann auf die Risiken und den Implementierungsaufwand geschlossen werden. Viele Identitätsmanagement-Projekte laufen zeitlich und finanziell aus dem Ruder, weil deren Komplexität unterschätzt wird. Dabei tauchen spezielle Problembereiche auf wie die Qualität der Benutzerdaten, rollenbasierte Berechtigungen versus direkt zugewiesene Berechtigungen bis hin zu der Diskussion, welches das beste Rollenmodell ist.

Viele Unternehmen machen den Fehler, die Erzielung einer möglichst hohen Datenqualität und die Benutzerverwaltung als rein technisches Problem einzustufen. Es kann keine zuverlässige Autorisierung und Authentifizierung geben, wenn die User gezwungen sind, sich gegen eine unzuverlässige Datenbasis auszuweisen. Bei Identity Federation geht es darum, Vertrauen herzustellen. Das hängt einerseits vom Sicherheitsniveau des Identity Providers und der Stärke der Authentifizierung ab, andererseits von der Qualität der von ihm verwendeten Identitätsdaten. Compliance-Ansprüche können ohne verlässliche Datenbasis nicht erfüllt werden. In jedem Fall gilt, dass die Qualität von Identitätsdaten als strategische, unternehmensübergreifende Aufgabe begriffen werden muss. Qualität setzt definierte Prozesse und Verantwortlichkeiten für Änderungen voraus, vom Self Service bis hin zu Stellen im Unternehmen, die die Qualität der Daten messen und bei Problemen frühzeitig gegensteuern. Qualität kann dabei nur durch eine integrierte Sicht entstehen: entweder durch die Nutzung eines Datenbestandes an verschiedenen Stellen (z. B.: Identity Federation) oder durch eine Synchronisation von Informationen, wie sie über Provisioning-Lösungen realisiert werden. Ein Unternehmen sollte sich neben der Verbesserung der Datenqualität auf zwei weitere wesentliche

Eckpfeiler konzentrieren. Zum einen sind dies die Mitarbeiter, damit die Notwendigkeit einer hohen Datenqualität zur Selbstverständlichkeit wird. Zum anderen geht es um die Prozesse. Entsprechende Regeln, Workflows und Audits sollten fester Bestandteil der Unternehmenskultur sein und von den Angestellten gelebt werden. Da es kein allgemein gültiges Patentrezept – unabhängig von Branche und Größe – gibt, muss eine Lösung zudem flexibel und individuell auf die Bedürfnisse des jeweiligen Betriebes zugeschnitten sein.

Eine Schlüsselanforderung ist die solide Definition von Identität, die sich auf die unterschiedlichen Prozesse, Programme und die bestehende IT-Infrastruktur einstellt. Im Rahmen einer Bedarfsanalyse sind die Anforderungen und Verantwortungen zu ermitteln, die aus den Geschäftsprozessen resultieren. Dies stellt die Basis für die Modellierung von Rollen- und Berechtigungskonzepten sowie für das Design der Prozesse dar. Die Rollendefinition ist in hohem Maße eine organisatorische Herausforderung. Weiters muss das Schutzniveau der Daten festgelegt werden, um angemessene Authentifizierungsverfahren auswählen zu können. Bei der technischen Sollfestlegung werden die Anforderungen an die IT-Architektur gemeinsam mit den verantwortlichen Administratoren definiert. Dabei gilt es zu überlegen, inwieweit vorhandene Komponenten genutzt werden können. Aus technischer Sicht konkurrieren verschiedene Architekturansätze. Es geht einerseits um die Datenhaltung – relationale Datenbank versus LDAP[829]– und um die Entscheidung, entweder ein modulares System mit zentraler und komponentenübergreifender Modellierung einzuführen oder eine lose Kopplung einzelner Produkte mit einer Synchronisation der User- und Strukturdaten zwischen den Produkten. Die Etablierung einer abstrahierten, unternehmensweiten Verzeichnisstruktur – vielfach Metadirectory genannt – muss sehr gut überlegt sein, oft führt ein Super-Directory nur zu überhöhten Kosten ohne die versprochene Effektivität. Zu beachten ist ferner, dass Rahmenlösungen von vielen Herstellern zur Verfügung stehen, jedoch Anpassungen erfordern. Beim Auditing fehlt es sowohl an Standards als auch an Produkten, die die Herausforderung wirklich umfassend adressieren. Je komplexer und unübersichtlicher die bisherigen Applikationen und die IT sind, desto teurer kommt die Implementierung. Schon bei der Planung ist zu beachten, dass die Umsetzung eines Identitätsmanagementsystems für eine große Anzahl von Benutzern in mehreren Phasen ablaufen soll und je nach Intensität zumindest ein Jahr lang dauern kann.

Die Durchführung von IT-Projekten, speziell Qualitätsthemen wie Identitätsmanagement, scheitert oft am gegenseitigen Unverständnis zwischen Business und IT. Der Abteilungsleiter bzw. Geschäftsführer und IT-Leiter „sprechen nicht die gleiche Sprache“. IT-Governance steht erst am Anfang der Verbreitung, findet nur zaghaft Anwendung in den Unternehmen. Es gibt aber noch weitere Hürden bei der Umsetzung, mit denen sich der Autor konfrontiert sieht.

[829] LDAP (steht für: Lightweight Directory Access Protocol) ist ein Protokoll für die Kommunikation zwischen dem sogenannten LDAP-Client und dem Verzeichnis (Directory Server). Ein solcher Verzeichnisdienst enthält objektbezogene Daten (z. B.: Personendaten, Systemkonfigurationen etc.).

Eine Hürde entsteht durch die fehlende Verbindung von Strategie und Technologie. Identitätsmanagement-Projekte müssen sowohl auf technische Lösungen von Problemen fokussieren als auch den strategischen Blickwinkel beinhalten. Sie dürfen nicht als Insellösung angelegt sein, sondern müssen auf das gesamte Unternehmen erweiterbar sein. Das bedeutet aber nicht, dass alle Systeme und Bereiche von Beginn an eingebunden sein müssen.

Eine zweite Hürde ergibt sich aus den Funktionsanforderungen an Identitätsmanagementlösungen und der damit verbundenen Komplexität. Ein Benutzer soll beispielsweise im Sinne der Funktion „Self Service" eine Web-Schnittstelle nutzen, um die Kennwörter in den angeschlossenen Anwendungen auf einen Wert zu setzen. Neben dem Umstand, dass die Kennwortrichtlinien der verschiedenen Systeme voneinander abweichen (z. B.: ein System unterstützt bei der Passwortlänge maximal sechs Zeichen, ein anderes acht) und nicht immer homogenisiert werden können, zeigt sich oft, dass die IDs in den verschiedenen Verzeichnissen unterschiedlich sind, „Karteileichen" somit die Folge sein können. Soll dennoch eine Passwort-Management-Lösung für verschiedene Systeme umgesetzt werden, gilt es, eine integrierte Sicht auf Identitäten zu schaffen. So wird aus einem scheinbar kleinen Projekt ein komplexes, in dem es um Datenqualität, Metadirectory und Provisioning geht.

Eine weitere Hürde stellt das fehlende *Pouvoir* der IT dar. Beim Identitätsmanagement werden Daten aus verschiedenen Verzeichnissen zusammengeführt – Datenquellen, über die verschiedene Stellen im Unternehmen die Hoheit haben. Da gibt es beispielsweise die Personalabteilung mit dem Personalinformationssystem, die Betreiber der ERP[830]-Umgebung oder die Administratoren des lokalen Netzwerks. Fehlt der IT-Abteilung die Unterstützung der Organisation bzw. Unternehmensleitung, kann das neben der technisch anspruchsvollen Herausforderung aufgrund zu leistender Überzeugungsarbeit zumindest eine zeitliche Verzögerung, im *worst case* sogar einen Projektstopp nach sich ziehen.

Werden die Antworten zu einigen Fragestellungen nach Einführung eines Identitätsmanagementsystems und einer angemessenen Durchlaufzeit überprüft, schaut die Bilanz erfahrungsgemäß nicht durchgängig positiv aus. Wurden die ursprünglichen Erwartungen vom eingeführten System erfüllt? Konnten die Kostensenkungspotenziale ganz oder teilweise erschlossen werden? Ist die Produktivität der Mitarbeiter gestiegen? Werden die Compliance-Ansprüche erfüllt? Das Problem ist, dass die Erwartungen in Bezug auf Kostenreduzierung, Verbesserungen des Komforts, Compliance etc. und die Realität noch immer auseinander gehen. Das ist auch darauf zurückzuführen, dass die Hersteller ihre Kunden nicht umfassend genug darüber informieren, was es bedeutet, ein IMS einzuführen. Andererseits kann es an der Organisation liegen, die ihre Prozesse

[830] ERP (steht für: Enterprise Resource Planning) bezeichnet die unternehmerische Aufgabe, die in einem Unternehmen vorhandenen Ressourcen (Kapital, Betriebsmittel, Personal) möglichst effizient für den betrieblichen Ablauf einzusetzen.

nicht entsprechend anpasst. Es scheint so, als ob die angebotenen Lösungen und die Prozessreife bei den Unternehmen noch nicht kompatibel genug zueinander sind.

4.2 AUSBLICK

Für die kommenden Jahre identifizieren Experten neue Gefahrenpotenziale für die Unternehmen. Der Datenschutz auf mobilen Endgeräten bedarf erhöhter Aufmerksamkeit, wird jedoch zunehmend schwieriger zu lösen. Banken müssen Personen- und Kontendaten noch besser sichern, das gilt insbesondere, wenn die Transaktionen von mobilen Geräten ausgeführt werden. Da der immer wichtiger werdende Austausch von elektronischen Datensätzen Sicherheitsrisiken birgt, werden Unternehmen den Einsatz von Verschlüsselungstechnologien noch viel stärker forcieren müssen. Die weiter fortschreitende Öffnung der Unternehmen und die damit verbundenen Technologien bringen neue Informationssicherheitsgefahren mit sich. Die Transformation zum „Unternehmen 2.0“, unterstützt durch eine partizipative Unternehmenskultur, Web 2.0-Lösungen und SOA[831] wird immer mehr als unternehmensstrategische Aufgabe gesehen. Mit dem Einzug von Web 2.0 in Unternehmen entwickelt sich eine neue Form von Wissensmanagement und damit eng verknüpfter Konzepte wie Collaboration. In Verbindung mit Social Software wie Wikis, Blogs und Social Bookmarking werden die Inhalte durch die Mitarbeiter erstellt. Über die Kommentierung und Bewertung wird die Qualität gesichert. Durch diese Anwendungen verändern sich Geschäftsprozesse, neue Vertriebswege werden etabliert und die Benutzer wissen in ihrer Gesamtheit als „kollektive Intelligenz“ mehr als die Experten, weil sie sich in Communities miteinander austauschen und lose, bedarfsorientierte Beziehungen knüpfen.

Hinsichtlich IT-Betriebsführung ist zu beobachten, dass die Bereiche Informationssicherheit und ITIL[832] weiter zusammenwachsen. Unternehmen verstärken die Investitionen in die operative Informationssicherheit. Das bringt Lösungen nicht nur zur Sicherheitsüberwachung, sondern auch zu den Service Support-Themen Störungs-, Problem-, Änderungs- und Konfigurationsmanagement. Somit wird der Ansatz der umfassenden Unterstützung aller operativen Sicherheitsprozesse in einem Unternehmen immer kompletter.

Aus IT-Sicherheit wurde durch die ganzheitliche Betrachtungsweise im physischen, technischen, organisatorischen und rechtlichen Bereich die Informationssicherheit. Das Aufgabengebiet eines Informationssicherheitsbeauftragen wächst analog zu den Entwicklungen. Neben dem Aufbau und der Durchführung eines Informationssicherheitsmanagementsystems gehören die Ausführung von

[831] *SOA* (steht für: Service Oriented Architecture) ist ein Rahmenwerk für die Integration von Geschäftsprozessen und unterstützender IT-Infrastruktur in Form von sicheren, standardisierten Komponenten (Services), die sich wiederverwenden und kombinieren lassen, um wechselnde Geschäftsanforderungen abzubilden.

[832] ITIL (steht für: Information Technology Infrastructure Library*)* ist ein de-facto-Standard für Gestaltung, Implementierung und Management elementarer Steuerungsprozesse in der IT.

Sensibilisierungsprogrammen, die Abhaltung von Koordinierungs- und Abstimmungsgesprächen, der Sitz in Fachausschüssen oder die Durchführung von Audits und Zertifizierungen zum umfangreichen Betätigungsfeld. Keine Stelle in der IT hat so viele Querschnittsfunktionen wie die Informationssicherheit. Die Handlungsfähigkeit eines Informationssicherheitsbeauftragten ist meist dadurch eingeschränkt, dass er nicht autonom über die vorgesehenen Budgetmittel verfügen kann. Er ist beispielsweise bei schnell zu treffenden Entscheidungen auf die Erreichbarkeit des IT-Leiters angewiesen. Im Sinne einer Security-Governance sollte der Informationssicherheitsbeauftragte mehr Unterstützung und Rückendeckung seitens des Unternehmens erfahren, indem er die notwendigen Mittel, Werkzeuge und Ressourcen zur Verfügung gestellt bekommt. Aufgrund der geänderten gesetzlichen Voraussetzungen (z. B.: EuroSOX[833]) ist die Haftungsfrage des Informationssicherheitsbeauftragten bzw. der im Vorstand zuständigen Person klärungsbedürftig. Aus heutiger Sicht besteht eine persönliche Haftung des Managements und wird als Organisationsverschulden sanktioniert werden.

Informationssicherheit entwickelt sich verstärkt zu einem Zukunftsthema für die Führungsetagen. Durch den stetig steigenden Grad an Vernetzung zwischen Unternehmen und die Steuerung der Kernprozesse über IT-Systeme wird ganzheitliche Informationssicherheit zu einer überlebenswichtigen Herausforderung. Unternehmenssicherheit ist zu einem Wettbewerbsfaktor geworden: Der Nachweis der Sicherheitsstandards gegenüber Kunden, Banken, Versicherungen, internen und externen Aufsichtsgremien ist unerlässlich geworden. Die Zertifizierung der sicherheitsrelevanten Prozesse und Systeme schafft Vertrauen in die Leistungsfähigkeit des Unternehmens.

„*Das Internet vergisst nicht, aber man kann es vergessen lassen*." Das Internet ermöglicht eine nahezu unbegrenzte Datensammlung und -speicherung. Während die Menschen vergessen, erinnert sich das Internet minutiös und dauerhaft an alles, was über jede einzelne Person gespeichert ist. Die Forderung nach einem Verfallsdatum für Daten ist durchaus gerechtfertigt. Die technische Umsetzung ist dabei nicht das Problem. Entscheidend wird sein, ob und wie weit die Daten speichernden Stellen auf eine derartige Forderung eingehen.

In der digitalen Welt spielt das Grundkonzept von Verkettung und (Un-)Verkettbarkeit eine wichtige Rolle, insbesondere wenn es um Datenverarbeitung in globalen Netzen geht. Jede Person hat eine wachsende Zahl von Identifikatoren und ihnen zugeordnete Identitätsattribute, etwa als Bürger, als Kunde einer bestimmten Firma oder als Benutzer einer Plattform im Internet. Digitale Identitäten sind

[833] EuroSox steht umgangssprachlich für die vom amerikanischen SOX abgeleitete europäische Version. Es handelt sich dabei um die 8. Europäische Richtlinie, welche am 17. Mai 2006 beschlossen wurde. Dabei geht es um Vorgaben für nationale Gesetze über Aktionärssicherheit sowie unabhängige Rechnungs- und Abschlussprüfung von Unternehmen bestimmter Rechtsformen. Ziel von EuroSox ist es, Transparenz darüber zu schaffen, wer auf welche Informationen im Unternehmensnetzwerk zugreifen kann und von wem wann welche Berechtigungen dazu erteilt wurden.

oft verkettet mit Informationen über diese Person, wie ihre sozialen Kontakte oder bestimmte Handlungen, die sie unter Nutzung dieser digitalen Identität vorgenommen hat. Diese Informationen können verfeinert oder erweitert werden, indem sie mit anderen Datenquellen verkettet werden oder Algorithmen eingesetzt werden, um diese auszuwerten.

Die beste Strategie, seine Privatsphäre zu schützen, ist jene der Datenvermeidung. Verfahren und Applikationen müssen so konzipiert werden, dass möglichst wenig personenbezogene Daten erfasst werden. Dieser Grundsatz muss bereits bei der Gestaltung von Technik und ihrer Einsatzbedingungen berücksichtigt werden. Für die Technikgestalter müssen Anreize geschaffen werden, Datenschutz in der Infrastrukturentwicklung zu integrieren. Besonders im Rahmen der E-Government-Aktivitäten sollte – aufgrund der Vorbildwirkung für die privatwirtschaftlichen Unternehmen – auf die Implementierung von Daten sparenden Technologien geachtet werden. Zudem ist es notwendig, die Benutzer entsprechend zu informieren, sie in die Lage zu versetzen, die Mechanismen zu erkennen, um dann bewusst eine Nutzungsentscheidung treffen zu können. Hinsichtlich Selbstregulierung gilt, dass einerseits bewusste Konsumenten und andererseits ein Staat, der bereit ist, bei Missachtung von Gesetzen entsprechende Sanktionen zu setzen, Grundvoraussetzungen für freiwillige Maßnahmen von Unternehmen sind. Als überwiegend unternehmensinterner Prozess mit eingeschränkter Kontrollierbarkeit ist ein faires Verhalten von Unternehmen notwendig, um die Privatsphäre der Kunden schützen zu können. Es ist entscheidend, dass sich die Akteure, also Technikgestalter, aber auch Recht und Politik, dieser Entwicklung zu mehr Verkettung digitaler Identitäten bewusst werden.

