FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

# ITIL als Methode gegen Attacken eines Social Engineers im IT-Betrieb

DISSERTATION

zur Erlangung des akademischen Grades

**Doktor der technischen Wissenschaften**

eingereicht von

**Andreas Ehringfeld**
Matrikelnummer 9726310

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Thomas Grechenig

Diese Dissertation haben begutachtet:

_____ (Vorname Nachname)

_____ (Vorname Nachname)

Wien, 10.01.2012

_____ (Andreas Ehringfeld)

# ITIL als Methode gegen Attacken eines Social Engineers im IT-Betrieb

## DISSERTATION

zur Erlangung des akademischen Grades

**Doktor der technischen Wissenschaften**

eingereicht von

**Andreas Ehringfeld**

9726310

ausgeführt am

Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software

der Fakultät für Informatik der Technischen Universität Wien

**Betreuung:** Thomas Grechenig

Wien, 10.01.2012

# Erklärung zur Verfassung der Arbeit

Andreas Ehringfeld

Neufeldergasse 13, 2463 Stixneusield

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

---------- ----------

(Ort, Datum) (Andreas Ehringfeld)

# Kurzfassung

Trotz des kontinuierlichen wissenschaftlichen Diskurses über Information Security sind gerade jene Angriffe noch nicht ausreichend behandelt, die auf menschlichen Aspekten basieren. Dies resultiert primär aus dem bisherigen Fokus, auf der personellen Sicherheitsebene einen wirksamen Schutz gegen Social Engineering aufzubauen.

Moderne Informationssicherheitsmodelle zeichnen sich allerdings unter anderem durch einen multi-dimensionalen Ansatz aus. Es ist daher naheliegend, auch gegen Social Engineering ein multi-dimensionales Sicherheitsmodell einzusetzen. Dieses Modell bedingt nicht nur eine Wechselwirkung zwischen den Dimensionen Technik, Mensch und Organisation, sondern auch eine Integration in die Corporate Governance. Diese Arbeit beleuchtet ITIL als ein solches mögliches Rahmenwerk gegen Hacker, die sich Social Engineering Methoden bedienen. Basierend auf beispielhaft dargestellten Prozessen werden Sicherheitsmerkmale in ITIL identifiziert und deren Wirkungsweise gegen Social Engineering diskutiert.

Nach der Evaluation der auf ITIL basierenden Sicherheitsmaßnahmen als eine multi-dimensionale Gegenstrategie werden die ITIL Maßnahmen entsprechend ihres Wirkungsbereichs klassifiziert. Daraus ergibt sich ein Management Katalog an Sicherheitsmaßnahmen gegen Social Engineering Angriffe. Abschließend wird gezeigt, dass ITIL als Rahmenwerk gegen Angriffe eines Social Engineers in eine unternehmensweite Information Security Governance integrierbar ist.

# Abstract

Despite all progress on the scientific foundations of information system security, human factor attacks are still not sufficiently researched. This is mostly due to the focus to build sufficient security against social engineering attacks based on personnel security measures.

Modern information security models rely on multi- dimensional approaches. Countering social engineering attacks more affectively would also demand a multidimensional approach to information security. Such an approach implies an interconnection of the technical, human and organizational domains and the relationship with corporate governance. This paper proposes ITIL to be such a framework against hackers using social engineering techniques. Based on an exemplified described process of a medium sized financial institution, security mechanisms are identified and classified in the ITIL framework, and their effectiveness against social engineering attacks is discussed.

After evaluating security measures according to ITIL for their potential to serve as such a multidimensional counter measure, ITIL measures will be classified according to their application area in preventing or counter acting attacks, thus providing a management catalogue of security measures against social engineering attacks. Finally it is shown that ITIL as a framework against hackers using social engineering techniques can be integrated into enterprise wide information security governance.

# Inhaltsverzeichnis

1 Einleitung ..... 1
1.1 Problemstellung ..... 3
1.2 Motivation ..... 5
1.3 Zielsetzung ..... 7
1.4 Verwandte Arbeiten ..... 8
1.5 Aufbau der Arbeit ..... 18
2 Grundlagen ..... 21
2.1 Sicherheit ..... 21
2.2 Systeme ..... 21
2.3 Systeme und Sicherheit ..... 22
2.4 Daten, Information und Wissen ..... 23
2.5 Informationssicherheit ..... 25
2.5.1 Sicherheitsbedürfnisse ..... 26
2.5.2 Standards für Informationssicherheit ..... 32
3 Information Technology Infrastructure Library ..... 36
3.1 Geschichte und Entwicklung von ITIL ..... 36
3.2 Aufbau von IT Service Management ..... 40
3.2.1 Service Strategy ..... 42
3.2.2 Service Design ..... 44
3.2.3 Service Transition ..... 46
3.2.1 Service Operation ..... 48
3.2.2 Continual Service Improvement ..... 49
3.3 ITIL und andere Referenzmodelle ..... 51
4 Bedrohungsanalyse – Risikofaktor Mensch ..... 57
4.1 Der Social Engineer ..... 58
4.2 Klassifizierung von Social Engineering ..... 60
4.3 Menschliche Faktoren von Social Engineering ..... 66
4.3.1 Reziprozität ..... 67
4.3.2 Konsistenz ..... 68

4.3.3 Soziale Bewährtheit ..... 69
4.3.4 Sympathie ..... 70
4.3.5 Autorität ..... 72
4.3.6 Knappheit ..... 73
4.4 Social Engineering Techniken ..... 75
4.4.1 Informationsbeschaffung ..... 75
4.4.2 Beziehungen aufbauen ..... 77
4.4.3 Beziehungen ausnutzen ..... 78
4.4.4 Ausführung ..... 79
4.5 Social Engineering Vertrauens- und Angriffsmodell ..... 80
5 Identifikation von allgemeinen Sicherheitsgrundsätzen in Service Operation Prozessen ..... 83
5.1 Choke Points verwenden ..... 83
5.2 Authentizität sicherstellen ..... 89
5.3 Gut planen und sich daran halten ..... 95
5.4 Risiko durch Aufteilung verringern ..... 105
5.5 Gestaffelte Abwehr ..... 110
5.6 Einfachheit ..... 120
5.7 Das schwächste Glied sichern ..... 127
5.8 Das Rad nicht immer neu erfinden ..... 139
5.9 In Frage stellen ..... 145
6 Analyse der Sicherheitsgrundsätzen in Service Operation Prozessen 151
6.1 Social Engineering Angriffe erschweren ..... 155
6.2 Social Engineering Angriffe erkennen ..... 156
6.3 Security Engineering Angriffe beheben ..... 156
6.4 Social Engineering Angriffe analysieren ..... 157
6.5 ITIL basierte Maßnahmenmatrix gegen Social Engineering Attacken ..... 157
6.5.1 Wirkungsweise ..... 161
6.5.2 Wirkungsbereich ..... 162
6.5.3 Wirkungsvektor ..... 163
6.5.4 Wirkungssteuerung und -kontrolle ..... 166

7 Umfassendes Sicherheitskonzept gegen Social Engineering Attacken 173

7.1 ITIL als Teil eines Sicherheitskonzepts ..... 174

7.2 Fallbeispiele ..... 179

7.2.1 ITIL bei Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft ..... 180

7.2.2 ITIL als Basis eines Kontrollsystems einer österreichischen Bank 185

7.3 Restrisikobestimmung ..... 189

8 Conclusio ..... 198

# Abbildungsverzeichnis

Abbildung 1: Anzahl Dateneinbrüche [ITRC09] ..... 4
Abbildung 2: Identitätsdiebstähle und andere Betrugsfälle [FTC09] ..... 5
Abbildung 3: Social Engineering – Verteidigungsringe [Mann08] ..... 6
Abbildung 4: Publikationslandschaft ITIL - Social Engineering (vereinfachte Darstellung) ..... 9
Abbildung 5: Vorgehensmodell basierend auf Engineering Methoden ..... 20
Abbildung 6: Daten, Information, Wissen, in Anlehnung an [FiSc05] ..... 24
Abbildung 7: Verfügbarkeit - Vertraulichkeit – Integrität [RaPf96] [ZSI89] ..... 27
Abbildung 8: Dimensionen von Informationssicherheit [Diem08] ..... 32
Abbildung 9: Verkettung von Sicherheitsnormen und -standards [Voss09] 35
Abbildung 10: ITIL V2 Framework [Dvwe05] ..... 37
Abbildung 11: ITIL Service Lifecycle [OGC07L] ..... 41
Abbildung 12: ITIL Prozesslandschaft ..... 42
Abbildung 13: Strategie der fünf P [Mint92] ..... 43
Abbildung 14: Information - Knowledge - Weisheit, basierend auf [Rowl07] [Zins07] ..... 48
Abbildung 15: CSI Verbesserungsprozess [OGC07I] ..... 50
Abbildung 16: Überblick Governance Frameworks, basierend auf [ISACA] ..... 51
Abbildung 17: COSO Würfel [COSO] ..... 52
Abbildung 18: COBIT Wüfel [ITGI07] ..... 53
Abbildung 19: CMMI Reifegradmodell ..... 54
Abbildung 20: TOGAF Architekturmodell [Open10] ..... 55
Abbildung 21: Mensch – Organisation – Technologie ..... 57
Abbildung 22: Phishing Mail Attacke 2006 gegen Kunden der BAWAG P.S.K. ..... 61
Abbildung 23: Meist gefälschte Internetseiten 2009 [APWG09] ..... 62
Abbildung 24: Reverse Social Engineering Phasen [Nels06] ..... 64
Abbildung 25: Social Engineering Kategorien ..... 66
Abbildung 26: Sympathie - Interaktion – Ähnlichkeit [Krol05] ..... 71
Abbildung 27: Phasen einer Social Engineering Attacke [Gartn02] ..... 75
Abbildung 28: Informationsbeschaffung durch automatisierte Zielpersonensuche [Hube09] ..... 77
Abbildung 29: Social Engineering Vertrauensmodell [Lari06] ..... 80
Abbildung 30: Social Engineering Angriffsmodell [Lari06] ..... 81
Abbildung 31: Zentrale Eigenschaft des Service Desks ..... 85
Abbildung 32: Überblick Service Desk Schnittstellen (vereinfacht) ..... 86

Abbildung 33: Zentraler Service Desk (1)/ Spezialisierte Service Desk Gruppen (2) / Verteilter Service Desk (3)/ Virtueller Service Desk (4) [OGC07O] ..... 88
Abbildung 34: ITIL Tool: Detailinformationen des Kunden darstellen ..... 93
Abbildung 35: ITSM - Prozessverbesserungsmodell [itSMF02] ..... 97
Abbildung 36: Prozess [itSMF02] ..... 98
Abbildung 37: Generisches ITIL Prozessmodell [itSMF02] ..... 99
Abbildung 38: ITIL Incident Management Prozess ..... 100
Abbildung 39: Incident Management Prozessabhängigkeiten [itSMF02] . 103
Abbildung 40: Incident Management Schnittstellen [itSMF02] ..... 104
Abbildung 41: Incident Management Support Levels ..... 108
Abbildung 42: Funktionsteilung in mehrere Aufgabenbereiche – Teilung in Durchführung und Kontrolle ..... 111
Abbildung 43: Funktionsteilung in mehrere Aufgabenbereiche – Verteilung auf mehrere Personen ..... 111
Abbildung 44: Funktionstrennung mit IKS ..... 112
Abbildung 45: Beispielprozess: Berechtigungsfreigabe – einfaches Szenario ..... 113
Abbildung 46: Beispielprozess: Berechtigungsfreigabe – erweitertes Szenario ..... 114
Abbildung 47: Beispielprozess: Berechtigungsfreigabe – Szenario mit Funktionstrennung ..... 115
Abbildung 48: Beispielprozess: Berechtigungsfreigabe – Sicherheitsmaßnahmen ..... 119
Abbildung 49: Post-it mit Passwort für eine Webanwendung ..... 121
Abbildung 50: Beispiel: Templates des Ticket Tools ..... 123
Abbildung 51: Beispiel: Verbindung zum SKMS (als Wiki realisiert) im Ticket Tool ..... 124
Abbildung 52: Beispiel: Auswahl des Standard Changes im Ticket Tool . 125
Abbildung 53: Beispiel: Standard- Change Formular im Ticket Tool ..... 126
Abbildung 54: Framework für Handhabung der Sicherheit [OGC07D] .... 128
Abbildung 55: Bestimmungsgrößen des Verhaltens [Rose02] ..... 132
Abbildung 56: Incident/ Service Request – CMDB – Spanngraph ..... 137
Abbildung 57: Incident/Service Request – CMDB – Spanngraph mit eingezeichneten Incidents ..... 138
Abbildung 58: Vier Phasen zur Etablierung einer Strategie für Bewusstsein von möglichen Social Engineering Angriffen [Mann08] ..... 139
Abbildung 59: OSI-Modell ..... 140
Abbildung 60: Überwachungsbereiche des ISO/ IEC 27001 Standards .... 142
Abbildung 61: PDCA-Zyklus [Demi86] ..... 146
Abbildung 62: Ablauf von Security Incidents [CaOv99] ..... 151