Die Entwicklung von Identitätsmanagement geht von monolithischen, funktional orientierten Produkten in Richtung service-orientierter Ansätze. Als wichtigste Trends sind dabei die Definition von Service-Schichten für Identitätsmanagement-Produkte in Form von Web Services, die Entwicklung von Lösungen für *Managed Services* im Identitätsmanagement, die Integration mit dem *Business Service Management* und die Unterstützung von *Software as a Service* zu nennen. Die heutigen, funktional orientierten Lösungen bieten nicht die nötige Flexibilität, dadurch entstehen vermeidbare Integrationsaufwände und Projektkosten. Die Zukunft gehört Anwendungen, die flexibel mit anderen Komponenten der IT-Infrastruktur zusammenarbeiten. Damit Anwendungen und Systemkomponenten Identitätsmanagement-Funktionen als Services nutzen können, müssen diese abstrahiert werden. Daraus ergeben sich zusätzliche Möglichkeiten für die Modularisierung von Identitätsmanagement-Komponenten und die Unterstützung von externen Workflows. Die Diskussion darüber, welche Modelle für die Ausführung von Services im Kontext von Identitäten für eine End-to-End-Sicherheit sorgen, unterstreicht die Bedeutung des Identitätsmanagements, insbesondere von Teilthemen wie Identity Federation und virtuellen Verzeichnissen, für SOA. IT-Governance und Compliance sind wichtige Treiber für den Wandel vom administrativen zum business-orientieren Identitätsmanagement. Mit der steigenden Nachfrage nach Governance und Compliance-Lösungen beginnen die klassischen zentralisierten Implementierungen von Identitätsmanagement-Technologien

wie Provisioning, Metadirectory und Access Management an ihre Grenzen zu stoßen. Zwar lassen sich damit – zumindest kurzfristig – Audit-Ziele erreichen und administrative Prozesse verbessern, bis zu einer reibungslosen Unterstützung dezentral organisierter, unternehmensübergreifender Prozesse ist noch einiges an Arbeitsaufwand nötig. Identitätsmanagement wird sich in den kommenden Jahren, gerade im Kontext der Governance- und Compliance Anforderungen und mit Blick auf eine das Business unterstützende IT, deutlich verändern und weiterentwickeln. Eine Zielrichtung dabei wird das *Enterprise Information Management* sein, bei dem die Information im Mittelpunkt steht. Anhand von Rollen können die Benutzer entscheiden, wer was mit der Information machen darf. Die Möglichkeiten der Service-Orientierung des Identitätsmanagements sind vielfältig. Jeder der Ansätze kann für ein Unternehmen nutzbringend sein. Aus diesem Grund ist es empfehlenswert, Service-Ansätze bei der Weiterentwicklung der Identitätsmanagement-Strategie zu beachten.

Der Gedanke der Service-Orientierung kann auf den Bereich des E-Government übertragen werden. In Zusammenarbeit aller Ebenen können konsolidierte Lösungen entwickelt werden, die sowohl mit Föderalismus und Gewaltenteilung im Einklang stehen als auch im Sinne des Service-orientierten One-Stop-Government den Einzelnen ins Zentrum stellen. In Weiterentwicklung des Portalverbundes empfiehlt sich ein an die jeweiligen User angepasstes Lebens- bzw. Geschäftslagenmodell: Bürger und Unternehmen erhalten Zugang zu ihren eigenen Daten. In diesem Zusammenhang könnte ein „Bürgerkonto“ Realität werden, wo die Bürger über ein Portal (*myGovernment*) Eingaben machen, Bescheide einsehen, aktuelle und historische Kontenstände abfragen sowie Zahlungen veranlassen können. Demnach können nicht mehr nur die Behörden, sondern die Bürger bzw. Betriebe selbst ihre Daten verwalten. Die technische Umsetzung von integriertem E-Government kann über erprobte Lösungskonzepte wie SOA erfolgen. Weitere architektonische Elemente in Analogie zum SOA-Konzept können ein *Service Access Layer* zum Identitäts- und Authentifizierungsmanagement und eine *Process Engine* für das Abbilden von Lebens- und Geschäftssituationen sein. Die rechtlichen Rahmenbedingungen sind durch das E-Government-Gesetz gegeben. Politisch gibt es allerdings Handlungsbedarf beim Eingriff in bestehende Verwaltungsstrukturen und -abläufe, beispielsweise bei verwaltungsübergreifenden Prozessen.

Viele der für ein vertrauenswürdiges Identitätsmanagement notwendigen Bausteine sind vorhanden, andere müssen erst entwickelt werden. Die Grundlagen dafür können in einer interdisziplinären Forschung und Entwicklung für die Konzeption, das Design und die Implementierung von Identitätsmanagementsystemen geschaffen werden. Sie sollte eine Rückkoppelung zwischen Recht und Technik berücksichtigen, um sowohl rechtliche Anforderungen technisch umzusetzen, als auch technische Ergebnisse bei der Interpretation geltenden Rechts und der Rechtsfortbildung einfließen zu lassen. Dies wird ein wichtiger Beitrag für die Diskussion sein, wie das Recht auf informationelle Selbstbestimmung umgesetzt werden kann.

5 QUELLEN

5.1 OFFLINE

5.1.1 BÜCHER/MANUSKRIPTE

[Amelung, 2002]
Amelung Ulrich, „Der Schutz der Privatheit im Zivilrecht: Schadensersatz und Gewinnabschöpfung bei Verletzung des Rechts auf Selbstbestimmung über personenbezogene Informationen im deutschen, englischen und US-amerikanischen Recht“, Mohr Siebeck, Tübingen, 2002.

[Beier, 2005]
Beier Christian, „Autonomie, Privatheit und Selbstbestimmung“, Seminararbeit, Humboldt Universität Berlin, 2005.

[Betz, Riegler, 2003]
Betz Fritz, Riegler Johanna, „Bilder der Arbeit im Spätkapitalismus – zum strategischen Machtverhältnis von Arbeit, Selbst und Technologien“, Erhard Löcker GmbH, Wien, 2003.

[Borking, 1997]
Borking John, „Der Identity Protector“, Datenschutz und Datensicherheit 11/96, Verlag Vieweg, Wiesbaden, 1997.

[Brauchle, 2000]
Brauchle Christian, „Qualitätscontrolling für Informationssysteme“, Dissertation, Universität Zürich, 2000.

[Österreichisches Sicherheitshandbuch, 2004]
Bundeskanzleramt Österreich, „Österreichisches IT-Sicherheitshandbuch“, Version 2.2, Österreichische Computer Gesellschaft, Wien, November 2004 (http://www.cio.gv.at/securenetworks/sihb/ [5. Mai 2007]).

[Österreichisches Sicherheitshandbuch, 2007]
Bundeskanzleramt Österreich, „Österreichisches IT-Sicherheitshandbuch“, Version 2.3, Österreichische Computer Gesellschaft, Wien, April 2007

[Bundeskanzleramt, 2006]
Bundeskanzleramt Österreich, „Behörden im Netz – Das österreichische E-Government ABC“, Österreichische Computer Gesellschaft, Wien, Jänner 2006 (http://www.cio.gv.at/egovernment/umbrella/ [5. Juli 2007]).

[Castells, 2005]
Castells Manuel, „Das Informationszeitalter I – Der Aufstieg der Netzwerkgesellschaft“, Leske+Budrich Opladen, 2003.

[Castells, 2003]
Castells Manuel, „Die Internet Galaxy – Internet, Wirtschaft und Gesellschaft“, 1. Auflage, VS Verlag für Sozialwissenschaften, Leske+Budrich, März 2005.

[Chaum, 1985]
Chaum David, „Security without Identification: Card Computers to make Big Brother Obsolete“, Communications of the ACM Nr. 10, Oktober 1985.

[Fleissner, 2005]
Fleissner Peter, „Verlässlichkeit von offenen Computersystemen“, Vorlesungsskriptum, Technische Universität Wien, 2005.

[Floyd, 1997]
Floyd Christiane, „Autooperationale Form und situiertes Handeln“, Deutscher Kongress für Philosophie, 1997.

[Frissen et al., 2007]
Frissen Valerie, Huijboom Noor, Kotterink Bas, van Staden Mildo, „The Glass House: Government Transparancy in a Networked Society“, in „Eastern European eGov Days 2007: Best Practice and Innovation“, Österreichische Computer Gesellschaft, Wien, 2007.

[Fuchs, Hofkirchner, 2003]
Fuchs Christian, Hofkirchner Wolfgang, „Studienbuch Informatik und Gesellschaft“, Wien, 2003.

[Holthaus, 2000]
Holthaus Marcus, „Management der Informationssicherheit in Unternehmen“, Dissertation, Universität Zürich, 2000.

[Janowicz, 2006]
Janowicz Krzysztof, „Sicherheit im Internet“, 2. Auflage, O’Reilly, Köln, 2006.

[Kunze, 2003]
Kunze Christian, „Digitale Identität und Identitäts-Management“, Diplomarbeit, Universität Hamburg, 2003.

[Maurer, 2007]
Maurer Hermann „Report on dangers and opportunities posed by large search engines, particularly Google“, Graz, September 2007

[Mezler-Andelberg, 2007]
Mezler-Andelberg Christian, „Identity Management – eine Einführung“, 1. Auflage, dpunkt Verlag, Heidelberg, Oktober 2007.

[Piller, 2005-1]
Piller Ernst, „Security“, Vorlesungsskriptum, Technische Universität Wien, 2005.

[Piller, 2005-2]
Piller Ernst, „Chipkarte/Smart Card und RFID – Gegenwart und Zukunft“, Vorlesungsskriptum, Technische Universität Wien, 2005.

[Proksch, 2006]
Proksch Wolfgang, „Rechtliche Aspekte von Informationstechnologien“, Vorlesungsskriptum, Technische Universität Wien, 2006.

[Rehäuser, Krcmar, 1996]
Rehäuser J., Krcmar H., „Wissensmanagement im Unternehmen. In: Schreyögg G., Conrad P. (Hrsg.): Managementforschung 6 – Wissensmanagement.“, Berlin – New York, 1996.

[Rickert, 2004]
Rickert Thoralf, „Integration von Datenschutzmechanismen in Identitäteninfrastrukturen“, Diplomarbeit, Universität Hamburg, 2004.

[Roßnagel, 2007]
Roßnagel Alexander, „Datenschutz in einem informatisierten Alltag“, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, 2007.

[Rössler, 2001]
Rössler Beate, „Der Wert des Privaten“, Suhrkamp Verlag, Frankfurt/Main, 2001.
[Stamer, 2005]
Stamer Jan, „Sicherheit und Anonymität im Netz“, Seminararbeit, Universität Freiburg, November 2005.

[Streitberger, 2003]
Streitberger Thomas, „Privacy am Rechnerarbeitsplatz – Datenschutzrechtliche Probleme durch die Protokollierung von Log-Files und e-Mails am Arbeitsplatz“, Master Thesis, Rechtswissenschaftliche Fakultät, Universität Wien, 2003.

[ULD, 2007]
Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein „Verkettung digitaler Identitäten“, Kiel, Oktober 2007

[Vise, 2006]
Vise David A., „Die Google Story“, Murmann, März 2006.

[Windley, 2005]
Windley Phillip, „Digital Identity“, 1. Ausgabe, O’Reilly, 2005.

[Weippl, 2004]
Weippl Edgar, „Internet Security“, Vorlesungsskriptum, Technische Universität Wien, 2004.

[Wojda, 2005]
Wojda Franz, „Organisation und Führung“, Vorlesungsskriptum, Technische Universität Wien, 2005.

[Wörndl, 2001]
Wörndl Wolfgang, „Privatheit und Zugriffskontrolle bei Agenten-basierter Verwaltung von Benutzerprofilen“, Dissertation, Technische Universität München, 2001.

[Zehentner, 2002]
Zehentner Johann „Privatheit bei Anwendungen für Identitätsmanagement im Internet“, Diplomarbeit, Technische Universität München, 2002.

5.1.2 ARTIKEL/STUDIEN/ZEITSCHRIFTEN

[AberdeenGroup, 2002]
AberdeenGroup, „Federated Identity Systems“, Boston, 2002
(http://www.sun.com/software/sunone/wp-federatedid.pdf [5. Mai 2007]).

[ARGE Daten, 2007]
ARGE Daten, „Analyse des Geschäftsprozesses Onlinebanking in Hinblick auf optimale, sichere und praxistaugliche Umsetzung für Konsumenten“, Wien, 2007.
(http://www.bmsk.gv.at/cms/site/attachments/4/0/7/CH0036/CMS1170676287948/online-banking-onlineversion.pdf [5. Mai 2007]).

[AMA, 2001]
American Management Association, „Workplace Monitoring & Surveillance: Policies and Practices“, Summary of Key Findings, 2001
(http://www.amanet.org/research/pdfs/emsfu_short.pdf [29. Juni 2007]).

[A-Sit, 2004]
Austria – Zentrum für sichere Informationstechnologie (A-Sit), „Leitfaden Biometrie – Überblick und Stand der Technik“, Wien, 2004
(http://www.a-sit.at/pdfs/Leitfaden_Biometrie.pdf [5. Mai 2007]).

[Atzinger et al., 2002]
Atzinger Markus, Brückner Christian, Müller Stefan, Schnier Torsten, „Gläserner Surfer – Anonym durchs Netz“, Seminararbeit, Fachhochschule Brandenburg, 2002.

[Bacher, 2004]
Bacher, „Intrusion Detection & Prevention“, Wien, 2004
(http://www.bacher.at/download/loesungen/bacher.at_intrusion-detection-&-prevention.pdf [5. Mai 2007]).

[Berger, Bitkom, 2007]
Berger, Bitkom, „Zukunft digitale Wirtschaft“, Studie, Berlin, 2007.

[Bitkom, 2006-1]
Bitkom, „Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk“, Version 2.0, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. und Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik, Berlin, Juni 2006.

[Bitkom, 2006-2]
Bitkom, „Wissensmanagement 2006-2010 Positionen und Trends“, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. und Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik, Berlin, 2006
(http://www.bitkom.org/files/documents/WM_2006-2010_-_Positionen__Trends(1).pdf [2. Mai 2007]).

[Bitkom, 2007]
Bitkom, „Wichtige Trends im Wissensmanagement 2007 bis 2011“, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. und Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik, Berlin, 2007.

[BMI, 2004-1]
Bundesministerium für Inneres (BMI), „Spezifikation Portalverbundprotokoll“, Wien, 2004
(http://reference.e-government.gv.at/Q-PV_PVP___pvp_1_8_9_-_Version.533.0.html [13. August 2007]).

[BMI, 2004-2]
Bundesministerium für Inneres (BMI), „Verarbeitung von Namensräumen und Cookies beim Umschreiben von URLs“, Wien, 2004
(http://reference.e-government.gv.at/Veroeffentlichte_Entwuerfe.579.0.html [23. November 2007]).

[BMI, 2005-1]
Bundesministerium für Inneres (BMI), „Der neue Reisepass. Die Entwicklung des neuen österreichischen Reisepasses mit biometrischen Daten.“, Wien, 2005
(http://www.bmi.gv.at/oeffentlsicherheit/2005/09_10/BIOMETRIE.pdf [5. Mai 2007]).

[BMI, 2005-2]
Bundesministerium für Inneres (BMI), „Portalverbund Whitepaper“, Wien, 2005
(http://portal.bmi.gv.at/ref/downloads/PVWhitepaper.pdf [7. August 2007]).

[BMI, 2006-1]
Bundesministerium für Inneres (BMI), „Datensicherheitsmaßnahmen für Web-Anwendungen“, Wien, 2006
(http://reference.e-government.gv.at/Q-PV_Datensicherheit___02_11_2.678.0.html [7. August 2007]).

[BMI, 2006-2]
Bundesministerium für Inneres (BMI), „Spezifikation LDAP-gv.at 2.3“, Konvention, Wien, 2006
(http://reference.e-government.gv.at/VD___LDAP-gv_at_2_3_0___Teil_1.777.0.html [5. September 2007]).

[BMI, 2006-3]
Bundesministerium für Inneres (BMI), „Rechtliche und organisatorische Aspekte des Portalverbunds“, Präsentationsunterlagen, Wien, 2006.

[BMI, 2007-1]
Bundesministerium für Inneres (BMI), „Ebenen- und Bereichskennungen für das Verwaltungskennzeichen bzw. Organisationskennzeichen“, Wien, 2007
(http://www.ref.gv.at/VKZ-Bereichskennungen.673.0.html [14. August 2007]).

[BMI, 2007-2]
Bundesministerium für Inneres (BMI), „Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen“, Wien, 2007
(http://reference.e-government.gv.at/Sicherheitsklassen_-_SecClass.1040.0.html [24. August 2007]).

[BMI, 2007-3]
Bundesministerium für Inneres (BMI), „Revisionsabfrage im Portalverbund“, Wien 2007
(http://reference.e-government.gv.at/Veroeffentlichte_Entwuerfe.579.0.html [24. November 2007]).

[BMI, 2007-4]
Bundesministerium für Inneres (BMI), „Revisionsleitfaden Portalverbund“, Wien 2007
(http://reference.e-government.gv.at/Veroeffentlichte_Entwuerfe.579.0.html [24. November 2007]).

[BMI, 2007-5]
Bundesministerium für Inneres (BMI), „Spezifikation Sicherheitsklassen“, Wien 2007
(http://reference.e-government.gv.at/Veroeffentlichte_Entwuerfe.579.0.html [9. Jänner 2008]).

[Böhme, 2005]
Böhme Rainer, „IT-Risiken im Schadenversicherungsmodell: Implikationen der Marktstruktur“, Technische Universität Dresden, 2005 (http://web.inf.tu-dresden.de/~rb21/publications/Boehme2005_IT-Versicherungen.pdf [5. Mai 2005]).

[Brodil, 2004]
Brodil Wolfgang, „Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis“, in ZAS (Zeitschrift für Arbeitsrecht und Sozialrecht), Wien, Juli 2004.

[BSI, 2003]
Bundesamt für Sicherheit in der Informationstechnik (BSI), „Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte“, Bonn, 2003 (http://www.bsi.de/literat/doc/drahtloskom/drahtloskom.pdf [5. Mai 2007]).

[BSI, 2005-1]
Bundesamt für Sicherheit in der Informationstechnik (BSI), „Antispam-Strategien Unerwünschte E-Mails erkennen und abwehren“, Bonn, März 2005 (http://www.bsi.de/literat/studien/antispam/antispam.pdf [5. Mai 2007]).

[BSI, 2005-2]
Bundesamt für Sicherheit in der Informationstechnik (BSI), „ITIL und Informationssicherheit Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management“, Bonn, 2005 (http://www.bsi.bund.de/literat/studien/ITinf/itil.pdf [5. Mai 2007]).

[BSI, 2006-1]
Bundesamt für Sicherheit in der Informationstechnik (BSI), „Grundlagen der elektronischen Signatur Recht Technik Anwendung“, Bonn, 2006 (http://www.bsi.de/esig/esig.pdf [5. Mai 2007]).

[BSI, 2006-2]
Bundesamt für Sicherheit in der Informationstechnik (BSI), „Zehn Thesen für eine datenschutzfreundliche Informationstechnik“, Bonn, Dezember 2006 (http://www.bfdi.bund.de/cln_030/nn_533554/SharedDocs/Publikationen/ZehnTesenF_C3_BCrEineDatenschutzfInformationstechnik.html [1. Juli 2007]).

[CA-1, 2005]
CA, „eTrust Identity and Access Management-Lösungen“, White Paper, November 2005.

[CA-2, 2005]
CA, „Identity Federation“, White Paper, Juni 2005.

[Cas, Peissl, 2000]
Cas Johann, Peissl Walter, „Beeinträchtigung der Privatsphäre in Österreich“, Bestandsaufnahme, Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, Wien, Oktober 2000.

[Cas, Peissl, 2002]
Cas Johann, Peissl Walter, „Datenvermeidung in der Praxis – individuelle und gesellschaftliche Verantwortung“, Endbericht, Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, Wien, August 2002.

[c’t, 2006-1]
c’t (Sixtus Mario), „Jenseits von gut und böse“ in 10/2006.

[c’t, 2006-2]
c’t (Heidrich Joerg), „Ausgeplaudert und ausgewertet“ in 7/2006.

[c’t, 2006-3]
c’t (Bleich Holger, Zota Volker), „Verfolgerwahn – Wie Online-Nutzer die Kontrolle über ihre Daten zurückgewinnen können“ in 24/2006.

[c’t, 2006-4]
c’t (Störing Marc), „Im Visier der Strafverfolger – Staatlicher Zugriff auf Anonymisierungsserver“ in 24/2006.

[c’t, 2007]
c’t (Braun Herbert, Bager Jo), „Heimliche Akten – Gefahren und Chancen der Cookie-Alternativen“ in 6/2007.

[c’t, 2008]
c’t (Wartmann Tim), „Risiko 2.0 – Eine Analyse der Sicherheit von Ajax“ in 2/2008.

[Deron, 2007]
Deron, „Identity Management Studie 2006/2007“, Studie, Stuttgart, 2007.

[Dohr, Weiss, Pollirer, 2006]
Dohr Walter, Weiss Ernst, Pollirer Hans-Jürgen, „Kommentar Datenschutzrecht“, 2. Auflage/5. Ergänzungslieferung, Wien, Mai 2006.

[Doubleslash, 2006]
Doubleslash, „Identity & Access Management – Funktionsbeschreibung eines Identity & Access Managements“, Version 1.0, Friedrichshafen, 10. Mai 2006 (http://www.doubleslash.de/de/Download/IAM_Funktionsbeschreibung.pdf [14. November 2007]).

[Drecker, Pohlmann, 2006]
Drecker Thomas, Pohlmann Norbert, „Datenübertragung im Automobil – mit Bluetooth und sicher?“, Gelsenkirchen, 2006 (https://www.internet-sicherheit.de/fileadmin/npo/artikel_berichte/ITS-1-06-Bluetooth.pdf Jänner 2006 [27. März 2007]).

[EPTA, 2006]
European Parliamentary Technology Assessment, „ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries“, Final Report, Oktober 2006.

[EU, 2006]
Europäische Union - Information Society and Media Directorate-General, „A roadmap for eID for the Implementation of the eGovernment Action Plan“, 2006 (http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_table.pdf).

[Evidian, 2005]
Evidian/Gartner, „Leveraging Identity & Access Management for enterprise productivity, agility and security, with quick ROI“, 2005 (http://www.evidian.com/iamnow/wp-iamnow.php [5. Mai 2007]).

[Evidian, 2007]
Evidian, „The 7 most used authentication methods“, White Paper, Les Clayes-sous-Bois (FR), 2007.

[Feiler, 2006]
Feiler Lukas, „Threat Update: Social Engineering“, 2006 (http://www.e-center.co.at/ecenter/threatupdate/Social_Engineering.pdf Seite 1 [7. März 2007]).

[Forrester, 2006]
Forrester, „The Forrester Wave: Enterprise Antispyware, Q1 2006“, Cambridge, 2006 (http://www.forrester.com/ [27. Feber 2007]).

[Fraunhofer, 2003]
Fraunhofer-Institut für Arbeitswirtschaft und Organisation, „Was ist ein Portal? Definition und Einsatz von Unternehmensportalen“, Whitepaper, Stuttgart, 2003 (http://www.gurzki.de/publications/padem/Was%20ist%20ein%20Portal/ [3. September 2007]).

[Gartner, 2006]
Gartner Research, “The Do’s and Don’t’s of Identity and Access Management”, Stamfort, April 2006.

[Gerstbach, Tomek, 2003]
Gerstbach Peter, Tomek Andreas, „Trusted Computing“, Wien 2003 (http://www.uniprojekt.org/tc/trusted_computing.pdf „Trusted Computing“[5. Mai 2007]).

[GI, 2007]
Deutsche Gesellschaft für Informatik, „Memorandum zur Identifizierung und Überwachung von Bürgern“, Bonn, Juli 2007.

[GPA, 2006]
Gewerkschaft der Privatangestellten, „Rächer der enterbten Daten – Technische Überwachung von Beschäftigten bei der Internet- und E-Mail-Nutzung“, Broschüre, Wien, 2006.

[Hall, Barbeau, Kranakis, 2005]
Hall Jeyanthi, Barbeau Michel, Kranakis Evangelos, „Radio Frequency Fingerprinting for Intrusion Detection in Wireless Networks“, Carleton University, 2005 (http://www.scs.carleton.ca/~jhall2/Publications/IEEETDSC.pdf [2. Mai 2007]).

[Hansen, 2003]
Hansen Marit, Henry Krasemann Henry, Rost Martin, Genghini Riccardo, „Datenschutzaspekte von Identitätsmanagementsystemen“, aus Datenschutz und Datensicherheit 27, 2003 (https://www.datenschutzzentrum.de/projekte/idmanage/DUD-27-9.pdf [17. Juni 2007]).

[Hansen-2, 2006]
Hansen Walter, „Digital Rights Management“, Vortragsunterlagen, Westfälische Wilhelms-Universität Münster, 2006

[Intel, 2002]
Intel, „Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper“, Juni 2002 (http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf [5. Mai 2007]).

[IT-Research, 2003]
IT-Research, „eProvisioning & Identity Management – Business Value, Markt & Anbieter“, Sauerlach, August 2003.

[IT-Research, 2005]
IT-Research, „Our Digital Identity“, White Paper, Sauerlach, Feber 2005.

[Jendricke, 2004]
Jendricke Uwe, Gerd tom Markotten Daniela, „Identitätsmanagement: Einheiten und Systemarchitektur“, Universität Freiburg, 2004.

[known_sense, 2006]
known_sense, „Entsicherung am Arbeitsplatz“, Köln/München, 2006 (http://www.known-sense.de/entsicherung/securitystudie_auszug_50dpi.pdf [5. Mai 2007]).

[Köhntopp, 2000]
Köhntopp Marit, „Identitätsmanagement – Anforderungen aus Nutzersicht“ in: Bäumler, H.; Breinlinger A.; Schrader, H.-J. (Hrsg.): Datenschutz von A-Z, Luchterhand, Neuwied, 2000 (http://www.datensicherheit.nrw.de/Daten/ws991122/koehntopp.pdf [8. Mai 2007], http://www.ldi.nrw.de/pressestelle/download/10vortrag-koehntopp.pdf [12. Mai 2007]).

[Köhntopp, Pfitzmann, 2001]
Köhntopp Marit, Pfitzmann Andreas, „Informationelle Selbstbestimmung durch Identitätsmanagement“, Unabhängiges Landeszentrum für Datenschutz, TU Dresden, 2001 (http://dud.inf.tu-dresden.de/literatur/KoePf_01ittiIdmanage_kurz.pdf [31. Mai 2007]).

[Kotschy, Reimer, 2004]
Kotschy Waltraud, Reimer Sebastian, „Die Überwachung der Internet-Kommunikation am Arbeitsplatz“, in ZAS (Zeitschrift für Arbeitsrecht und Sozialrecht), Juli 2004.

[Kraft, 2006]
Kraft Thomas, „Der neue §107 TKG – Verbesserter Schutz vor unerbetenen Werbemails?“ in ecolex 03/2006 ecolex, Zeitschrift, 03/2006.

[KCP, 2004]
Kuppinger Cole + Partner, „Flexible Geschäftsprozesse brauchen integrierte Identitäten“, White Paper, München, 2004.

[KCP, 2007]
Kuppinger Cole + Partner, „IAM Vision 2010 – Identity as a Service“, Trend Report, München, Juli 2007.

[Landesk, 2005]
Landesk, „Sicherheitsmanagement in modernen IT-Netzwerken“, München, 2005 (http://www.landesk.de/docs/whitepapers/Sicherheitsmanagement.pdf [27. Feber 2007]).

[Löser, 2007]
Löser C., „Schutz der Privatsphäre und Kernbereich privater Lebensgestaltung“, Universität Greifswald, 2007 (http://www.cloeser.org/ext/Schutz%20der%20Privatsph%E4re.pdf [31. Mai 2007]).

[McAfee, 2007]
McAfee, „McAfee Report Projects Wave of International Cyber Crime“, November 2007 (http://www.crn.com/security/204301389 [11. März 2008])

[MERLINnovations, 2007]
MERLINnovations, „SecLookOn – Beschreibung des Verfahrens und Lösung für Man-in-the-Middle Attacken“, Wien, 2007 (http://www.seclookon.com/seclookon/SecLookOn-MitM-Attacke.pdf [5. Mai 2007]).

[Messagelabs, 2007]
Messagelabs, **MessageLabs Intelligence: 2007 Annual Security Report“**, Feber 2008 (http://www.messagelabs.com/intelligence.aspx [11. März 2008])

[Parycek, 2007]
Parycek Peter, „Gläserne Bürger – transparenter Staat? Risiken und Reformpotenziale des öffentlichen Sektors in der Wissensgesellschaft“, Bericht, Institut für Technikfolgenabschätzung der Österreichischen Akademie der Wissenschaften, Wien, Mai 2007.

[Pfitzmann, Hansen, 2005]
Pfitzmann Andreas, Hansen Marit, „Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology“, Unabhängiges Landeszentrum für Datenschutz, TU Dresden, 2005.

[Posch, 2002]
Posch Katharina, „Neue Medien im Lichte des Arbeitsrechts“
(http://www.it-law.at/uploads/tx_publications/Posch_Vortrag.pdf [5. Mai 2007]).

[Reiter, Rubin, 1997]
Reiter Michael K., Rubin Aviel D., „Crowds: Anonymity for Web Transactions“, AT&T Labs|Research, 1997 (http://avirubin.com/crowds.pdf [3. Juli 2007]).

[Rolf, 2003]
Rolf Arno, „Informationstechnologien in Organisationen und Gesellschaft. Die Veränderungen von Arbeitsabläufen anhand von Beispielen“, 2003 (http://www.bpb.de/files/VB7NOV.pdf [2. Mai 2007]).

[SAP, 2005]
SAP, „Mobile Supply Chain Management“, Walldorf, 2005
(http://www.sap.com/solutions/business-suite/scm/pdf/SB_Mobile_SCM.pdf Juni 2006 [5. Mai 2007]).

[Scheer, 2007]
Scheer Magazin, „Die Arbeit der Zukunft“, IDS Scheer AG, Jänner 2007.

[Sonnenreich, 2002]
Sonnenreich Wes, „Return On Security Investment (ROSI): A Practical Quantitative Model, New York, 2002
(http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf [5. Mai 2007]).

[Sommer, Vlastos, 2004]
Sommer Gottfried, Vlastos Michael, „Betriebsrat – Personalvertretung Rechte und Pflichten“, Wien, 2004 (http://www.voegb.at/bildungsangebote/skripten/ar/AR-19.pdf [5. Mai 2007]).

[Stiller-Erdpresser, 2005]
Stiller-Erdpresser Elisabeth, „Single Sign On – Secure Access“, Präsentationsunterlagen, Wien, 2005 (http://www.conect.at/files/papers/20050531/Stiller-Erdpresser.pdf [12. Mai 2007]).

[Symantec, 2006-1]
Symantec, „Symantec Internet Security Threat Report Trends for January 06–June 06“, Volume X, Cupertino, September 2006
(http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport [5. Mai 2007]).

[Symantec, 2006-2]
Symantec, „Symantec Internet Security Threat Report Trends for July–December 06“, Volume XI, Cupertino, März 2007
(http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport [5. Mai 2007]).

[Symantec, 2007]
Symantec, „Symantec Internet Security Threat Report Trends for January 07–June 07“, Volume XII, Cupertino, September 2007
(http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport [11. März 2008]).

[Sun, 2006]
Sun Microsystems, „Vernetztes Identity Management: Sicherheit für große Outsourcing-Projekte“, White Paper, Santa Clara, November 2006.

[TA-Swiss, 2003]
TA-Swiss Zentrum für Technologiefolgen-Abschätzung, „Das Vorsorgeprinzip in der Informationsgesellschaft“, Studie, Bern, 2003.

[Tallo, 2007]
Tallo Ivar, „Creating single governance space: e-gov lessons from Estonia“, Vortrag, E-Government-Konferenz, Krems, 2007
(http://e-government.adv.at/2007/pdf//Tallo_Estonia_20070524.pdf [9. Juni 2007]).

[Teuteberg, Hilker, Kurbel, 2003]
Teuteberg Frank, Hilker Jens, Kurbel Karl, „Anwendungsschwerpunkte im Mobile Enterprise Ressource Planning“, Frankfurt, 2003
(http://www.vg-u.de/wi-www/download/MC_Papers/teu_hil_kur_marcneu.pdf [5. Mai 2007]).

[Tonninger, 2005]
Tonninger Bernhard, „IT-Security & das Gesetz“, Seminarunterlagen, it-versity, Wien, 24.8.2005.

[ULD, 2005]
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (kurz: ULD), „privacy4DRM Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management“, Studie, Ilmenau und Kiel, Mai 2005.

[Wirtz, Burda, Beaujean, 2006]
Wirtz Bernd W., Burda Hubert, Beaujean Rainer, „Deutschland Online 3 – Die Zukunft des Breitband-Internets“, Darmstadt/München, Jänner 2006
(http://www.studie-deutschland-online.de/do3/studie_do3.pdf [2. Mai 2007]).