Abbildung 63: Social Engineering Model of Protection [Mann08] ..... 153
Abbildung 64: Erweitertes Social Engineering Sicherheitsmodell von [Mann08] ..... 154
Abbildung 65: Erweitertes Social Engineering Sicherheitsmodell von [Mann08] (Systemische Sicherheit als Stärkung bestehender Sicherheitsmaßnahmen) ..... 155
Abbildung 66: Überblick der Kategorisierung der auf ITIL basierten Sicherheitsmaßnahmen gegen Human- based Social Engineering Attacken ..... 163
Abbildung 67: Sicherheit von Services (vereinfachte Darstellung) ..... 164
Abbildung 68: Einfluss von ITIL auf die Sicherheit von Services ..... 165
Abbildung 69: Information Security Prozess, basierend auf [OGC07D] .. 166
Abbildung 70: Information Security Governance [Klai10] ..... 175
Abbildung 71: IT Governance Modell von COBIT [ITGI07] ..... 176
Abbildung 72: Systemic Security Management Model [KiBe06] ..... 178
Abbildung 73: Prozessbeschreibung zum Anhalten einer Wahl ..... 183
Abbildung 74: Prozessbeschreibung des Zurücksetzen eines Passworts ... 187
Abbildung 75: Sicherheit in Relation zum Aufwand für Sicherheitsmaßnahmen [Raep01] ..... 190
Abbildung 76: Das optimale betriebliche Kosten-Nutzen-Verhältnis in Abhängigkeit von Sicherheitskosten und potentiellen finanziellen Schäden [Raep01] ..... 191
Abbildung 77: Soziale Netzwerke ..... 195

# Tabellenverzeichnis

Tabelle 1: Abgrenzung von Daten, Information und Wissen [Gelb03] ..... 25
Tabelle 2: ITIL V2 zu ITIL V3 Prozess Mapping ..... 39
Tabelle 3: Social Engineering und Faktoren menschlichen Verhaltens, basierend auf [Cial07], [Lari06] und [HaPr09] ..... 67
Tabelle 4: Ziele eines Social Engineers [Hone04] ..... 79
Tabelle 5: Incident Management Support Levels ..... 108
Tabelle 6: Human Ressource Security aus ISO/ IEC 27002 ..... 132
Tabelle 7: Gründe für Demotivation von Mitarbeiter [LiHe07] ..... 135
Tabelle 8: Verbindung zwischen ITIL und COBIT [SaSh08] ..... 150
Tabelle 9: Maßnahmenkatalog gegen Social Engineering ..... 161
Tabelle 10: Beispielhafte Kontrollen und Steuerungen der Umsetzung des Maßnahmenkatalogs gegen Social Engineering ..... 172

# Abkürzungsverzeichnis

| Abkürzung | Bedeutung |
|---|---|
| **BSC** | Balanced Score Card |
| **CC** | Common Criteria for Information Security |
| **CMDB** | Configuration Management Database |
| **CMMI** | Capacity Maturity Model |
| **CSF** | Critical Success Factor |
| **CSI** | Continual Service Improvement |
| **ICT** | Information and Communications Technology |
| **IDS** | Intrusion Detection System |
| **IT** | Informationstechnologie |
| **ITIL** | Information Technology Infrastructure Library |
| **IKS** | Internes Kontrollsystem |
| **ISO** | International Organization for Standardization |
| **ISMS** | Information Security Management System |
| **KPI** | Key Performance Indicator |
| **OLA** | Operation Level Agreement |
| **OS** | Operating System |
| **PoLP** | Principle of Least Privilege |
| **RfC** | Request for Change |
| **RPC** | Remote Procedure Call |
| **SIP** | Service Improvement Plan |
| **SKMS** | Service Knowlegment Management System |
| **SLA** | Service Level Agreement |
| **SPoC** | Single Point of Contact |

# Hinweis im Sinne der Gleichbehandlung

Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung, wie z.B. Teilnehmer/Innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

# 1 Einleitung

*Eve arbeitet seit vielen Jahren in einer Bank, wo sie ihrer Tätigkeit als Händlerin nachkommt. Unzufrieden sitzt die Bankmitarbeiterin im Handelsraum und beobachtet an diesem Tag nur sehr uninteressiert die Marktbewegungen. Heute hat sie noch kein Geschäft abgeschlossen. Die letzte Bonuszahlung hat nicht annähernd ihre Erwartungen erfüllt. Gleichzeitig hat ihre viel jüngere Arbeitskollegin Alice eine für ihr Dafürhalten viel zu großzügige Sonderzahlung erhalten. Überhaupt werden ihre Leistungen nicht anerkannt und für die frei werdende Position der Teamleiterin sieht sie sich bereits übergangen. Die junge Kollegin, welche frisch von der Universität kommt und im Vergleich zu ihr überhaupt keine Erfahrung aufweist, gilt als sichere Kandidatin für die selbst erträumte Beförderung.*

*Frustriert und gedemütigt ist Eve, sie ist enttäuscht von der Firmenleitung. Mittlerweile ist ihr einziger Gedanke, der Kollegin Schaden zuzufügen. Alice soll ein derart katastrophales Geschäft abschließen, dass ihre Inkompetenz nicht weiter verleugnet werden kann. Wenn erst offensichtlich wird, wie fahrlässig ihre Kollegin Geschäfte tätigt, wird sich die Führungsebene besinnen und ihr selbst die Position der Teamleiterin zusprechen.*

*Ihr Plan ist sehr einfach und gerade deshalb genial. Auf der Intranet Seite des Unternehmens sucht sie nach den Fotos der Helpdesk Mitarbeiter. Sie entdeckt Bob, der aufgrund seines jungen Alters noch nicht lange berufstätig sein kann. Die nächsten Tage nimmt sie sich frei und beobachtet von einen nahen Cafe aus das Kommen und Gehen der Mitarbeiter. Besonders achtet Eve auf Bob, wodurch sie schon nach drei Tagen ein gutes Bild über dessen Arbeitszeiten bekommt.*

*Schließlich ist es soweit. An einem der nächsten Tage, an denen aufgrund eines Release Einsatzes der neuen Softwareversion besonders viele Störungen auftreten und der Helpdesk stark belastet ist, ruft Eve Bob an. Die Zeit ihres Anrufs ist nicht willkürlich gewählt, sondern auf wenige Minuten nach Arbeitsbeginn des Helpdesk Mitarbeiters abgestimmt. Kaum hat dieser den Hörer abgehoben, wird er bereits lautstark angebrüllt. Seit einer Stunde könne die Mitarbeiterin nicht mehr arbeiten. Man habe ihr eine Zurücksetzung des Passworts versprochen und nichts ist passiert. Niemand hat sie zurückgerufen und noch immer kann sie sich nicht im System anmelden. Noch dazu kommen in ein paar Minuten die neuen*