5.2 ONLINE

[A]
https://www.a-i3.org/ [8. März 2007] Selbstbeschreibung: „Die Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3) ist eine unabhängige, interdisziplinäre Organisation, die sich den Identitätsschutz im Internet zur Aufgabe gemacht hat.“
http://www.ajax-community.de/ [21. Feber 2008] Online-Forum zum Thema AJAX, betrieben von Schönmann IT Services & Consulting.
http://www.amanet.org/ [29. Juni 2007] Selbstbeschreibung: „American Management Association (kurz: AMA) provides professional development and performance-based learning solutions.“
http://www.amazon.com/ [2. Juni 2007] Webseite (Portal) des Unternehmens Amazon.com Inc.
http://www.americanexpress.com/ [26. Juni 2007] Webseite des Finanzinstituts American Express Company.
http://www.ammering.org/ [2. Juni 2007] Selbstbeschreibung: „Eine private, politisch unabhängige Webseite mit dem Ziel, dem Leser die Aspekte des Datenschutzes allgemein und im Zusammenhang mit der elektronischen Datenverarbeitung im besonderen näher zu bringen.“

http://www.ams.or.at/neu/ [28. Juni 2007] Webseite des Arbeitsmarktservice Österreich.

http://www.anon.gildemax.de/ [25. Feber 2008] Webseite über Anonymität, betrieben von Gildemax (Pseudonym).

http://www.anonymitaet.com/anonymisierer/index.html [3. Juli 2007] Die Kanzlei Krasemann (http://www.kanzlei-krasemann.de/) beschäftigt sich im Schwerpunkt mit den Bereichen Datenschutzrecht/Internetrech/Domainrecht/Telekommunikationsrecht/Medienrecht. Dazu gehört insbesondere auch das neue Gebiet des Rechts der virtuellen Welten bzw. das Onlinespielrecht.

http://www.antiphishing.org/ [27. Feber 2008] Selbstbeschreibung: „The Anti-Phishing Working Group is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types."

http://www.antispywarecoalition.org/ [27. Feber 2008] Selbstbeschreibung: „The Anti-Spyware Coalition (kurz: ASC) is a group dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies."

http://www.antyspyware.pl/ [21. Feber 2008] Webseite des Antispyware-Zentrum Polens, betrieben von Dagma Sp. z o.o.

http://www.aol.com/ [21. Feber 2008] Webseite des Internetunternehmens AOL aus dem Verbund von Time Warner.

http://www.apache.org/ [27. Feber 2008] Selbstbeschreibung: „The Apache Software Foundation provides support for the Apache community of open-source software projects. The Apache projects are characterized by a collaborative, consensus based development process, an open and pragmatic software license, and a desire to create high quality software that leads the way in its field. We consider ourselves not simply a group of projects sharing a server, but rather a community of developers and users."

http://www.apple.com/ [26. Juni 2007] Webseite des IT-Konzerns Apple Inc.

http://www.ard.de/ [2. Juni 2007] Webseite des deutschen Südwestrundfunks (Anstalt des öffentlichen Rechts).

http://www.argedaten.at/ [21. Feber 2008] Selbstbeschreibung: „Die ARGE DATEN beschäftigt sich seit 1983 intensiv mit Fragen des Informationsrechts, des Datenschutzes, der Telekommunikation und des Einsatzes neuer Techniken. Der Verein ist parteipolitisch unabhängig und seine Tätigkeit ist nicht auf Gewinn gerichtet. Er verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne § 35 Abs. 2 BAO überwiegend im Inland."

http://www.a-sit.at/ [21. Feber 2008] und http://www.buergerkarte.at/ [21. Feber 2008] Webseite des Zentrums für sichere Informationstechnologie – Austria.

http://www.atkearney.de/ [21. Feber 2008] Webseite des Beratungsunternehmens A.T. Kearney GmbH.

http://www.a-trust.at/ [21. Jänner 2008] Webseite der A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.

[B]

http://www.ba-ca.com/ [21. Feber 2008] Webseite des Kreditinstituts Bank Austria Creditanstalt AG.

http://www.bacher.at/ [27. Feber 2008] Webseite des österreichischen IT-Unternehmens Bacher Systems EDV GmbH.

http://www.balancedscorecard.org/ [21. Feber 2008] Selbstbeschreibung: „The Balanced Scorecard Institute, a Strategy Management Group company, provides training and consulting services to commercial, government, and non-profit organizations in applying best practices in balanced scorecard (kurz: BSC), strategic performance management and measurement, and transformation and change management."

http://www.bandit-project.org/ [21. Feber 2008] Selbstbeschreibung: „Bandit is a set of loosely-coupled components that provide consistent identity services for Authentication, Authorization, and Auditing. The Bandit project creates a community that organizes and standardizes identity-related technologies in an open way, promoting both interoperability and collaboration."

http://www.basel-ii.info/ [21. Feber 2008] Webseite zu „Basel II", betrieben von Corporate-Consulting.Network.

http://www.bdu.de/ [7. Juli 2007] Webseite des Bundesverbandes Deutscher Unternehmensberater BDU e.V.

http://www.bfdi.bund.de/ [21. Feber 2008] Webseite des Deutschen Bundesbeauftragten für Datenschutz und Informationsfreiheit.

http://www.bigstring.com/ [3. Juli 2007] Selbstbeschreibung: „BigString Corporation has created a revolutionary new email service that allows users to control their sent email. The Company's BigString product is an email service for both individuals and businesses that is recallable and changeable. With a patent pending technology, BigString allows a user to easily send, recall, erase, self-destruct and modify an email after it has been sent. BigString users have unprecedented control over all of their email, whether they choose to send it through the BigString.com website or an email client such as Outlook."

http://www.bis.org/ [21. Feber 2008] Selbstbeschreibung: „The Bank for International Settlements (kurz: BIS) is an international organisation which fosters international monetary and financial cooperation and serves as a bank for central banks."

http://www.bundeskanzleramt.at/ [21. Feber 2008] Webseite des Österreichischen Bundeskanzleramtes.

http://www.ag.bka.gv.at/ [21. Feber 2008] Wiki des Österreichischen Bundeskanzleramts.

http://www.digitales.oesterreich.gv.at/ [22. Feber 2008] Webseite zum Thema E-Government des österreichischen Bundeskanzleramts.

http://www.help.gv.at/ [25. Feber 2008] Selbstbeschreibung: „HELP ist eine behördenübergreifende Plattform im Internet, die Sie – ausgehend von konkreten Lebenssituationen, wie etwa Schwangerschaft, Geburt, Heirat oder Wohnen – über Amtswege in Österreich informiert und teilweise deren elektronische Erledigung zulässt. HELP versteht sich als Drehscheibe zwischen Behörden und Bürgern und Bürgerinnen wobei Kriterien wie Transparenz, Übersichtlichkeit, Verständlichkeit und die Konzentration auf das Wesentliche im Vordergrund stehen.“, betrieben vom Österreichischen Bundeskanzleramt.

http://www.ris.bka.gv.at/ [17. Juni 2007] Webseite für Rechtsinformation des Österreichischen Bundeskanzleramts.

http://www.blackhat.com/ [27. Feber 2007] Selbstbeschreibung: „The Black Hat Briefings are a series of highly technical information security conferences that bring together thought leaders from all facets of the infosec world – from the corporate and government sectors to academic and even underground researchers. The environment is strictly vendor-neutral and focused on the sharing of practical insights and timely, actionable knowledge. Black Hat remains the best and biggest event of its kind, unique in its ability to define tomorrow’s information security landscape.“

http://www.blogger.com/ [10. Juni 2007] Ein Unternehmen der Google Inc.

http://www.bmbf.de/ [21. Feber 2008] Webseite des Deutschen Bundesministeriums für Bildung und Forschung.

http://www.bmi.bund.de/ [10. Juni 2007] Webseite des Deutschen Bundesministeriums für Inneres.

http://www.bmi.gv.at/ [21. Feber 2008] Webseite des Österreichischen Bundesministeriums für Inneres.

http://zmr.bmi.gv.at/ [17. Juni 2007] Webseite für das Zentrale Melderegister des Österreichischen Bundesministeriums für Inneres.

http://www.bmsg.gv.at/ [21. Feber 2008] Webseite des Österreichischen Bundesministeriums für Soziales und Konsumentenschutz.

http://www.bmw.com/ [14. Feber 2008] Webseite des Autoherstellers BMW AG.

http://www.brain-pro.de/ [21. Feber 2008] ehemalige Webseite des Sicherheitsberatungsunternehmens Marko Rogge; aktuelle Webseite: http://www.marko-rooge.de/ [21. Feber 2008].

http://www.bris.ac.uk/ [21. Feber 2008] Webseite der britischen Universität Bristol.

http://www.browzar.com/ [7. Feber 2008] Webseite des Softwareunternehmens Browzar Limited.

http://www.brz.gv.at/ [27. Feber 2008] Webseite des Österreichischen Bundesrechenzentrums.

http://www.bsi.de/ [2. Juni 2007] Webseite des Deutschen Bundesamts für Sicherheit in der Informationstechnik.

http://malware.bul-online.de/ [21. Feber 2008] Webseite über Malware, betrieben von Lutz Kleimann.

http://www.bull.at/ [21. Feber 2008] Webseite des IT-Lösungsanbieters Bull GmbH.

http://www.bundesgerichtshof.de/ [21. Juni 2007] Webseite des Deutschen Bundesgerichtshofs.

http://www.bundeskriminalamt.de/ [27. Feber 2008] Webseite des Deutschen Bundeskriminalamts.

http://www.bundestrojaner.de/ [21. Juni 2007] Selbstbeschreibung: „Das Portal Bundestrojaner.de hat es sich zur Aufgabe gemacht über die Geschehnisse rund um den Trojaner zur informieren, den die Regierung einsetzen will, um verdeckte Online-Durchsuchungen durchführen zu können."

http://www.businessportal24.com/ [21. Feber 2008] Webseite (Portal) für internationale Pressemitteilungen, betrieben von ANCOSO Business Technologies AG.

https://www.bwin.com/ [18. Feber 2008] Webseite (Portal) des Onlinewettanbieters bwin International Ltd.

[C]

http://www.ca.com/ [27. Feber 2008] Webseite des IT-Unternehmens CA.

http://www.cacert.org/ [21. Feber 2008] Selbstbeschreibung: „CAcert.org is a community driven, Certificate Authority that issues certificates to the public at large for free. CAcert's goal is to promote awareness and education on computer security through the use of encryption, specifically with the X.509 family of standards. We have compiled a document base that has helpful hints and tips on setting up encryption with common software, and general information about Public Key Infrastructures."

http://www.capurro.de/ [21. Feber 2008] Webseite des Philosophen Rafael Capurro.

http://www.ccc.de/ [27. Juni 2007] Webseite des Chaos Computer Club.

http://www.centennial-software.com/ [21. Feber 2008] Webseite des Softwareunternehmens Centennial Software.

http://www.cert.org/ [21. Feber 2008] Selbstbeschreibung: „The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Morris worm incident, which brought 10 percent of internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency charged the Software Engineering Institute with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. This center was named the CERT Coordination Center. While we continue to respond to major security incidents and analyze product vulnerabilities, our role has expanded over the years. Along with the rapid increase in the size of the internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers. To better manage these changes, the CERT/CC is now part of the larger CERT Program, which develops and promotes the use of

appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services."

http://www.cgisecurity.com/ [21. Feber 2008] Webseite der IT-Informationssicherheitsplattform CGI Security.

http://www.chipkarte.at/ [21. Feber 2008] Webseite mit Informationen zur österreichischen e-Card, betrieben von der Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H. – SVC, einer Tochter des Hauptverbands der österreichischen Sozialversicherungsträger.

http://www.chkrootkit.org/ [27. Feber 2008] Webseite zum Download des Tools chkrootkit zum Aufspüren von Rootkits.

http://www.cio.de/ [21. Feber 2008] Webseite fokussiert auf Informationen für IT-Manager, betrieben von IDG Business Media GmbH (IDG Group).

http://www.cio.gv.at/ [1. Juli 2007] Webseite des Österreichischen Bundeskanzleramts für E-Government.

http://reference.e-government.gv.at/ [21. Feber 2008] Webseite mit Informationen im Bereich E-Government für Bund, Länder und Gemeinden, betrieben vom Amt der Steiermärkischen Landesregierung.

http://www.cisco.com/ [21. Feber 2008] Webseite des IT-Konzerns Cisco Systems, Inc.

http://www.citibank.de/ [21. Feber 2008] Webseite des Kreditinstituts Citibank Privatkunden AG & Co. KGaA.

http://www.citrix.de/ [26. Feber 2008] Webseite des IT-Unternehmens Citrix Systems GmbH.

http://www.clearsightnet.com/ [27. Feber 2008] Selbstbeschreibung: „ClearSight is a leading provider of network monitoring and analysis tools for real-time application troubleshooting. It is the only company that identifies network problems at the application layer, enabling IT administrators to easily and immediately visualize and pinpoint the source of network problems, leading to faster resolution that ensures business continuity."

http://www.commercemanager.de/ und http://www.securitymanager.de/ [21. Feber 2008] Webseiten zu E-Commerce und Informationssicherheit, betrieben von FEiG & PARTNER.

http://www.competence-site.de/ [25. Feber 2008] Selbstbeschreibung: Competence Site ist eine der führenden Kompetenzplattformen für Manager, Fachexperten, Nachwuchskräfte und ihre Dienstleister im Internet. Die Plattform bietet vorselektiertes und strukturiertes Wissen aus den Bereichen Management, IT, Recht, den Erfahrungsaustausch mit Top-Experten aus Wissenschaft und Unternehmenspraxis, ein hochkarätiges Netzwerk sowie Marktplätze zur Anbahnung von Geschäftskontakten.

http://www.compliancemagazin.de/ [21. Feber 2008] Webseite zu IT-Compliance und IT-Governance, betrieben von PMK Presse, Messe & Kongresse Verlags GmbH.

http://www.computacenter.de/ [21. Feber 2008] Webseite des IT-Lösungsanbieters Computacenter AG & Co. OHG.

http://www.computer.org/ [26. Juni 2007] Webseite der IEEE Inc.

http://www.computerbetrug.de/ [21. Feber 2008] Webseite mit Informationen zu Computerbetrug, betrieben von Heiko Rittelmeier und Sascha Borowski.

http://www.computerforensik.org/ [27. Feber 2007] Online-Forum zum Thema Computerforensik, betrieben von Holger Morgenstern.

http://www.computerwelt.at/ [20. Jänner 2008] Webseite mit Neuigkeiten im IT-Bereich, betrieben von Info Technologie Verlag GmbH.

http://www.computerwoche.de/ [21. Feber 2008] Webseite mit Neuigkeiten im IT-Bereich, betrieben von IDG Business Media GmbH (IDG Group).

http://www.computerworld.com/ [21. Feber 2008] oder http://utilitycomputing.itworld.com/ [23. Feber 2008] Selbstbeschreibung: „Computerworld, the 'Voice of IT Management,' is the most trusted source for the critical information needs of senior IT management at medium-size to large companies. It has earned this reputation by maintaining its focus on IT management for thirty-seven years, despite the never-ending changes in the technology landscape. Computerworld covers news from the IT manager's perspective with a broad analytical view of how that news affects the daily operations of large technology enterprises.“, betrieben von der IDG Group.

http://www.comscore.com/ [23. Jänner 2008] Selbstbeschreibung: „comScore, Inc. ist a Global Internet Information Provider. comScore maintains massive proprietary databases that provide a continuous, real-time measurement of the myriad ways in which the Internet is used and the wide variety of activities that are occurring online. Mission-critical information relating to both offline and online activities is collected through comScore's innovative use of the Internet as a timely and powerful data collection medium.“

http://www.consumeraffairs.com/ [21. Feber 2008] Webseite zum Konsumentenschutz, betrieben von ConsumerAffairs.Com Inc.

http://www.consumerreports.org/ [21. Feber 2008] Selbstbeschreibung: „Consumer Reports and ConsumerReports.org are published by Consumers Union, an expert, independent nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. To achieve this mission, we test, inform, and protect. To maintain our independence and impartiality, CU accepts no outside advertising, no free test samples, and has no agenda other than the interests of consumers. CU supports itself through the sale of our information products and services, individual contributions, and a few noncommercial grants.“

http://www.contentmanager.de/ [21. Feber 2008] Webseite mit den Schwerpunkten Content Management und Einsatz moderner Web-Lösungen, betrieben von der Agentur FEiG & PARTNER.

http://www.cookiecooker.de/ [3. Juli 2007] Webseite des IT-Sicherheitsexperten Oliver Berthold.

http://www.copyright.gov/ [27. Juni 2007] Webseite des U.S. Copyright Offices.

http://www.corporate-governance.at/ [2. Juni 2007] Webseite des Österreichischen Arbeitskreises für Corporate Governance.

http://xml.coverpages.org/cpex.html [21. Feber 2008] Selbstbeschreibung: „The Cover Pages is a comprehensive, online reference collection supporting the XML family of markup language standards, XML vocabularies, and related structured information standards. Edited by Robin Cover since 1986, this public access knowledgebase promotes and enables the use of open, interoperable, standards-based solutions which protect digital information and enhance the quality of data processing."

http://www.cryptoshop.com/ [21. Feber 2008] Webseite des Consultingunternehmens CRYPTAS it-Security GmbH AUSTRIA.

http://www.csoonline.com/ [10. Juni 2007] Webseite des Medienunternehmens CXO Media Inc., einem Unternehmen der IDG Group.

http://www.cutecircuit.com/ [21. Feber 2008] Selbstbeschreibung: „CuteCircuit is a Technology company that creates design excellence and beauty in the fields of Wearable Technology and Interaction Design."

http://www.cyberstalking.at/ [21. Feber 2008] Webseite zum Thema Cyberstalking, betrieben von Cornelia Belik.