*Handelsdaten raus und da muss sie vorher ein paar Geschäfte in den Markt stellen. Die Worte „Frechheit“, „Inkompetenz“ und „Konsequenzen“ werden gezielt mehrfach eingesetzt. Schon nach wenigen Augenblicken ist Bob in der Defensive. Seine Beruhigungsversuche fruchten nicht. Offensichtlich hat einer seiner Kollegen die Anfrage von Alice liegengelassen und vergessen. Vielleicht ist es gerade zur Schichtübergabe passiert. Immer wieder gibt es Probleme bei der Übergabe von einer Schichtmannschaft zur nächsten und so entschuldigt sich Bob vielmals und hofft durch sein schnelles Handeln die Mitarbeiterin zu beruhigen. Er lässt sich Benutzername und gewünschte Applikation für das Zurücksetzen des Passworts durchsagen. Da Eve darauf drängt und da die Zeit knapp ist, bis die erwähnten neuen Handelsdaten reinkommen, einigt man sich bereits am Telefon auf ein Standardpasswort. Erleichtert, die Situation gerettet zu haben, legt der Helpdesk Mitarbeiter auf und kümmert sich um weitere Anrufer. Heute ist ein stressiger Tag für den Helpdesk und so geht dieser Anruf in der Flut der Störungsmeldungen unter.*

*Eve hat nun alles, was sie braucht. Als Benutzername hat sie nämlich nicht ihren eigenen genannt, sondern jenen von Alice. Schnell meldet sie sich als diese im System an. Sie tätigt ein paar katastrophale Geschäfte und hat sichtlich Freude daran. Bevor sie sich wieder als Alice abmeldet, löscht Eve innerhalb der Applikation essentielle Benutzerdateien, welche beim Laden der Applikation benötigt werden. Ihr Angriff ist erfolgreich abgeschlossen.*

*Die Spuren ihres Angriffs werden von Alice selbst in Zusammenwirken mit dem Helpdesk am nächsten Tag gelöscht. Als Alice sich nicht mehr im System anmelden kann, kontaktiert sie den Helpdesk. Nachdem das Passwort neuerlich zurückgesetzt wurde, entdeckt man, dass essentielle Benutzerdaten für die Applikation fehlen. Erst durch ein Wiederherstellen des Profils durch Rücksichern eines Backups kann Alice endlich wieder arbeiten. Als Ursache wird vom Helpdesk ein zerstörtes Benutzerprofil diagnostiziert. Da das Problem aber nunmehr gelöst ist, wird es nicht weiter analysiert.*

*Tage später werden die fatalen Geschäfte vom Back Office Team der Bank gesichtet. Alice wird augenblicklich zur Geschäftsleitung zitiert, wo man das Dienstverhältnis löst, da die Mitarbeiterin keine schlüssige Rechtfertigung darlegen kann.*

*Die Bank verfügt über ein hochmodernes Rechenzentrum. Sämtliche sensible Systeme und deren Daten sind durch mehrfache Firewall Systeme und Intrusion Detection Systeme geschützt. Die Serverräume sind videoüberwacht, haben Bewegungsmelder und Sicherheitsschleusen. Für*

*Sicherheit gibt man jährlich große Summen aus. Keine dieser Maßnahmen konnte den Angriff erkennen oder verhindern.*

## 1.1 Problemstellung

Das angeführte einleitende Beispiel zeigt, wie leicht es ist, technologische Sicherheitsmechanismen auszuhebeln, indem klassische Social Engineering Methoden vom Angreifer angewendet werden.

Social Engineering ist die Kunst und die Wissenschaft, Menschen nach den eigenen Willen zu beeinflussen und zu lenken. Social Engineering ist ein Euphemismus für nicht-technische oder wenig technische Mittel, wie Lügen, Täuschen, betrügerisches Auftreten, welche zur Attacke auf Informationssysteme genutzt werden. [McDo09]

> Bruce Schneier: "*Amateure hacken Systeme, Profis hacken Menschen.*"
>
> Kevin Mitnick: "*Um ein guter Hacker zu sein, ist es nicht notwendig, ein guter Techniker zu sein, es reicht, wenn man ein guter Lügner ist!*"

Ein Bericht von Infosecurity Europe [Info07] von 576 Büroangestellten ergab, dass Frauen viel eher dazu zu überreden waren, ihr Passwort Fremden gegenüber zu verraten als Männer. 44% der Frauen gaben ihr Passwort bei einer telefonisch durchgeführten vermeintlichen Marktumfrage preis, während dies 10% der Männer taten. Als Motivation zur Teilnahme an der Umfrage wurde eine Tafel Schokolade versprochen. Tatsächlich handelte es sich aber nicht um eine Marktforschung, sondern um ein Experiment zur Wirksamkeit von Social Engineering Attacken.

Obwohl im Vergleich zum Vorjahr anstelle von 61% der Büroangestellten nur mehr 21% der Befragten ihr Passwort im Rahmen einer Befragung verrieten, ist diese Zahl nicht minder alarmierend. Hinzu kommen noch die besorgniserregenden Erkenntnisse, dass scheinbar harmlose Informationen, wie zum Beispiel das Geburtsdatum, weiterhin von 61% der Befragten Fremden mitgeteilt wurden. 60% der Männer und 62% der Frauen gaben ihre Kontaktdaten weiter. Über die Hälfte der Beteiligten verwendeten das selbe Passwort für alle Anwendungen. Hierunter fallen diverse Webseiten, Online Banking Portale, Zugänge in der Firma uvm.