[D]

http://www.datenschutz-berlin.de/ [17. Juni 2007] Webseite des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

http://www.datenschutzzentrum.de/ [22. Feber 2008] und http://www.uld-i.de/ [22. Feber 2008] oder http://www.datenschutz.de/ [24. Feber 2008] Webseite des Landesbeauftragten für den Datenschutz Schleswig-Holstein.

http://www.deloitte.com/ [11. März 2008] Webseite des Consulting-Unternehmens Deloitte Touche Tohmatsu.

http://www.dhs.gov/ [24. Feber 2008] Selbstbeschreibung: „The National Strategy for Homeland Security and the Homeland Security Act of 2002 served to mobilize and organize our nation to secure the homeland from terrorist attacks. This exceedingly complex mission requires a focused effort from our entire society if we are to be successful. To this end, one primary reason for the establishment of the Department of Homeland Security was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our nation. In order to better do this and to provide guidance to the 180,000 DHS men and women who work every day on this important task, the Department developed its own high-level strategic plan. The vision and mission statements, strategic goals and objectives provide the framework guiding the actions that make up the daily operations of the department."

http://www.dialogdata.com/ [22. Feber 2008] Webseite des IT-Anbieters Dialog Data Betriebsberatungs- und Datenverarbeitungsgesellschaft mbH.

http://www.diepresse.at/ [18. Feber 2008] Webseite der Tageszeitung Die Presse Verlagsgesellschaft mbH & Co KG.

http://www.digitalidworld.com/ [2. Juni 2007] Selbstbeschreibung: „Digital Identity World is the hub of the digital identity industry, providing comprehensive news, exclusive interviews, market statistics and expert commentary on the people, companies, products and events shaping the digital identity space. Digital Identity World is dedicated to providing only the highest quality online industry resources, newsletters and community building conferences, events and tradeshows."

http://www.digital-rights-management.de/ [27. Juni 2007] Webseite der DRM-Experten Buhse, Becker, Günnewig.

http://www.doubleslash.de/ [24. Feber 2008] Webseite des deutschen Softwareunternehmens doubleSlash Net-Business GmbH mit Fokus auf Identity Management.

http://www.dsk.gv.at/ [23. Feber 2008] Webseite der Österreichischen Datenschutzkommission.

[E]

http://www.ebay.com/ [18. Feber 2008] Selbstbeschreibung: „eBay is The World's Online Marketplace, enabling trade on a local, national and international basis. With a diverse and passionate community of individuals and small businesses, eBay offers an online platform where millions of items are traded each day."

http://www.e-center.co.at/ [22. Feber 2008] Webseite des Zentrums für e-commerce und internetrecht (kurz: e-center), eine Organisationseinrichtung der Juranovit ForschungsGmbH.

http://www.echelonwatch.org/ [28. Feber 2008] Selbstbeschreibung: „This site is designed to encourage public discussion of this potential threat to civil liberties, and to urge the governments of the world to protect our rights", betrieben von Free Congress Foundation, the Electronic Privacy Information Center, Cyber-Rights and Cyber-Liberties (UK) and the Omega Foundation.

http://www.eclipse.org/ [22. Feber 2008] Webseite zum Open Source Projekts „Eclipse", betrieben von der Eclipse Foundation.

http://www.e-democracy.org/ [21. Feber 2008] Selbstbeschreibung: "Expanded participation and stronger democracies and communities through the power of information and communication technologies and strategies.", betrieben von E-Democracy.Org.

http://www.eff.org/ [4. Feber 2008] Selbstbeschreibung: „From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our freedoms in the networked world come under attack, the Electronic Frontier Foundation (kurz: EFF) is the first line of defense. EFF broke new ground when it was founded in 1990 and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today.

From the beginning, EFF has championed the public interest in every critical battle affecting digital rights.“

http://www.elektronik-kompendium.de/ [22. Feber 2008] Webseite zur Erklärung von Elektronik, betrieben von Patrick Schnabel.

http://www.emailprivacy.info/ [24. Feber 2008] Selbstbeschreibung: EmailPrivacy.info investigates the risks of compromising your email privacy and security and offers you the ways of reducing these risks to a minimum.“, betrieben von Glastonberry Inc.

http://www.enfsi.org/ [27. Feber 2007], jetzt http://www.enfsi.eu/ [24. Feber 2008] Selbstbeschreibung: „ENFSI is the European Network of Forensic Science Institutes. ENFSI has been established with the purpose of sharing knowledge, exchanging experiences and coming to mutual agreements in the field of forensic science. The aim of ENFSI is to ensure that the quality of development and delivery of forensic science throughout Europe is at the forefront of the world.“

http://www.entrust.com/ [24. Feber 2008] Webseite des IT-Security Beratungsunternehmens Entrust mit Fokus auf „Securing Digital Identities“.

http://www.epic.org/ [21. Juni 2007] Selbstbeschreibung: „EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.“

http://www.eptanetwork.org/EPTA/ [10. Juni 2007] Selbstbeschreibung: „The EPTA Partners advise parliaments on the possible social, economic and environmental impact of new sciences and technologies. The common aim is to provide impartial and high quality accounts and reports of developments in issues such as bioethics and biotechnology, public health, environment and energy, ICTs, and R&D policy.“

http://www.ethereal.com/ [16. Feber 2008] Webseite des Netzwerkanalyse-Tools Ethereal, betrieben von Ethereal, Inc.

http://www.8-eu-richtlinie.de/ [24. Feber 2008] Webseite mit Informationen zur 8. EU-Richtlinie, betrieben von CONSUVATION GmbH.

http://www.europol.europa.eu/ [4. Feber 2008] Selbstbeschreibung: „Europol is the European Law Enforcement Organisation which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international organised crime.“

http://conventions.coe.int/ [24. Feber 2008] Webseite des Europarates.

http://ec.europa.eu/ [5. Mai 2007] Webseite der Europäischen Union (kurz: EU).

http://cordis.europa.eu/ [24. Feber 2008] Selbstbeschreibung: „CORDIS, der Forschungs- und Entwicklungsinformationsdienst der Gemeinschaft, der über die neuesten Ereignisse im Bereich Wissenschaft, Forschung und Entwicklung berichtet, ist die offizielle Informationsstelle für Ausschreibungen unter dem Siebten Rahmenprogramm (RP7). Der Dienst bringt Forscher, politische

Entscheidungsträger, Manager und Schlüsselakteure im Bereich Forschung anhand seiner interaktiven Webseiten zusammen.“

http://www.fidis.net/ [24. Feber 2008] Selbstbeschreibung: „FIDIS is a Network of Excellence supported by the European Union under the 6th Framework Programme for Research and Technological Development within the Information Society Technologies (kurz: IST) priority in the Action Line: "Towards a global dependability and security framework. The European Information Society (kurz: EIS) requires technologies which address trust and security yet also preserve the privacy of individuals. As the EIS develops, the increasingly digital representation of personal characteristics changes our ways of identifying individuals, and supplementary digital identities, so-called virtual identities, embodying concepts such as pseudonymity and anonymity, are being created for security, profit, convenience or even for fun. These new identities are feeding back into the world of social and business affairs, offering a mix of plural identities and challenging traditional notions of identity. At the same time, European states manage identities in very different ways. For example, in Germany holding an ID card is mandatory for every adult, while in the UK state-issued ID cards do not exist. FIDIS objectives are shaping the requirements for the future management of identity in the EIS and contributing to the technologies and infrastructures needed.“

http://www.prime-project.eu.org/ [5. Mai 2007] Webseite des „Privacy and Identity Management for Europe“-Projekts der EU.

http://swami.jrc.es/ [10. Juni 2007] Webseite der EU betreffend „Information/Society/Technologies“.

http://eur-lex.europa.eu/ [24. Feber 2008] Selbstbeschreibung: „EUR-Lex bietet einen unmittelbaren und kostenlosen Zugang zu den Rechtsvorschriften der Europäischen Union. Über das System können das Amtsblatt der Europäischen Union sowie insbesondere die Verträge, die Rechtsetzungsakte, die Rechtsprechung und die vorbereitenden Rechtsakte konsultiert werden.“

http://www.evidian.com/ [24. Feber 2008] Webseite des Lösungsanbieters Evidian für Identity- und Access-Management.

http://www.eweek.com/ [24. Feber 2008] Webseite des IT-Medienunternehmens Ziff Davis Enterprise Holdings Inc.

http://www.exine.de/netlife/e-democracy.htm [24. Feber 2008] Webseite über E-Democracy, betrieben von der Exine.de.

http://www.export.gov/ [24. Feber 2008] Selbstbeschreibung: „Export.gov brings together resources from across the U.S. Government to assist American businesses in planning their international sales strategies and succeed in todays global marketplace. From market research and trade leads from the U.S. Department of Commerce’s Commercial Service to export finance information from Export-Import Bank and the Small Business Administration to agricultural export assistance from USDA, Export.gov helps American exporters navigate the international sales process and avoid pitfalls such as non-payment and intellectual property misappropriation. Export.gov is one of the Presidential E-

Government initiatives created to provide better customer service for businesses interacting with the Federal Government.“

[F]

http://www.facebook.com/ [22. Feber 2008] Selbstbeschreibung: „Facebook is a social utility that connects people with friends and others who work, study and live around them. People use Facebook to keep up with friends, upload an unlimited number of photos, share links and videos, and learn more about the people they meet.“

http://www.fbi.gov/ [24. Feber 2008] Selbstbeschreibung: „FBI.gov is an official site of the U.S. Federal Government, U.S. Department of Justice.“

http://www.fh-wedel.de/ [25. Feber 2008] Webseite der deutschen Fachhochschule Wedel.

http://www.fittkaumaass.de/ [18. Feber 2008] Webseite des Beratungsunternehmens Fittkau & Maaß Consulting GmbH.

http://www.flickr.com/ [18. Feber 2008] Webseite (Online-Fotoplattform) von Yahoo!

http://www.fortinet.com/ [25. Feber 2008] Webseite des IT-Sicherheitshardwareherstellers Fortinet, Inc.

http://www.fraunhofer.de/ [24. Feber 2008] Webseite der Fraunhofer-Gesellschaft. Die Gesellschaft ist eine Organisation für angewandte Forschung in Europa. Sie betreibt anwendungsorientierte Forschung zum direkten Nutzen für Unternehmen und zum Vorteil der Gesellschaft.

http://www.iao.fraunhofer.de/ [26. Feber 2008] Webseite des Instituts für Arbeitswirtschaft und Organisation der Fraunhofer-Gesellschaft.

http://freenetproject.org/ [3. Juli 2007] Selbstbeschreibung: „Freenet is free software which lets you publish and obtain information on the Internet without fear of censorship. To achieve this freedom, the network is entirely decentralized and publishers and consumers of information are anonymous. Without anonymity there can never be true freedom of speech, and without decentralization the network will be vulnerable to attack.“

http://www.fsa.gov.uk/ [25. Feber 2008] Selbstbeschreibung: „The Financial Services Authority (kurz: FSA) is an independent non-governmental body, given statutory powers by the Financial Services and Markets Act 2000. We are a company limited by guarantee and financed by the financial services industry.“

http://www.futurefoundation.net/ [25. Feber 2008] Webseite des Beratungsunternehmens Future Foundation.

[G]

http://www.gartner.com/ [25. Feber 2008] Webseite des Beratungsunternehmens und Marktanalysten Gartner, Inc.

http://www.genericiam.org/ [20. Feber 2008] Webseite zu generischen Prozessen von Identity Management, betrieben von doubleSlash Net-Business GmbH.

http://www.gewerbeverein.at/ [25. Feber 2008] Webseite des Österreichischen Gewerbevereins.

http://www.gi-ev.de/ [25. Feber 2008] Webseite der Deutschen Gesellschaft für Informatik.

http://www.golem.de/ [25. Feber 2008] Selbstbeschreibung: „Als tagesaktuelle Publikation berichtet Golem.de aus den Bereichen Soft- und Hardware, Internet, Telekommunikation, Entertainment und dem allgemeinen Branchengeschehen.“, betrieben von Klaß & Ihlenfeld Verlag GmbH.

http://www.google.com/ [10. Juni 2007] Webseite des IT-Konzerns Google Inc.

http://guetezeichen.at/ [1. Juli 2007] Webseite des Vereins zur Förderung der kundenfreundlichen Nutzung des Internets Euro-Label – Das Europäische E-Commerce-Gütezeichen.

[H]

http://www.hacktivismo.com/ [3. Juli 2007] Selbstbeschreibung: „Hacktivismo is an international group of hackers, human rights workers, lawyers and artists that evolved out of The Cult of the Dead Cow (kurz: cDc), a publishing and computer security group. We believe that privacy and access to information are basic human rights. Hacktivismo assumes as an ethical point of departure the principles enshrined in the Universal Declaration on Human Rights and the International Convention on Civil and Political Rights. We also support the Free Software and open-source movements.“

http://www.harvard.de/ [10. Juni 2007] Webseite des deutschen PR-Unternehmens Harvard Public Relations GmbH.

http://www.health-first.org/ [25. Feber 2008] Webseite des Krankenhausbetreibers Health First.

http://www.heise.de/ [25. Feber 2008] Webseite des Medienunternehmens Heise Zeitschriften Verlag GmbH & Co. KG.

http://www.hipaa.org/ [25. Feber 2008] Webseite zu HIPPA, betrieben von CMS.

http://www.howstuffworks.com/ [25. Feber 2008] Selbstbeschreibung: „HowStuffWorks, a wholly owned subsidiary of Discovery Communications, is the award-winning source of credible, unbiased, and easy-to-understand explanations of how the world actually works. From car engines to search engines, from cell phones to stem cells, and thousands of subjects in between, HowStuffWorks has it covered. No topic is too big or too small for our expert editorial staff to unmask ... or for you to understand. In addition to comprehensive articles, our helpful graphics and informative videos walk you through every topic clearly, simply and objectively. Our premise is simple: Demystify the world and do it in a simple, clear-cut way that anyone can understand.“, betrieben von HowStuffWorks, Inc.

http://www.hp.com/ [24. Feber 2008] Webseite des IT-Konzerns HP.

[I]

http://www.iam-wiki.org/ [24. Feber 2008] Webseite zum Identity and Access Management. Die Inhalte stammen aus den Erkenntnissen vieler Kundenprojekte und einer ständigen Marktbeobachtung. Experten, Analysten und Hersteller von Identity Management-Lösungen sind aufgerufen Inhalte zu dieser Website beizusteuern.

http://www.ibm.com/ [22. Feber 2008] Webseite des IT-Konzerns IBM.

http://www.icann.org/ [21. Juni 2007] Selbstbeschreibung: „As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. ICANN, a public benefit, non-profit entity, is the international organization responsible for the management and oversight of the coordination of the Internets domain name system and its unique identifiers.“

http://www.idc.com/ [27. Feber 2007] Selbstbeschreibung: „IDC is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy.“

http://www.identityblog.com/ [22. Feber 2008] Selbstbeschreibung: „This blog is about building a multi-centered system of digital identity that its users control. All kinds of things pass themselves off as “digital identity”, so I want to start by pruning enough trees that we can see a forest.“, betrieben vom Identityexperten Kim Cameron.

http://www.identitytheft.org/ [10. Juni 2007] Diese Seite wird federführend von (einem ehemaligen Opfer eines Identitätsdiebstahls) Mari J. Frank serviciert. Sie enthält mehr als 70 Seiten Information über Identitätsdiebstahlvorbeugung und -gegenmaßnahmen.

http://www.identix.ch/ [24. Feber 2008] oder http://www.idematrix.com/ [24. Feber 2008] Webseiten für Biometrie Identity Management des Lösungsanbieters idematrix GmbH.

http://www.idg.net/ [27. Feber 2008] Webseite der IDG Group – siehe http://www.tecchannel.de/, http://www.cio.de/, http://www.computerwoche.de/, http://www.computerworld.com/, http://www.csoonline.com/ und http://www.pcwelt.de/.

http://www.idnwebshield.com/ [27. Feber 2007] Webseite mit einer Security-Lösung für Aktivitäten des Browsers, betrieben vom österreichischen Software-Techniker Thomas Meike.

http://standards.ieee.org/ [27. Feber 2008] Webseite des gemeinnützigen technischen Berufsverbands zur Normung von Techniken, Hardware und Software mit folgender Selbstbeschreibung: „The world's leading professional association for the advancement of technology.“

http://www.ietf.org/ [22. Feber 2008] Webseite der Internet Engineering Task Force (kurz: IETF), welche zur Internet Society (kurz: ISOC) gehört. Selbstbeschreibung: „The Internet Society (kurz: ISOC) is a not-for-profit organization founded in 1992 to provide leadership in Internet related

standards, education, and policy. ISOC is supported by more than 90 organizational members and 26.000 individual members.“

http://www.ifm.eng.cam.ac.uk/ [22. Feber 2008] Webseite der Abteilung für Engineering der Universität Cambridge.

http://www.ikarus-software.at/ [24. Feber 2008] Webseite des österreichischen Anbieters für „Antivirus und Content Security“ IKARUS Security Software GmbH.

http://www.infineon.com/tpm [22. Feber 2008] Webseite des Halbleiterherstellers Infineon Technologies AG mit Fokus auf TPM.

http://www.info-rfid.de/technologie/25.html [22. Feber 2008] Selbstbeschreibung: „Das Informationsforum RFID ist ein eingetragener Verein mit Sitz in Berlin. Mitglieder sind weltweit führende Unternehmen aus den Bereichen Handel, Konsumgüterindustrie, Automobilbranche, IT und Dienstleistung. Gemeinsam wollen sie die zukunftsweisenden Möglichkeiten der Radiofrequenz-Identifikation nutzen und der Diskussion um ihre Anwendung neue Impulse geben.“

http://www.informationelle-selbstbestimmung.com/ [22. Feber 2008] Webseite über das Grundrecht der informationellen Selbstbestimmung, betrieben vom Juristen Jens Ferner.

http://www.informationelle-selbstbestimmung-im-internet.de/ [22. Feber 2008] Webseite über informationelle Selbstbestimmung im Internet mit Firefox, NoScript, JAP/JonDo, Tor, GPG/PGP und Mixminion, betrieben von Jens Lechtenbörger.