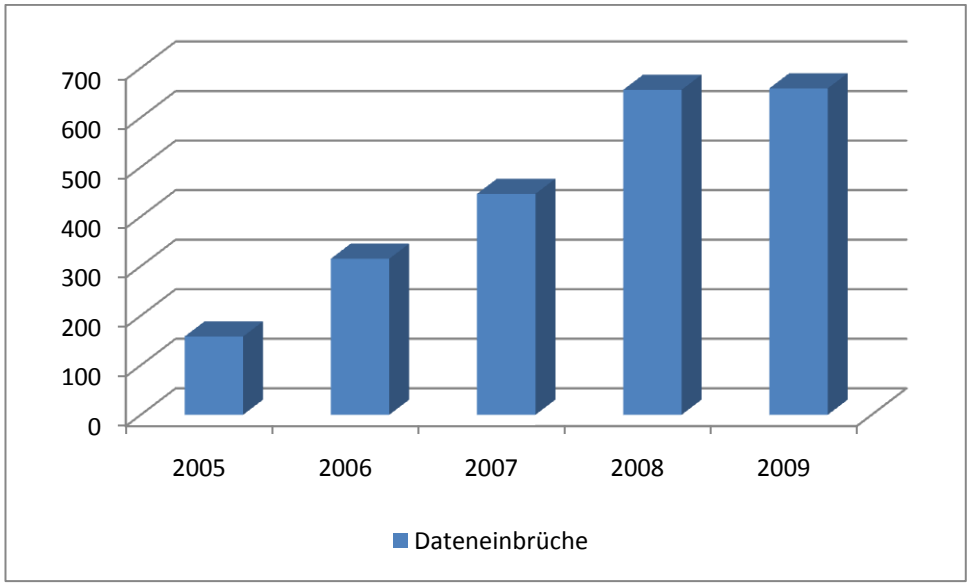



**Abbildung 1: Anzahl Dateneinbrüche [ITRC09]**

Abbildung 1 stellt die Anzahl der Dateneinbrüche über die letzten Jahre dar, die dem Identity Thief Resource Center (ITRC) [ITRC09] gemeldet wurden. Hierbei ist ein starker und kontinuierlicher Anstieg in den letzten Jahren bis 2008 festzustellen. Die Anzahl der gemeldeten Dateneinbrüche stieg zwischen 2008 und 2009 nur mehr marginal. Von den Bereichen Regierung/ Militär und Behörden, Bildungs-, Gesundheits-, Finanz- und Unternehmenssektor entwickelte sich der Unternehmenssektor am schlechtesten. Von einem 21% Anteil an Dateneinbrüchen im Jahr 2006 stieg dieser auf dramatische 41% bis 2009 an.

Betrachtet man den Schaden durch Datendiebstahl, welcher auf Software Engineering Angriffe zurückgeführt werden kann, so ergibt das im Jahr 2007 eine Schadenssumme von zwanzig Millionen Euro und im Jahr 2008 eine Schadenssumme von dreißig Millionen Euro in deutschen Industrieunternehmen [ASW10]. Im Report Internet Crime Complaint Center 2009 (IC3) [ICCC09] werden die jährlichen Verluste basierend auf gemeldeten Internetstraftaten mit 559,7 Millionen Dollar angegeben, was eine Verdoppelung zum Vorjahr darstellt. Die Anzahl der Schadensmeldungen ist um 22% gestiegen.

Identitätsdiebstahl, ein typisches Werkzeug des Social Engineerings, ist laut Federal Trade Commission (FTC) [FTC09] seit Beginn der Aufzeichnungen im Jahr 2000 der meist gemeldete Betrugsfall. Die folgende Abbildung stellt die Anzahl gemeldeter Identitätsdiebstähle zwischen 2000 und 2009 im Vergleich zu allen gemeldeten Betrugsfällen dar.

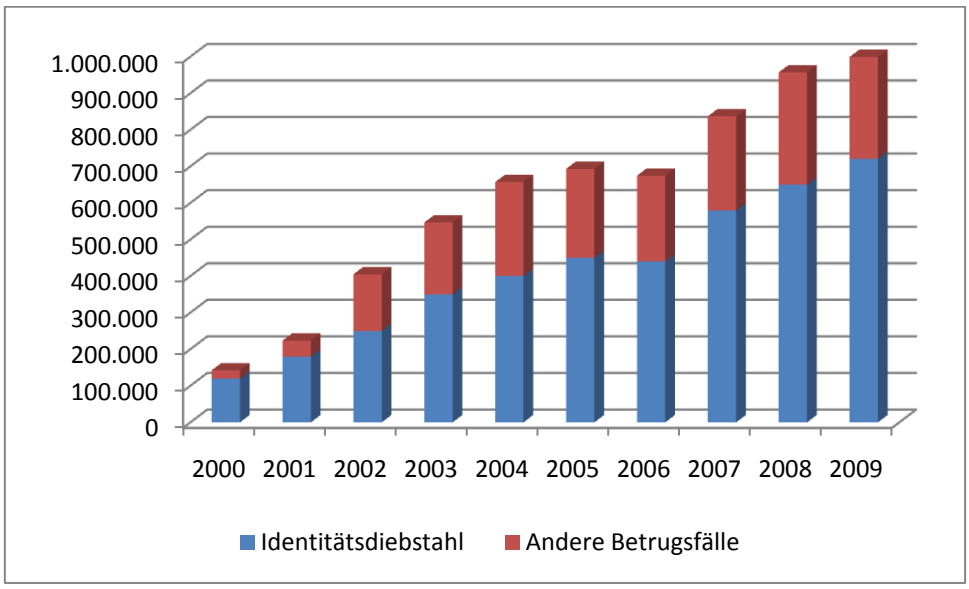



**Abbildung 2: Identitätsdiebstähle und andere Betrugsfälle [FTC09]**

Die Problemstellung dieser Arbeit ergibt sich somit aus der Analyse einer Möglichkeit, in Unternehmen der wohl immer gegenwertigen Gefahr, dass Menschen manipulierbar sind, entgegenzuwirken. Die Aktualität und Notwendigkeit der Analyse leitet sich aus den jährlichen Schadensfällen für Industrie und Wirtschaft ab.

## 1.2 Motivation

Die Motivation dieser Arbeit besteht darin aufzuzeigen, wie durch den korrekten Einsatz von Information Technology Infrastructure Library (ITIL) Angriffe eines Social Engineers erkannt und verhindert werden können.

Systeme werden zur Erledigung nahezu aller Aufgaben genutzt, wobei der Faktor Mensch eine zentrale Rolle spielt. Daher ist es von äußerster Wichtigkeit, den „Faktor Mensch“, entsprechend seiner Bedeutung, in den Sicherheitsprozess eines Unternehmens mit einzubeziehen.

In Arbeiten wie [Unbe01], [Kee08] und [ScMi08] wird der Schwerpunkt auf bewusstseinsbildende Maßnahmen gegen Social Engineering Attacken bei den Mitarbeitern gelegt. Schlüsselprinzip hierfür sind entsprechende Schulungsprogramme für Mitarbeiter, welche die Einhaltung von Sicherheitsrichtlinien vermitteln.