http://www.informationweek.de/ [22. Feber 2008] Webseite des praxisbezogenen Online-Magazins für IT-Manager, betrieben von InformationWeek CMP-WEKA GmbH & Co. KG.

http://www.infoworld.com/ [27. Feber 2008] Selbstbeschreibung: „InfoWorld is a leading publisher of technology information and product reviews on topics including viruses, phishing, worms, firewalls, security, servers, storage, networking, wireless, databases, and web services.“, betrieben von der IDG Group.

http://www.innovation-aktuell.de/ [24. Feber 2008] Webseite über Innovationen für Produkte, Prozesse und Dienstleistungen, betrieben von Symposion Publishing GmbH.

http://www.innovations-report.de/ [22. Feber 2008] Forum für Wissenschaft, Industrie und Wirtschaft zur Förderung der Innovationsdynamik und Vernetzung von Innovations- und Leistungspotenzialen.

http://insecure.org/nmap/ [21. Feber 2008] Webseite zum Download von Internet Tools wie beispielsweise „Nmap“, betrieben von Gordon Lyon (Pseudonym: Fyodor).

http://www.integral.co.at/ [18. Feber 2008] Webseite der INTEGRAL Markt- und Meinungsforschung GesmbH.

http://www.intel.com/ [15. Jänner 2008] Webseite des Chipherstellers Intel Corp.

http://www.internet4jurists.at/ [21. Feber 2008] Selbstbeschreibung: „Neben der Vermittlung technischer Grundkenntnisse und der rechtlichen Vorschriften für das Internet werden Gesetzgebung und Judikatur im Zusammenhang mit dem Internet einer kritischen Betrachtung unter besonderer

Berücksichtigung der Grund- und Freiheitsrechte unterzogen. Ziel ist die Schaffung von rechtlichen Lösungen, die den Besonderheiten des Internets gerecht werden, und die Förderung der Rechtssicherheit der neuen Medien.“, betrieben von Franz Schmidbauer.

http://www.internetnews.com/ [24. Feber 2008] Webseite mit Neuigkeiten im Bereich Internet, betrieben von Jupitermedia Corporate.

http://www.internet-sicherheit.de/ [5. Mai 2007] Webseite des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen.

http://www.internetworldstats.com/stats.htm [18. Feber 2008] Selbstbeschreibung: „An International website featuring up to date world Internet Usage, Population Statistics and Internet Market Research Data, for over 233 individual countries and world regions.“

http://www.interpol.int/ [24. Feber 2008] Webseite der internationalen kriminalpolizeilichen Organisation INTERPOL.

http://www.irnis.net/ [24. Feber 2008] Webseite zum Download von Tools für den Sicherheitsbereich, betrieben von irnis.

http://www.isaca.org/ [24. Feber 2007] Selbstbeschreibung :“Der ISACA-Verband ist ein globaler Schrittmacher in der Verwaltung, Steuerung und Sicherung unter den Informationssystems-Auditoren. Die Standards des Verbandes bei der Prüfung und Steuerung von Informationssystemen werden weltweit praktiziert. Die Zertifizierung als Certified Information Systems Auditor (kurz: CISA) genießt weltweite Anerkennung und wurde bisher von über 50.000 Mitarbeitern der Branche erworben. Das neue Zertifizierungsprogramm als Certified Information Systems Manager (kurz: CISM) konzentriert sich speziell auf die Zielgruppe von Führungskräften in der IS-Sicherungssparte. Der Verband veröffentlicht das Information Systems Control Journal und veranstaltet eine Reihe internationaler Tagungen, die sich sowohl auf technische als auch auf einschlägig verwaltungsorientierte Themen der Sparten IS-Prüfung, -Steuerung und -Sicherung, sowie auf deren Verwaltung konzentrieren.“

http://www.iso.org/ [14. Feber 2008] Selbstbeschreibung: „ISO is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 157 countries, one member per country, with a Central Secretariat in Geneva, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.“

http://www.isode.com/ [23. Feber 2008] Webseite des Softwareherstellers Isode mit Fokus auf Messaging- and Directory-Server-Produkte.

http://www.iss.net/ [23. Feber 2008] Webseite des Securityproduktherstellers ISS.

http://istrg.som.surrey.ac.uk/ [5. Feber 2008] Webseite der Information Societies Research Group.

http://www.itil.org/de/ [11. Feber 2008] Webseite zum Thema ITIL, betrieben von Glenfis AG.

http://www.it-innovations.de/ [22. Feber 2008] Webseite des IT-Dienstleisters (Netzwerk, Business Intelligence) it innovations.

http://www.itirol.at/ [28. Feber 2008] Selbstbeschreibung: „Die vorliegende Website ist ein Online-Angebot der Firma trans IT Entwicklungs- und Transfercenter Universität Innsbruck GmbH, getragen von der Universität Innsbruck, der Tiroler Zukunftsstiftung und dem Management Center Innsbruck. Unter dieser Web-Adresse und allfälliger Subdomains werden umfangreiche Informations- und Online-Dienste zu Produkten und Leistungen unseres Unternehmens bereit gestellt. Die Informationsplattform iTirol informiert Wirtschaftstreibende und Wissenschaftler der Region über aktuelle Entwicklungen im Bereich Informations- und Kommunikationstechnologien."

http://www.itsmf.de/ [21. Feber 2008] Selbstbeschreibung: „Das 1991 in England gegründete Information Technology Service Management Forum (kurz: itSMF) ist die weltweit einzige unabhängige und international anerkannte Organisation für IT Service Management. itSMF Deutschland e.V. bietet eine Plattform zum Wissens- und Erfahrungsaustausch für Einzelpersonen, Unternehmen, Hersteller und Gesellschaften in Deutschland."

http://www.itsolution.at/ [23. Feber 2008] Webseite des österreichischen Unternehmens IT-Solution mit Schwerpunkt Elektronische Signatur.

http://www.itu.int/ [23. Feber 2008] Selbstbeschreibung: „ITU is the leading United Nations agency for information and communication technologies. As the global focal point for governments and the private sector, ITU's role in helping the world communicate spans 3 core sectors: radiocommunication, standardization and development. ITU also organizes TELECOM events and was the lead organizing agency of the World Summit on the Information Society."

http://www.itwissen.info/ [20. Feber 2008] Webseite (Online-Lexikon) für Informationstechnologie, betrieben von DATACOM Buchverlag GmbH.

http://us.ixquick.com/deu/ [23. Feber 2008] Selbstbeschreibung: „Ixquick is a powerful metasearch engine, which unlike single search engines, such as Google and Ask Jeeves, among others, simultaneously searches multiple Internet databases, gathering and displaying comprehensive and accurate Web results to Internet users. Founded in New York and launched on the Web in 1998, Ixquick is owned by Surfboard Holding BV, a Dutch company."

[J]

http://www.jajah.com/ [18. Feber 2008] Webseite (Telefonservice) der JAJAH Inc.

http://jcmc.indiana.edu/ [10. Juni 2007] Selbstbeschreibung: „The Journal of Computer-Mediated Communication (kurz: JCMC) is a web-based, peer-reviewed scholarly journal. Its focus is social

science research on computer-mediated communication via the Internet, the World Wide Web, and wireless technologies. Within that general purview, the journal is broadly interdisciplinary, publishing work by scholars in communication, business, education, political science, sociology, media studies, information science, and other disciplines. Acceptable formats for submission include original research articles, meta-analyses of prior research, synthesizing literature surveys, and proposals for special issues.“

http://www.jeckle.de/ [25. Feber 2008] Webseite zu XML und Semantic Web, betrieben von Mario Jeckle.

http://johnny.ihackstuff.com/ghdb.php [25. Feber 2008] Selbstbeschreibung: „Welcome to the Google Hacking Database (kurz: GHDB)! We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe! Stop by our forums to see where the magic happens!“

http://www.jondos.de/ [24. Feber 2008] Webseite des Anonymisierungsdienteanbieters JonDos GmbH.

[K]

http://www.kaspersky.com/ [22. Feber 2008] und http://www.viruslist.com/ [22. Feber 2008] Webseiten des Informationssicherheitsspezialisten Kaspersky Lab.

http://www.kes.info/ [25. Feber 2008] Webseite zur Zeitschrift für Informationssicherheit, betrieben von SecuMedia Verlags-GmbH.

http://hash_funktion.know-library.net/ [21. Feber 2008] Selbstbeschreibung: „Diese universelle freie Wissensdatenbank sammelt Wissen zu allen möglichen Themen mit dem Ziel das Wissen der Welt zu jedem Fach in einfach lesbaren und verständlichen Form zusammen zu fassen und darzustellen. Mit dem direkten Querverweis zu jedem Thema im Form eines Suchformulars stellt diese elektronische Bibliothek ein großes Nachschlagewerk mit vielen Hunderttausenden Definitionen und Beschreibungen zur Verfügung. Die Inhalte unterliegen der GNU- Lizenz für freie Dokumentation.“

http://www.known-sense.de/ [25. Feber 2008] Webseite des deutschen PR- und Marketingunternehmens known_sense.

http://www.kpmg.at/ [25. Feber 2008] Webseite des Beratungsunternehmens KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft.

http://www.kuppingercole.de/ [25. Feber 2008] Webseite der Analystengruppe Kuppinger & Cole mit Schwerpunkt auf Identitätsmanagement.

http://www.kurier.at/ [25. Feber 2008] Webseite der Tageszeitung KURIER, betrieben von Telekurier Online Medien GmbH & CoKG.

[L]

http://www.landesk.de/ [10. Juni 2007] Webseite des Softwareunternehmens LANDesk.

http://www.lanline.de/ [25. Feber2008] Webseite des Medienunternehmens Konradin IT-Verlag GmbH.

http://www.lavasoft.de/ [25. Feber 2008] Webseite des Informationssicherheitssoftwareherstellers Lavasoft.

http://www.lawrence.edu/ [10. Juni 2007] Webseite der US-Universität Lawrence.

http://ldap.gv.at/ [25. Feber 2008] Webseite mit Adress- und Organisationsverzeichnis der österreichischen Verwaltung.

http://www.lexikon-suchmaschinenoptimierung.de/ [24. Feber 2008] Selbstbeschreibung: „Das Lexikon Suchmaschinenoptimierung ist ein Glossar für Fachbegriffe rund um das Thema Suchmaschinenoptimierung bzw. Search Engine Optimization (kurz: SEO). Es ist ein unkompliziertes Nachschlagewerk für alle, die Webseiten für Suchmaschinen optimieren oder sich über Suchmaschinenoptimierung als Marketing-Instrument informieren wollen. Das Ziel des Lexikons ist, jeden Begriff aus dem Bereich der Suchmaschinenoptimierung zu erfassen und dessen Bedeutung zu erklären. Das Lexikon wird daher ständig erweitert und aktualisiert. Derzeit umfasst das Lexikon 372 Begriffe und Definitionen rund um die Optimierung von Webseiten für Suchmaschinen."

http://www.lfd.niedersachsen.de/ [28. Juni 2007] Webseite des Landesbeauftragten für den Datenschutz Niedersachsen (Deutschland).

[M]

http://www.marketagent.com/ [25. Feber 2008] Webseite zur Online Markt- und Meinungsforschung, betrieben von Marketagent.com online reSEARCH GmbH.

http://www.maroki.de/ [25. Feber 2008] Webseite mit Publikationen zum Thema Datenschutz und Privacy, betrieben von Martin Rost.

http://www.marshal.com/ [11. März 2008] Webseite des Security-Spezialisten (Internet Content, E-Mail) Marshal Limited.

http://www.mcafee.com/ [25. Feber 2008] Webseite des Informationssicherheitssoftwareherstellers McAfee, Inc.

http://www.merlinnovations.com/ [25. Feber 2008] Selbstbeschreibung: „Wir sind ein auf IT-Sicherheit spezialisiertes Unternehmen mit Sitz in Wien. Unser wichtigstes Produkt ist SecLookOn - eine einzigartige graphische Authentifizierungs- und Autorisierungssoftware, die Ihnen höchste Sicherheit bei einfacher Handhabung ohne Eingabe einer PIN (Personal Identification Number) bietet.", betrieben von MERLINnovations Consulting GmbH.

http://www.messagelabs.com/ [25. Feber 2008] Webseite des Managed Service-Anbieters MessageLabs Ltd.

http://www.microsoft.com/ [5. Mai 2007] Webseite des IT-Konzerns Microsoft.

http://at.msn.com/ [25. Feber 2008] Webseite (Portal) von Microsoft.

http://cardspace.netfx3.com/ [28. Oktober 2007] und http://netfx3.com/content/WindowsCardspaceHome.aspx [25. Feber 2008] Webseite zu Windows CardSpace.

http://www.live.com/ [25. Feber 2008] Webseite (Portal), Suchfunktion von Microsoft.

https://accountservices.passport.net/ [21. Feber 2008] Webseite von Microsoft zur Anmeldung für das Service Live ID.

http://www.sysinternals.com/ [23. Feber 2008] Webseite zum Download von System-Tools, betrieben von Microsoft.

http://www.sicher-im-internet.at/ [22. Feber 2008] Webseite der österreichischen Initiative „Sicher im Internet“, betrieben von Microsoft Österreich GmbH.

http://www.mitlinx.de/ [25. Feber 2008] Webseite des Webdesignspezialisten MitLinX Internetdienstleistungen.

http://www.mobilkom.at/ [24. Feber 2008] Webseite des Mobilfunkunternehmens mobilkom.

http://www.monitor.co.at/ [25. Feber 2008] Webseite des Magazins Monitor, betrieben von Bohmann Druck und Verlag Gesellschaft m.b.H. & Co. KG.

http://www.mozilla.com/firefox/ [25. Feber 2008] Webseite des Softwareherstellers Mozilla zum Download des Produkts „Firefox“.

http://www.mtv.com/ [23. Feber 2008] Webseite des Medienunternehmens MTV Networks.

http://www.myspace.com/ [18. Feber 2008] Webseite (Portal) von MySpace Inc.

[N]

http://www.napster.com/ [18. Feber 2008] Webseite (Online-Musikplattform) der Napster Inc.

http://www.nasdaq.com/ [23. Feber 2008] Webseite der Börse NASDAQ Stock Market, Inc.

http://www.nessus.org/ [25. Feber 2008] Webseite des Netzwerkanalysetools-Produzenten Tenable Network Security.

http://www.nethics.net/ [24. Feber 2008] Webseite über Informationsethik, betrieben vom Verein nethics.net.

http://netmesh.info/ [25. Feber 2008] Selbstbeschreibung: „This blog is about the emerging Situational Software paradigm, which will make mobile software truly valuable to business and non-business users alike. The Situational Software paradigm will carry mobile software into the mass market, and create substantial new business opportunities for technology providers, content providers, operators, device manufacturers and companies engaged in many kinds of e-business.“, betrieben von NetMesh Inc., a trademark of R-Objects Inc.

http://www.netstumbler.com/ [25. Feber 2008] Selbstbeschreibung: „The Home of the award winning wireless networking tool and the best source for your daily Wi-Fi, WiMAX, 3G, and VoIP news.“, betrieben von NetStumbler.com.

http://www.networkgeneral.com/ [25. Feber 2008] übernommen von NetScout

http://www.netscout.com/ [25. Feber 2008] Webseite des IT-Security-Spezialisten NetScout Systems, Inc.

http://netzpolitik.org/ [25. Feber 2008] Selbstbeschreibung: „netzpolitik.org ist ein Weblog über die Themen der Informationsgesellschaft. netzpolitik.org ist nicht neutral, sondern steht klar auf der Seite der Open Source-Revolution und setzt sich für mehr Bürgerrechte im digitalen Zeitalter ein.“, betrieben von Markus Beckedahl.

http://www.newscorp.com/ [23. Feber 2008] Webseite des Medienkonzerns news corporation.

http://www.nextiraone.de/ [25. Feber 2008] Webseite des Kommunikationsdienstleisters NextiraOne.

http://www.nia.din.de/ [25. Feber 2008] Selbstbeschreibung: „Der Normenausschuss Informationstechnik und Anwendungen (kurz: NIA) ist als Teil des DIN Deutsches Institut für Normung e.V. das offizielle nationale Gremium für Normung und Standardisierung in der Informationstechnik und in ausgewählten Anwendungsbereichen der Informationstechnik.“

http://www.nic.at/ [25. Juni 2007] Webseite der nic.at Internet Verwaltungs- und Betriebs GesmbH mit Unternehmensgegenstand: Vergabe und Verwaltung von .at, .co.at und .or.at Domains.

http://www.nifis.de/ [23. Feber 2008] Selbstbeschreibung: „Die Nationale Initiative für Informations- und Internet-Sicherheit (kurz: NIFIS) ist die Selbsthilfeorganisation der Wirtschaft, um Unternehmen im Kampf gegen die wachsenden Gefahren aus dem Internet technisch, organisatorisch und rechtlich zu stärken. Ziel ist, die Vertraulichkeit, Verfügbarkeit und Integrität von Daten in digitalen Netzwerken zu fördern und sicherzustellen. Zur Erfüllung dieser Aufgabe wird NIFIS Konzepte für den Schutz vor Angriffen aus dem Datennetz entwickeln, in pragmatische Lösungen umsetzen und der Wirtschaft zur Verfügung stellen.“

http://www.nike.com/ [25. Feber 2008] Webseite des Sportartikelherstellers Nike Inc.

http://csrc.nist.gov/ [24. Feber 2008] Selbstbeschreibung: „The Computer Security Division (kurz: CSD) mission is to provide standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in IT systems.“

http://www.itl.nist.gov/ [24. Feber 2008] Selbstbeschreibung: „In todays' complex technology-driven world, the Information Technology Laboratory (kurz: ITL) has the broad mission of supporting U.S. industry, government, and academia by promoting U.S. innovation and industrial competitiveness through advancement of information technology measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.“

http://www.nordea.com/ [25. Feber 2008] Webseite des Finanzdienstleisters Nordea.

http://www.novell.com/ [25. Feber 2008] Webseite des Software-Konzerns Novell, Inc.

http://www.nytimes.com/ [22. Juni 2007] Webseite des Medienunternehmens The New York Times Company.