Eine Erweiterung dieser Maßnahmen wird in [Mann08] vorgestellt, welche auf aufeinander aufbauende Sicherheitsringe basiert. Sollte ein Angreifer einen Ring durchbrechen, so ist die sensible Information bzw. das Angriffsziel von weiter innen liegenden Ringen immer noch geschützt.

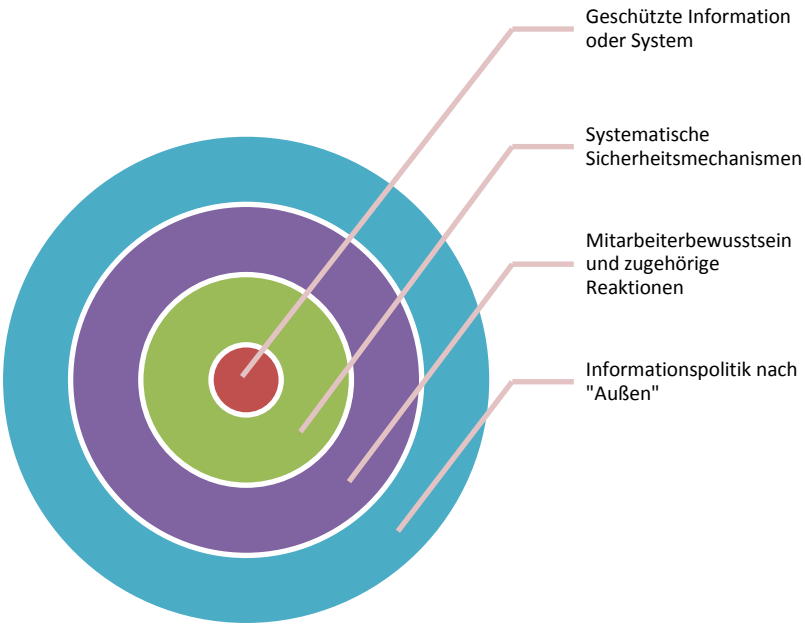



**Abbildung 3: Social Engineering – Verteidigungsringe [Mann08]**

Die Bildung und Kontrolle eines Sicherheitsbewusstseins der Mitarbeiter ist nur einer von mehreren Verteidigungsringen gegen Social Engineering Attacken. Die einzelnen Ringe werden im Detail in den folgenden Kapiteln erläutert.

Der Einsatz der IT zur Erreichung der Unternehmensziele ist essentiell für eine Unternehmung. Dabei liegt die Priorität nicht auf der Technik, sondern auf den Services. Diese sorgen im Zusammenspiel mit der Technik für eine konsequente Unterstützung der Geschäftsprozesse, damit die Dienstleistungen insgesamt effektiv, effizient und kundenorientiert ausgeführt werden können. Ein entscheidender Faktor für die Produktivität und Flexibilität und damit auch für die Produkt- oder Dienstleistungsqualität eines Unternehmens ist der Einsatz einer Informationstechnologie, die leistungsfähig, zuverlässig, flexibel, leicht benutzbar und auch sicher ist [KoKu07].

Betrachtet man die Notwendigkeit zur Absicherung vor Social Engineering Attacken als Teil der zu erbringenden Leistung eines Unternehmens, so ist der Schluss nahe, dass die Behandlung von Social Engineering Attacken

integraler Bestandteil des ITIL Rahmenwerks sein sollte. Nur unter dieser zu beweisenden Schlussfolgerung würden die Kriterien der Effizienz und Wirksamkeit erfüllt sein. Sind die Maßnahmen zur Abwehr von Social Engineering Attacken innerhalb des ITIL Frameworks hingegen nicht abbildbar, so ist sogar ein Widerspruch zwischen dem Konzept von ITIL und den orthogonalen Sicherheitsprozessen denkbar.

## 1.3 Zielsetzung

Ziel der Arbeit ist, durch die Beantwortung der folgenden Forschungsfragen eine Aussage über die Möglichkeit zur Erkennung und Abwehr (Erschwerung) von Attacken eines Social Engineers durch die Anwendung von ITIL Konzepten innerhalb des Betriebs (in ITIL als „Service Operation“ bezeichnet) zu treffen.

- Welche Sicherheitsmaßnahmen zur Erkennung, Abwehr (Erschwerung) und Analyse von Angriffen eines Engineers sind in Service Operation Prozessen nach ITIL abgebildet beziehungsweise abbildbar? Wodurch können Konzepte von ITIL und die damit verbundene serviceorientierte Sichtweise einen Schutz vor Social Engineering Attacken darstellen? Welche Rolle spielt ein auf ITIL basierendes Ticket Tool?
- Welche Klassenbildung ergibt sich beim Mapping von ITIL auf Social Engineering Attacken? Welche Machbarkeitsgrenzen sind bei der praktischen Anwendung identifizierbar?
- Stellt das auf ITIL basierende Konzept zur Erkennung und Abwehr von Attacken eines Social Engineers eine Erweiterung der Social Engineering Verteidigungsringe entsprechend [Mann08] dar? Was ergibt die Analyse der Migration und die Aufgabenteiler zwischen IT-Sicherheit und der IS-Governance eines Unternehmens? Gibt es durch die Einführung von ITIL neue Angriffsvektoren für einen Social Engineer?

Durch die Behandlung der Forschungsfragen soll die Hypothese, dass ITIL ein mögliches Rahmenwerk gegen Social Engineering Angriffe eines Hackers darstellt, bewiesen werden. Es soll gezeigt werden, dass ITIL ein multi-dimensionales Sicherheitsmodell gegen Social Engineering definiert, welches in eine unternehmensweite Information Security Governance integrierbar ist.

## 1.4 Verwandte Arbeiten

In [WiDe95] wird die Gefahr von Social Engineering dargestellt. Ein Social Engineering Angriff wird beleuchtet, bei dem auf sensible Unternehmensdaten erfolgreich zugegriffen werden konnte. Die Autoren kommen zum Schluss, dass selbst die besten technologischen Sicherheitsmaßnahmen den Angriff nicht verhindern konnten, da Schwächen im Sicherheitsbewusstsein ausgenutzt werden. Sicherheitsmanager müssten nicht-technische Aspekte von Computer Security gemeinsam mit technischen Maßnahmen berücksichtigen.

Als über die technischen und prozeduralen Maßnahmen gegen Social Engineering hinausgehende wissenschaftliche Betrachtungsweise der zugrundeliegenden Ursachen von Sicherheitsverletzungen werden in [Caca04] und [DoCa07] die Stärkung von Sicherheitsbewusstsein vorgeschlagen. Artikel wie [Unbe01], [Kee08] und [ScMi08] beschreiben Schulungsprogramme für Mitarbeiter, um die Einhaltung von Sicherheitsrichtlinien zu stärken. In [StWe98] wird ein Modell zur Wertung, Belohnung und Strafe von Verhalten und Fehlverhalten analysiert. In [Harr96], [MeFe03] und [Kurl95] werden Anleitungen zur situationsabhängigen ethischen und verantwortungsvollen Führung angeführt. Schulungsmaßnahmen für spezifische Sicherheitstechniken werden in [StNa90] diskutiert.

Die Social Engineering - Verteidigungsringe von [Mann08] stellen einen Versuch der visuellen Kategorisierung der Maßnahmen gegen Social Engineering dar, die im Zuge dieser Arbeit um die systemische Sichtweise von [KiBe06] erweitert werden und im Betrachtungsraum von ITIL und Social Engineering analysiert werden. Wie ITIL die Informationssicherheit in einer Organisation allgemein steigern kann, wird in den Artikeln [Kuhn07], [Marq08] und [Weil08] in Form von Punktelisten angeführt. Sie wurden in dieser Arbeit in Kapitel 5 bei der methodischen Identifikation und Analyse von Maßnahmen gegen Social Engineering Angriffe berücksichtigt.

Als weitere verwandte Arbeit beschäftigt sich [Semm09] mit einem ganzheitlichen Konzept für Informationssicherheit in ITIL unter Berücksichtigung des Schwachpunktes Mensch. Die Arbeit diskutiert personelle, technische und prozessuale Sicherheitsmaßnahmen. Die personellen Maßnahmen beinhalten Aspekte wie Motivation und Qualifikation von Mitarbeitern. In den technischen Sicherheitsmaßnahmen wird beispielsweise der Einsatz von Firewall Systemen und Anti- Viren Software erläutert. ITIL wird als Möglichkeit für prozedurale Sicherheit

angeführt, allerdings nicht im Detail analysiert. Im Gegensatz zu dieser Arbeit werden in [Semm09] technische, personelle und prozedurale Sicherheit als isolierte Maßnahmen angesehen, welche in keinem systematischen Modell behandelt werden, wie es in [KiBe06] vorgestellt wird. Das Modell von [KiBe06] beinhaltet die drei Eckpfeiler traditioneller Sicherheitsmodelle – „Mensch“ (Personal), „Prozesse“ (Organisation) und „Technologie“. Die signifikanteste Neuerung in diesem Modell ist gemäß [Klai10] die Sichtweise, dass sich Sicherheit aus dynamischen Interaktionen multidimensionaler Eckpunkte ergibt, worin sich moderne Informationssicherheitsmodelle auszeichnen. Dies stellt die Basis für die Beleuchtung von ITIL als ein solches Modell in dieser Arbeit dar und ist auch wesentlichstes Unterscheidungsmerkmal zu den anderen bisherigen wissenschaftlichen Betrachtungen von Social Engineering.

Betrachtet man die wissenschaftliche Landschaft an Publikationen in den beiden Domänen Social Engineering und ITIL, so kann folgende vereinfachte Visualisierung erstellt werden.

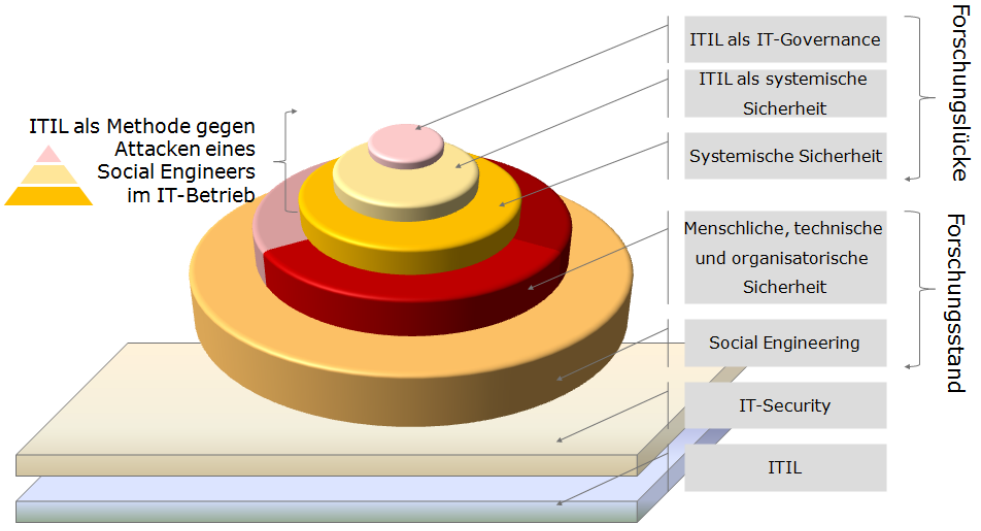



**Abbildung 4: Publikationslandschaft ITIL - Social Engineering (vereinfachte Darstellung)**

Aufbauend auf den Forschungsstand stellt ITIL das Fundament dieser Arbeit dar. Die betrachtete Forschungslücke ergibt sich aus der Analyse von ITIL als Methode gegen Attacken eines Social Engineers im IT-Betrieb. Im Fokus der Arbeit ist die Analyse der Kernelemente von IT-Governance und dessen Eigenschaften als systemisches Modell als kategorisierende

Elemente der Maßnahmen gegen Social Engineering Angriffe. Im Folgenden wird der Betrachtungsraum verwandter wissenschaftlicher Publikationen aufgespannt.

Zu ITIL gibt es eine Reihe wissenschaftlicher Publikationen über die verschiedenen Service Bereiche.

[EsGa10] Der Artikel analysiert die Effizienz von ITIL als strategisches IT-Geschäftsmodell, indem es mit dem Strategic Alignment Model (SAM) verglichen wird. Dieses Modell stellt die Basis für einige Forschungsarbeiten im IT-Strategiebereich dar. Durch den Vergleich wird beleuchtet, dass ITIL interne und externe Aspekte von IT innerhalb der IT-Strategie, Information Security Infrastruktur und Prozeduren in SAM abdeckt. Des Weiteren wird zusammengefasst, dass ITIL zwei Rollen im Management einer Organisation einnimmt. Generell gelten IT-Services als unterstützende Rolle für Geschäftsfelder. Zusätzlich nutzt ITIL die IT als "Enabler" für neue geschäftliche Möglichkeiten.