[O]

http://www.oasis-open.org/ [8. Juli 2007] Selbstbeschreibung: „OASIS (steht für: Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5.000 participants representing over 600 organizations and individual members in 100 countries. The Consortium hosts two of the most widely respected information portals on XML and Web services standards, Cover Pages and XML.org. OASIS Member Sections include CGM Open, IDtrust, LegalXML, and Open CSA.“

http://www.oeaw.ac.at/ [22. Feber 2008] Webseite der Österreichischen Akademie der Wissenschaften.

http://www.oenb.at/ [24. Feber 2008] Webseite der Österreichischen Nationalbank.

http://www.ogh.gv.at/ [11. Feber 2008] Webseite des Österreichischen Obersten Gerichtshofes.

http://www.oio.de/ [24. Feber 2008] Webseite des deutschen Softwareentwicklungs-Dienstleisters Orientation in Objects GmbH.

http://www.ojp.usdoj.gov/ [10. Juni 2007] Selbstbeschreibung: „Since 1984 the Office of Justice Programs has provided federal leadership in developing the nation's capacity to prevent and control crime, improve the criminal and juvenile justice systems, increase knowledge about crime and related issues, and assist crime victims. Through the programs developed and funded by its bureaus and offices, OJP works to form partnerships among federal, state, and local government officials to control drug abuse and trafficking; reduce and prevent crime; rehabilitate neighborhoods; improve the administration of justice in America; meet the needs of crime victims; and address problems such as gang violence, prison crowding, juvenile crime, and white-collar crime. The functions of each bureau or program office are interrelated.“

http://www.onforma.de/ [18. November 2007] Online-Forum für mobiles Arbeiten, betrieben von Cornelia Brandt.

http://www.onion-router.net/ [3. Juli 2007] Webseite des US Naval Research Labs der Information Technology Division des Center for High Assurance Computer Systems (Official U.S. Navy Web Site).

https://www.on-norm.at/ [15. Feber 2008] Webseite des Österreichischen Normungsinstituts bzw. dessen Tochter Austrian Standards plus GmbH.

http://openid.net/ [28. Feber 2008] Selbstbeschreibung: „OpenID is a free and easy way to use a single digital identity across the Internet. With one OpenID you can login to all your favorite websites and forget about online paperwork.“, betrieben von der OpenID Foundation.

http://pki.openca.org/ [21. Feber 2008] Selbstbeschreibung: „The OpenCA PKI Research Labs, born from the former OpenCA Project, is an open organization aimed to provide a framework for PKI studying and development of related projects.“

http://www.openldap.org/ [24. Feber 2008] Selbstbeschreibung: „The OpenLDAP Project is a collaborative effort to develop a robust, commercial-grade, fully featured, and open source LDAP suite of applications and development tools. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenLDAP Suite and its related documentation.“, betrieben von der OpenLDAP Foundation.

http://www.openliberty.org/ [24. Feber 2008] Selbstbeschreibung: „openLiberty is a community effort started by a handful of us with a common need for open source software to Liberty-enable relying parties in a SOA. The first deliverable we have agreed to is a Java library and reference implementation for what Liberty Alliance calls a Web Services Consumer.“

http://www.oracle.com/ [24. Feber 2008] Webseite des Datenbankherstellers Oracle.

https://www.orkut.com/ [24. Jänner 2008] Online-Community aus der Unternehmensgruppe Google Inc.

http://futurezone.orf.at/ [28. Juni 2007] Webseite des Österreichischen Rundfunks mit Fokus auf IKT-Themen.

http://mediaresearch.orf.at/ [18. Feber 2008] Webseite des Österreichischen Rundfunks mit Fokus auf Medienforschung.

http://oe1.orf.at/ [24. Feber 2008] Webseite des Österreichischen Rundfunks mit Fokus auf Kultur.

http://www.osa.org/ [22. Feber 2008] Selbstbeschreibung: „The mission of the Optical Society of America (kurz: OSA) is to promote the generation, application and archiving of knowledge in optics and photonics and to disseminate this knowledge worldwide. The purposes of the Society are scientific, technical and educational.“

http://www.output.at/ [24. Feber 2008] Webseite des IT-Magazins, betrieben von MBO Media Verlagsgesellschaft mbH.

[P]

http://www.pandasoftware.com/ [20. Feber 2008] Webseite des Malwareschutz-Herstellers Panda.

http://www.parlament.gv.at/ [26. Juni 2007] Webseite des Österreichischen Parlaments.

http://www.pctools.com/ [27. Feber 2008] Webseite zum Download von Tools für den PC.

http://www.pcwelt.de/ [24. Feber 2008] Webseite zu Computer und Technik, betrieben von IDG Magazine Media GmbH.

http://www.peterfmayer.at/ [25. Feber 2008] Webseite zu Infrastruktur und Technologie, betrieben von Telekom Presse Dr. Peter F. Mayer KG.

http://www.pharming.org/ [24. Feber 2008] Webseite mit Informationen zu Pharming.

http://www.phenoelit.net/ [27. März 2007] Seit Juni 2007 inaktiv mit Verweis auf Seite: http://www.phenoelit-us.org/ [24. Feber 2008] Selbstbeschreibung: „You are entering the lands of packets, brute force and misuse of trust. This is a dark land. Full of problems and choices. Be carefull when you use your knowledge. Be also carefull with your tools and weapons. Never underestimate your enemy.“

http://www.phoenix.com/ [24. Feber 2007] Webseite des IT-Sicherheitssoftwarespezialisten Phoenix Technologies LTD.

http://www.pingidentity.com/ [24. Feber 2008] Webseite des Single-Sign-On-Spezialisten Ping Identity Corporation.

http://www.pki-page.org/ [24. Feber 2008] Webseite mit Informationen über PKI und CA, betrieben von Secorvo Security Consulting.

http://www.politicsonline.com/ [18. Feber 2008] Selbstbeschreibung: „News, Tools & Strategies - the premiere company providing products and services to use the Internet in politics.”, betrieben von PoliticsOnline, Inc.

http://www.politik-digital.de/ [24. Feber 2008] Webseite des Vereins pol-di. Selbstbeschreibung: „pol-di.net ist eine Nichtregierungsorganisation neuer Ausprägung: Wir sind sowohl Anbieter marktorientierter Dienstleistungen als auch überparteilicher gemeinnütziger Akteur für glaubwürdigere politische Kommunikation im Internet.“

http://www.pressetext.at/ [22. Feber 2008] Webseite der pressetext Nachrichtenagentur GmbH.

http://preventingidentitythefttips.com/ [24. Feber 2008] Webseite über Identitätsdiebstahl, betrieben von Identity Theft Protection.

http://www.privacyinternational.org/ [10. Feber 2008] Selbstbeschreibung: „Privacy International is an independent, non-government organization with the primary role of advocacy and support. We have an international advisory board with members from over 30 countries, and a board of trustees who oversee our staff.“, betrieben von Privacy International London Headquarters.

http://www.projectliberty.org/ [5. Mai 2007] Webseite des Liberty Alliance-Projekts.

http://www.psychohelp.at/ [18. Feber 2008] Webseite zur psychologischen Online-Beratung, betrieben von Christiane Turnheim.

http://www.pwc.com/ [5. Mai 2007] Webseite des Beratungsunternehmens PricewaterhouseCoopers.

[Q]

http://www.quantenkryptographie.at/ [27. Feber 2008] und http://www.secoqc.net/ [27. Feber 2008] Webseiten zum Projekt „SECOQC - Development of a Global Network for Secure Communication based on Quantum Cryptography“, betrieben von Austrian Research Centers GmbH.

http://www.quantum.at/ [15. Feber 2008] Webseite des Instituts für Quantenoptik und Quanteninformation (kurz: IQOQI) der Universität Wien.

http://www.quintessenz.at/ [2. Juni 2007] Webseite des Vereins quintessenz – zur Wiederherstellung der Bürgerrechte im Informationszeitalter.

[R]

http://www.rechtsfreund.at/ [24. Feber 2008] Webseite zum Thema Recht, betrieben von Johannes Öhlböck.

http://www.reputationdefender.com/ [21. Feber 2008] Selbstbeschreibung: „ReputationDefender was created to defend you and your family's good name on the Internet. Our goal is straightforward: To search out all information about you and/or your child on the Internet, wherever it may be, and present it to you in a clear report. To destroy, at your command, all inaccurate, inappropriate, hurtful, and slanderous information about you and/or your child using our proprietary in-house methodology.“, betrieben von ReputationDefender, Inc.

http://www.rfid-journal.de/ [26. Feber 2008] Webseite zum Thema RFID, betrieben von Tim Kröner.

http://www.ripe.net/ [27. Feber 2008] Selbstbeschreibung: „The RIPE NCC is an independent, not-for-profit membership organisation that supports the infrastructure of the Internet through technical co-ordination in its service region. The most prominent activity of the RIPE NCC is to act as the Regional Internet Registry (kurz: RIR) providing global Internet resources and related services (IPv4, IPv6 and AS Number resources) to members in the RIPE NCC service region. The membership consists mainly of Internet Service Providers (ISPs), telecommunication organisations and large corporations located in Europe, the Middle East and parts of Central Asia.“

http://www.rolandberger.com/ [9. Feber 2008] Webseite des Beratungsunternehmens Roland Berger Strategy Consultants.

http://www.rsasecurity.com/ [7. Feber 2008] Webseite der Security Division von EMC².

http://www.rtr.at/ [8. Dezember 2006] Webseite der Österreichischen Rundfunk und Telekom Regulierungs-GmbH (kurz: RTR-GmbH).

[S]

http://www.sabre-labs.com/ [6. März 2007; 22. Feber 2008: Webseite nicht mehr verfügbar] Selbstbeschreibung: „SABRE Labs, the consulting arm of SABRE Security, specializes in reverse engineering, source code audits and on-demand R&D of industry grade security architectures & solutions. Analyzing complex systems and software for actual or potential security vulnerabilities requires extensive knowledge, real world experience and the right tools applied at the right time.“

http://www.safer-networking.org/ [22. Feber 2008] Webseite zum Download von Programmen zum Schutz der Privatsphäre, betrieben von Safer-Networking Limited.

http://www.sans.org/ [11. März 2008] Selbstbeschreibung: „SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internets early warning system - Internet Storm Center.“

http://www.sap.com/ [22. Feber 2008] Webseite des Business-Softwareherstellers SAP AG.

http://www.sarbanes-oxley.com/ [21. Feber 2008] Selbstbeschreibung: „Sarbanes-Oxley provides a complete cross-referenced index of SEC filers, audit firms, offices, CPAs, services, fees, compliance/enforcement actions and other critical disclosure information.“, betrieben von Karl Nagel & Company, LLC's.

http://www.schuler-ds.de/ [23. Feber 2008] Webseite der IT-Informationssicherheitsexpertin Karin Schuler.

http://www.scs.carleton.ca/ [2. Feber 2008] Webseite der kanadischen Universität Carleton.

http://www.secondlife.com/ [28. Feber 2008] Selbstbeschreibung: „Second Life is a 3-D virtual world entirely created by its Residents. From the moment you enter the World you'll discover a vast digital continent, teeming with people, entertainment, experiences and opportunity. Once you've explored a bit, perhaps you'll find a perfect parcel of land to build your house or business. You'll also be surrounded by the Creations of your fellow Residents. Because Residents retain the rights to their digital creations, they can buy, sell and trade with other Residents. The Marketplace currently supports millions of US dollars in monthly transactions. This commerce is handled with the in-world unit-of-trade, the Linden dollar, which can be converted to US dollars at several thriving online Linden Dollar exchanges.“

http://www.securityinfo.ch/ [24. Feber 2008] Webseite zur Informationssicherheit, betrieben von Werz IT Consulting.

http://www.semantic-web.at/ [24. Feber 2008] Webseite des Dienstleistungsunternehmens Semantic Web School Blumauer & Partner OEG für Semantic Web.

http://www.servat.unibe.ch/law/dfr/bv065001.html [24. Feber 2008] Webseite des Instituts für öffentliches Recht der Universität Bern mit Link auf das Bundesverfassungsrecht.

http://www.service-architecture.com/ [24. Feber 2008] Webseite zu Web Services und SOA, betrieben von Barry & Associates, Inc.

http://sicherheitskultur.at/ [23. Feber 2008] Webseite des IT-Experten Philipp Schaumann.

http://www.sirenic.com/ [23. Feber 2008] Webseite des Wissensmanagement-Softwareherstellers Sirenic.

http://www.skype.com/ [18. Feber 2008] Webseite der Skype Technologies S.A.

http://news.softpedia.com/ [24. Feber 2008] Webseite zur Übersicht über frei downloadbare Software, betrieben von Softpedia.

http://www.solnet.ch/ [23. Feber 2008] Webseite des Internetlösungsanbieters SolNet.

http://www.sonybmg.com/ [27. Feber 2008] Webseite des Musik-Joint Ventures Sony und BMG.

http://www.sophos.com/ [27. Feber 2008] Webseite des Informationssicherheitsspezialisten Sophos Pic.

http://mixmaster.sourceforge.net/ [4. Juli 2007] Selbstbeschreibung: „SourceForge.net is the world's largest Open Source software development web site, hosting more than 100.000 projects and over 1.000.000 registered users with a centralized resource for managing projects, issues, communications, and code. SourceForge.net has the largest repository of Open Source code and applications available on the Internet, and hosts more Open Source development products than any other site or network worldwide. SourceForge.net provides a wide variety of services to projects we host, and to the Open Source community."

http://www.soxlaw.com/ [23. Feber 2008] Webseite zur Sarbanes-Oxley, betrieben von Addison-Hewitt Associates B2B Consultancy.

http://www.sozialversicherung.at/ [28. Juni 2007] Webseite des Hauptverbandes der österreichischen Sozialversicherungsträger.

http://www.spamhaus.org/ [27. Feber 2008] Selbstbeschreibung: „The Spamhaus Project is an international non-profit organization whose mission is to track the Internets Spam Gangs, to provide dependable realtime anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spammers worldwide, and to lobby governments for effective anti-spam legislation."

http://www.spionagecheck.de/ [1. Feber 2008] Webseite der Deutschen Gewerkschaft für Dienstleistung (kurz: ver.di), Bereich Innovations- und Technologiepolitik.

http://www.spychips.com/ [26. Feber 2008] Selbstbeschreibung: „Spychips - How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move - is a project of CASPIAN, Consumers Against Supermarket Privacy Invasion and Numbering."

http://www.ssrn.com/ [27. März 2007] Selbstbeschreibung: „Social Science Research Network (kurz: SSRN) is devoted to the rapid worldwide dissemination of social science research and is composed of a number of specialized research networks in each of the social sciences. Each of SSRN's networks

encourages the early distribution of research results by publishing Submitted abstracts and by soliciting abstracts of top quality research papers around the world. We now have hundreds of journals, publishers, and institutions in Partners in Publishing that provide working papers for distribution through SSRN's eLibrary and abstracts for publication in SSRN's electronic journals.“

http://derstandard.at/ [5. Juli 2007] Webseite der österreichischen Tageszeitung derStandard.

http://www.stanford.edu/ [10. Feber 2008] Webseite der Universität Standford.

http://www.statistik.at/ [28. Juni 2007] Webseite der Bundesanstalt Statistik Österreich.

http://www.steria-mummert.de/ [27. Feber 2008] Webseite des IT-Beratungsunternehmens Steria Mummert Consulting.

http://www.stern.de/ [21. Feber 2008] Webseite des Medienunternehmens stern – Das deutsche Magazin.

http://stop1984.com/ [2. Feber 2008] Webseite der Non-Governmental Organisation (kurz: NGO) STOP1984, die sich mit Bürgerrechten befaßt, schwerpunktmäßig dem Recht auf informationelle Selbstbestimmung und dem Schutz der Privatsphäre. Hinzu kommt eine Vielzahl von verwandten Themen, von der Zensur in China bis hin zu aktuellen Ereignissen.

http://www.s-trust.de/ [23. Feber 2008] Webseite des Trustcenters der DSV-Gruppe, betrieben von der Deutschen Sparkassen Verlag GmbH.

http://www.sueddeutsche.de/ [21. Feber 2008] Webseite des Medienunternehmens sueddeutsche.de GmbH.

http://www.sun.com/ [2. Feber 2008] Webseite des IT-Konzerns Sun Microsystems.

http://www.sunbelt.com/ [27. Feber 2008] Webseite des Hardware-Distributors Sunbelt Telecommunications Inc.

http://www.symantec.com/ [20. Feber 2008] Webseite des Malwareschutz-Herstellers Symantec Corp.

http://www.symlabs.com/ [22. Feber 2008] Webseite mit Spezialisierung auf Identity Management und Directory Infrastructure des Unternehmens Symlabs.

http://www.synspector.de/ [22. Feber 2008] Webseite des deutschen Internetdienstleisters synergetic Medien- und Systemtechnologie AG.

[T]

http://www.tcpdump.org/ [27. Feber 2008] Selbstbeschreibung: „This page was started to collect various patches that have been floating around for LBL's tcpdump and libpcap programs, and to continue the work needed on both projects.“

http://www.tcp-ip-info.de/ [22. Feber 2008] Webseite mit Informationen über TCP/IP, Internet und Sicherheit, betrieben von Gerhard Glaser.

http://www.tct.de/ [22. Feber 2008] Webseite des Geschäftsprozessexperten TC&T Consult und Training GmbH.

http://www.tecchannel.de/ [22. Feber 2008] Webseite zu Techniken und Technologien im IT-Bereich, betrieben von IDG Business Media GmbH.

http://www.tech-faq.com/ [22. Feber 2008] Selbstbeschreibung: „At the Tech FAQ, the technical answers you have been looking for are answered in detail, yet in a way the average person can understand. We pride ourselves on answering all of your toughest technology questions, yet in a way that you can comprehend. If you want to know what VoIP is or how to rid your computer of spyware, not to mention learning how to network your home office you will find all the answers at the Tech FAQ."

http://www.techpresident.com/ [22. Feber 2008] Selbstbeschreibung: "TechPresident was started by Andrew Rasiej and Micah Sifry as a new group blog that covers how the 2008 presidential candidates are using the web, and vice versa, how content generated by voters is affecting the campaign."

http://www.telekom-presse.at/ [22. Feber 2008] Webseite mit Pressemitteilungen aus dem Telekombereich, betrieben von Telekom Presse Dr. Peter F. Mayer KG.

http://www.tenebril.com/ [27. Feber 2008] Webseite des Geschäftsprozess-Softwareherstellers Tenebril, Inc.

http://www.tfh-berlin.de/ [22. Feber 2008] Webseite der Technischen Fachhochschule Berlin.

http://www.thawte.com/ [9. Jänner 2008] Webseite der Certification Authority thawte, Inc.

http://www.43things.com/ [18. Feber 2008] Selbstbeschreibung: „People have known for years that making a list of goals is the best way to achieve them. But most of us never get around to making a list. Make a list on 43 Things and see what changes happen in your life. Best of all it's a way of connecting with other enthusiasts interested in everything from watching a space shuttle launch to grow my own vegetables. So the next time someone asks you, "what do you do?" you can answer with confidence, "I am doing 43 things!".

http://spam-filter-review.toptenreviews.com/ [21. Feber 2008] Webseite über Spam, betrieben von TopTenREVIEWS, Inc.

http://www.trendmicro.com/ [22. Feber 2008] Webseite des Malwareschutz-Herstellers Trend Micro, Inc.

http://www.trojaner-info.de/ [22. Feber 2008] Webseite über Trojanische Pferde, betrieben von trojaner-info.de.

https://www.trustedcomputinggroup.org/ [22. Feber 2008] Selbstbeschreibung: „The Trusted Computing Group (kurz: TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys etc.) from compromise due to external software attack and physical theft.

TCG has adopted the specifications of TCPA and will both enhance these specifications and extend the specifications across multiple platforms such as servers, PDA's, and digital phones. In addition, TCG will create TCG software interface specifications to enable broad industry adoption."

http://ig.cs.tu-berlin.de/ [22. Feber 2008] und http://user.cs.tu-berlin.de/ [22. Feber 2008] Webseiten des Lehrstuhls für Informatik und Gesellschaft bzw. der Fakultät Elektrotechnik und Informatik der Technischen Universität Berlin.

http://anon.inf.tu-dresden.de/ [3. Juli 2007] Webseite des Instituts für Systemarchitektur der Technischen Universität Dresden.

[U]

http://www.uddi.org/ [22. Feber 2008] Selbstbeschreibung: „This is the official community gathering place and information resource for the UDDI OASIS Standard, which defines a universal method for enterprises to dynamically discover and invoke Web services. The standard is advanced through an open process by the OASIS UDDI Specification Technical Committee, a group that encourages new participation from developers and users. This is a community-driven site, and the public is encouraged to contribute content."

http://istlab.dmst.aueb.gr/ [21. Feber 2008] Webseite der Abteilung Managementwissenschaften der griechischen Universität Athen.

http://www.uibk.ac.at/ [7. Feber 2008] Webseite des Instituts für Biostatistik und Dokumentation der österreichischen Universität Innsbruck.

http://research.umbc.edu/ [21. Feber 2008] Webseite der amerikanischen Universität Maryland.

http://www.zdv.uni-mainz.de/ [22. Feber 2008] Webseite des Zentrums für Datenverarbeitung der deutschen Gutenberg-Universität Mainz.

http://www.uni-muenster.de/ [21. Feber 2008] Webseite der deutschen Universität Münster mit Informatikangebot.

http://www.united-security-providers.ch/ [22. Feber 2008] Webseite des Informationssicherheitsexperten United Security Providers Holding AG.

[V]

http://www.verisign.com/ [22. Feber 2008] Webseite des Internetinfrastruktur-Anbieters VeriSign, Inc.

http://www.verzeichnisdienst.de/ [22. Feber 2008] Webseite für Informationen rund um LDAP- und X.500-Verzeichnisdienste sowie verwandte Themen wie PKI, betrieben von Arnim Rupp.

http://www.vignette.at/ [2. Juni 2007] Webseite der österreichischen Autobahnen- und Schnellstrassenfinanzierungs AG [kurz: ASFINAG].

http://www.virenschutz.info/ [22. Feber 2008] Webseite mit Informationen zum Virenschutz, betrieben von InternetServiceAgentur.com.

http://www.vmware.com/ [22. Feber 2008] Webseite des Virtualisierungsspezialisten VMware, Inc.

http://www.voelcker.com/ [8. Dezember 2007] Webseite des Softwareherstellers und IT-Service Management-Anbieters Völcker Informatik AG.

http://www.volksbank.de/ [27. Feber 2007] Webseite des deutschen Kreditinstituts Volksbanken Raiffeisenbanken VR-NetWorld GmbH.

[W]

http://www.w3.org/ [1. Juli 2007] Selbstbeschreibung: „The World Wide Web Consortium (kurz: W3C) is an international consortium where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is: To lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web.“

http://www.wahlkampf-digital.de/ [21. Feber 2008] Webseite als Infopoint für digitale Wahlkämpfer, betrieben von Infoorg.Net LTD. & Co. KG.

http://www.washington.edu/ [10. Juni 2007] Webseite der Universität Washington.

http://www.webroot.com/ [27. Feber 2008] Webseite des Softwareunternehmens Webroot Software, Inc.

http://www.websense.com/ [27. Feber 2008] Webseite des IT-Unternehmens Websense, Inc.

http://www.weforum.org/ [21. Feber 2008] Selbstbeschreibung: „The World Economic Forum is an independent, international organization incorporated as a Swiss not-for-profit foundation. We are striving towards a world-class corporate governance system where values are as important a basis as rules. Our motto is entrepreneurship in the global public interest. We believe that economic progress without social development is not sustainable, while social development without economic progress is not feasible.”

http://www.whatwg.org/ [22. Juni 2007] Webseite der Web Hypertext Application Technology Working Group (kurz: WHATWG). WHATWG ist eine Arbeitsgruppe, deren Ziel darin besteht, durch Erweiterung von bereits bestehenden Technologien neue Technologien zu entwickeln, die es Autoren erleichtern soll, Internetanwendungen zu erstellen.

http://www.whitehouse.gov/ [21. Juni 2007] Webseite der Repräsentanz des US-amerikanischen Präsidenten.

http://www.wikipedia.org/ [18. Feber 2008] Selbstbeschreibung: „Wiki ist eine Webseite, deren Seiten jedermann leicht und ohne technische Vorkenntnisse direkt im Internetbrowser ändern kann. Wikipedia ist ein Projekt freiwilliger Autoren zum Aufbau einer Enzyklopädie. Die Artikel sollen Wissen aus belegten und zuverlässigen Quellen enthalten. Anders als herkömmliche Enzyklopädien ist die Wikipedia frei. Es gibt sie nicht nur kostenlos im Internet, sondern jeder darf sie mit Angabe der

Quelle und der Autoren frei kopieren und verwenden. Dafür sorgt die GNU-Lizenz für freie Dokumentation, unter der die Autoren ihre Texte veröffentlichen."

http://www.wiwi.hu-berlin.de/ [21. Feber 2008] Webseite der wirtschaftswissenschaftlichen Fakultät der Humboldt Universität Berlin.

http://www.ws-standards.com/ [5. Mai 2007] Webseite mit Übersicht über Web Service-Standards, betrieben von SOA Systems Inc.

[X]

http://www.xerobank.com/ [21. Feber 2008] Webseite des IT-Securityspezialisten Xerobank.

http://www.xing.com/ [2. März 2008] Webseite (Online-Community) zur Pflege von beruflichen Kontakten und zum Austausch von Informationen, betrieben von der XING AG.

[Y]

http://yadis.org/ [21. Feber 2008] Selbstbeschreibung: „This wiki supports the Yadis community whose goal it is to make URL-based identity widespread and interoperable, while enabling developers around the world to participate and implement their own identity-related ideas without stepping on others' toes."

http://www.yahoo.com/ [21. Feber 2008] Webseite (Portal) der Yahoo Inc.

http://www.youtube.com/ [21. Feber 2008] Webseite (Online-Videoplattform) der YouTube LLC.

[Z]

http://www.zdnet.de/ [22. Feber 2008] und http://www.silicon.de/ [24. Feber 2008] Webseiten mit Fokus auf technologie- und handelsbezogene Informationen, Daten und Dienstleistungen über die gesamte IT-Wertschöpfungskette hinweg, betrieben von der CNET Networks Inc.

http://www.zeit.de/ [21. Feber 2008] Webseite des Medienunternehmens ZEIT online GmbH.

5.3 BESUCHTE VERANSTALTUNGEN/PROJEKTE

[2004]

Informationssicherheitskonzept Amt der Burgenländischen Landesregierung [Frühjahr 2003 – lfd.]: Erstellung, Durchführung, Überwachung; Teilnahme an internen und externen Meetings.

Fundamentals of Network Security [8. – 12. November 2004, Kurs, Global Knowledge, Wien]

Sicherheitsmanagement mit Schwerpunkt Identity Management [10. November 2004, Konferenz, BRZ, Wien]

[2005]

Portalverbund [Frühjahr 2005 – lfd.]: Planung und Umsetzung; Teilnahme an internen und externen Meetings.

Mobility [1. Feber 2005, Konferenz, IDC, Wien]

Device Control [10. Feber 2005, Workshop, Bacher Systems, Wien]

ITnT [17. Feber 2005, Messe, Wien]

Notebook Security/Device Control [23. Feber 2005, Workshop, Bacher Systems, Wien]

IT-Governance [3. März 2005, Konferenz, future.net, Wien]

Sicherheit im Netzwerk [7. April 2005, Workshop, Cisco, Wien]

Virtualisierung [12. April 2005, Herstellerbesprechung, HP, Eisenstadt]

ITCOM [14. April 2005, Konferenz, ITCOM Bischinger, Baden]

Datenschutz [25. April 2005, Seminar, Amt der Burgenländischen Landesregierung, Eisenstadt]

Virtualisierung [28. April 2005, Herstellerbesprechung, IBM, Eisenstadt]

Servertrends Blade-Technologie [29. April 2005, Herstellerbesprechung, IBM, Eisenstadt]

Business Intelligence [19. Mai 2005, Konferenz, LSZ, Wien]

Security in Depth: Verschlüsselung mit Microsoft Technologien [31. Mai 2005, Workshop, MII, Wien]

Microsoft Big Days [8. Juni 2005, Konferenz, Microsoft, Wien-Vösendorf]

Security Conference [14. Juni 2005, Konferenz, IIR, Wien]

Virtual Criminology Report [18. August 2005, Konferenz, McAfee, Wien]

IT-Security und das Gesetz, rechtliche Grundlagen der IT-Sicherheit [24. August 2005, Workshop, it-versity, Wien]

Security Conference Day 1 + 2 [6. – 7. September 2005, Konferenz, IDC, Wien]

IBM Symposium [8. September 2005, Roadshow, IBM, Wien]

Cisco-mii-Microsoft Roadshow [22. September 2005, Roadshow, MII, Wien]

Schoeller Forum 2005 [12. Oktober 2005, Konferenz, Schoeller, Wien]

Virtualisierung [24. Oktober, Herstellerbesprechung, HP, Wien]

IT-Governance/E-Government [15. – 16. November 2005, Konferenz, CONEX, Wien]

[2006]

Client (Notebook) Security [12. Jänner 2006, Meeting, BRZ, Wien]

Security und Identity Management [23. Jänner 2006, Konferenz, Austrian Security Forum/CON.ECT, Wien]

Service Oriented Architecture [2. Feber 2006, Konferenz, LSZ/HP/Oracle, Wien]

ITnT [15. Feber 2006, Messe, Wien]

ITIL Foundation Training [20. – 21. Feber 2006, Training mit Prüfung, CON.ECT, Wien]

Process Management [22. März 2006, Konferenz, CONEX, Wien]

2. Information Security Symposium [29. März 2006, Konferenz, CIS, Wien]

Identity Management Day [4. April 2006, Konferenz, IT-Verlag, München]

Business Continuity/Disaster Recovery [17. Mai 2006, Konferenz, IDC, Wien]

E-Government Konferenz 2006 [1. – 2. Juni 2006, Konferenz, ADV, Linz]

Standardportal – der Weg in den Portalverbund [22. Juni 2006, Meeting, BMI, Wien]

IBM Symposium [7. September 2006, Roadshow, IBM, Wien]

Security Roadshow [12. – 13. September 2006, Roadshow, IDC, Wien]

Security & Identity Roadshow [19. September 2006, Roadshow, CON.ECT, Wien]

EDV-Expertenkonferenz [26. – 27. September 2006, Konferenz, Bundes- und Länderarbeitsgruppe, Admont]

SecurITy [10. – 11. Oktober 2006, Konferenz, IIR, Wien]

Geschäftsprozessoptimierung/ITIL [12. Oktober 2006, Konferenz, LSZ, Wien]

Haftungsrisiko/IT-Sicherheit [17. Oktober 2006, Konferenz, Symantec, Wien]

3. Österreichischer IT-Sicherheitstag [8. November 2006, Konferenz, Universität Klagenfurt, Wien]

Forum IT Sicherheit 2006 [8. – 9. November 2006, Konferenz, CONEX, Wien]

Arbeitsgruppensitzung Sicherheit [16. November 2006, Meeting, Bundes- und Länderarbeitsgruppe, Wien]

[2007]

ITnT [31. Jänner 2007, Messe, Wien]

Arbeitsgruppensitzung Sicherheit [22. Feber 2007, Meeting, Bundes- und Länderarbeitsgruppe, Wien]

Security-, Risiko- & Identity-Management [1. März 2007, Informunity, CON.ECT, Wien]

3. Information Security Symposium [21. März 2007, Konferenz, CIS, Wien]

Arbeitsgruppensitzung Sicherheit [5. April 2007, Meeting, Bundes- und Länderarbeitsgruppe, Wien]

Web 2.0 goes Business [9. Mai 2007, Konferenz, CONEX, Wien]

E-Government Konferenz 2007 [24. – 25. Mai 2007, Konferenz, ADV, Krems]

Branchenkonferenz Behörden [19. September 2007, Konferenz, LSZ, Wien]

IT-Security, Rechtslage, Identity Management [19. September 2007, Konferenz, CON.ECT, Wien]

Information Security Konferenz [16. November 2007, Konferenz, Donau Universität Krems, Wien]

Strategieworkshop [29. – 30. November 2007, Workshop, IBM, Kukmirn]

IT-Update: Trends und künftige Entwicklungen [3. – 4. Dezember 2007, Seminar, IIR, Wien]

[2008]

Netzwerk- und Applikationsüberwachung [15. Jänner 2008, Workshop, Schoeller Networks, Wien]

Portal, Web Services, SOA [29. Jänner 2008, Workshop, IBM, Eisenstadt]

Authentifizierung mittels Smartcard [März 2008 – lfd.]: Planung und Umsetzung; Teilnahme an internen und externen Meetings.

Lebenslauf Mag. Josef Heinschink

Persönliche Informationen	Nationalität: Familienstand: Alter: Geburtsort:	▪ Österreich ▪ verheiratet, 2 Kinder ▪ 37 Jahre ▪ Eisenstadt	
Ausbildung	2004-2008 1991-1997 1991	Technische Universität Doktorratsstudium Informatik Universität/Technische Universität Wien Diplomstudium Betriebsinformatik Matura	Wien Wien Wien
Berufserfahrung	1.7.2002-lfd. 1.2.1993-30.6.2002 1989, 1990, 1991, 1992	**EBRZ** ▪ IT-Projektabwicklung/Informationssicherheit **Hewlett-Packard** ▪ Technical Consultant (Österreich, Osteuropa) ▪ Customer Service Representative (Osteuropa) ▪ Sales Admin Coordinator (Österreich) ▪ Werkstudent IT-Department **Austrian Research** ▪ Werkstudent	Eisenstadt Wien Seibersdorf
Sprachen	Deutsch, Englisch		
Kenntnisse	Hardware (LAN, WLAN, Server), Betriebssysteme, Software, Datenbanken (Microsoft, Linux, Citrix, SQL), Programmiersprachen (C++, Perl), Mobile Computing, Webtechnologien, Informationssicherheit, ITIL		