[QiJu10] Der Artikel [QiJu10] beschreibt ein Design eines auf ITIL basierenden Incident Management Prozesses mit wohldefinierten Rollen, Verantwortlichkeiten und Statuswerten von Incidents. Der analysierte Prozess beruht auf manuellen Tätigkeiten, weshalb er nicht als effizient angesehen werden kann. Die Toolunterstützung als Mittel zur Automation wird für weitere Analysen empfohlen. Des Weiteren wird die Wichtigkeit von Problem Management und einer adäquaten CMDB Implementierung unterstrichen.

[CuMa10] Im Gegensatz zur theoretischen Beleuchtung von [QiJu10] wird im Artikel [CuMa10] am Fallbeispiel eines Support Teams die praktische Implementierung eines Incident Management Prozesses dargestellt. Hierbei wird die Verwendung eines speziell angepassten Tools vorgestellt. Anschließend werden die operativen Erfahrungen bezüglich Incident Erkennung und Behebung, Automatisierung bei der Behandlung von Incidents und dem weiterführenden Problem Management von achtzehn Monaten Betrieb zusammengefasst. Der Artikel zeigt, dass durch die Berücksichtigung der ITIL Empfehlungen eine strukturierte Behandlung von Störungen erzielt werden kann.

[Kain08] Eine wissenschaftliche Beleuchtung, welche ebenso auf praktische Erfahrungen beruht, ist jene von [Kain08]. Hierbei wurden statistische Daten bei der Einführung von Incident Management und eines Service Desks in einer Bank über mehrere Jahre gesammelt und analysiert. Aus zum Beispiel der Anzahl der Störungsmeldungen, der Häufigkeit von Eskalationen aufgrund mangelnder Behebung und der Behebungsrate im 1st Level Support werden Schlüsse zur Anwendbarkeit und Effizienz von ITIL gezogen. Dabei wird festgestellt, dass die Konzepte von ITIL selbst in Stresssituationen, wie sie etwa nach großen Release Umstellungen auftreten, effizient anwendbar sind.

[JaEe06] Das Problem Management soll die Auswirkung von Störungen auf die Geschäftsprozesse minimieren und die effektive Störungsursache identifizieren Im Artikel [JaEe06] wird bezüglich Problem Management nicht nur das zugrundeliegende Konzept beleuchtet sowie die Vorzüge und Einschränkungen aufgezeigt, sondern auch wie Incidents, Problems und Known Errors anhand eines praktischen Beispiels erfasst werden sollten.

Einige wissenschaftlicher Artikel beleuchten die Verbindung und Kompatibilität von ITIL zu anderen Frameworks und Standards. Dabei wird beispielsweise ITIL mit COBIT und ISO/IEC 27002 verglichen und kombiniert, oder der Zusammenhang zwischen ITIL und IT-Governance bzw. SOA Governance analysiert. Dies verdeutlicht zum einen die Vernetzung mit anderen Frameworks und Standards als auch die Mächtigkeit von ITIL.

[NaSa08] Basierend auf [CrCe05] benötigt IT-Governance ein Rahmenwerk mit den folgenden drei Säulen: Struktur, Prozesse, Kommunikation. Zusätzlich müssen die Ziele der Haftung und Verantwortlichkeit des Managements, Messungen der Zielerfüllung (Performance-Kontrolle), Risiko-Management, Strategische Ausrichtung und Wertbeitrag in einem IT-Governance Rahmenwerk abgedeckt werden. Im Artikel wird die Konformität der Service Strategie gemäß ITIL Version 3 zu einem IT-Governance Framework diskutiert und prinzipiell festgestellt. Die einzelnen ITIL Prozesse müssten allerdings noch analog zu

[SaSh08] und [ISACA10] dem IT-Governance Modell zugeordnet werden, um den Beweisschritt zu vervollständigen.

[SuSe11] In [SuSe11] wird gezeigt, dass ITIL V3 und SOA viele elementare Verbindungen aufweisen. Die drei Hauptbestandteile von SOA-Governance sind Prozesse, Technologie und Menschen. SOA-Governance ist ein Management Modell, welches die Adaptionsfähigkeit und Integrität von SOA Systemen sicherstellt. Außerdem sollen Leistungsvermögen, Sicherheit und strategische Ausrichtung überprüfbar sein. Im Artikel [SuSe11] wird der Service Begriff als Verbindungselement zwischen SOA und ITIL angesehen. Jede Phase des SOA Governance Lifecycles kann ITIL V3 zugewiesen werden. Die wesentlichen Verbindungen sind zwischen „Plan“ und Service Strategy, „Design“ und Service Design, „Implement“ und Service Transition, „Control“ und Service Operation sowie „Evaluate“ und Continual Service Improvement.

[SaSh08] Die Kompatibilität zwischen ITIL und COBIT wird in [SaSh08] wissenschaftlich betrachtet und nachgewiesen. Ergebnis der Analyse ist die Feststellung, dass wenn man ITIL mit COBIT bewertet, die beiden Standards sehr gut miteinander korrespondieren. Vor allem wenn die COBIT Prozesse auf ITIL basieren, wie das in der aktuellen Version von COBIT der Fall ist, ist die Wechselwirkung und Kompatibilität der beiden Standards besonders hoch.

Im Fokus dieser Arbeit ist die Analyse, wie Methoden von ITIL gegen Social Engineering Attacken eingesetzt werden können. ITIL selbst wird als Rahmenwerk mit inhärenten Sicherheitsempfehlungen betrachtet. Die folgenden wissenschaftlichen Artikel und Whitepapers analysieren das ITIL Rahmenwerk auf allgemeine sicherheitsrelevante Grundzüge.

[LaMi10] In diesem Artikel wird festgestellt, dass ITIL V2 die Sicherheitsproblematik unzureichend aufgreift. Die Autoren folgern, dass vor allem durch die Verweise auf ISO 27001 die nachfolgende und derzeit aktuelle ITIL Version entscheidend mächtiger ist, wodurch ein Information Security Management System aufgebaut werden kann.

[Weil08] Der Autor beschreibt im Artikel [Weil08], wie in ITIL die Informationssicherheit in die Bereiche Policies, Prozesse, Prozeduren und Arbeitsinstruktionen gegliedert ist. Entscheidend für diese Gliederung ist die Einbettung in einen Zyklus ständiger Kontrolle und Verbesserung. Zusammenfassend werden im Artikel [Weil08] zehn Punkte aufgelistet, wie ITIL die Informationssicherheit erhöhen kann, welche sich auch in dieser Arbeit wiederfinden.

[Marq08] In ähnlicher Weise wie [Weil08] werden in [Marq08] elf Punkte angeführt, wie man mit ITIL einen Sicherheitsgewinn erzielen kann. Diese Maßnahmen überschneiden sich mit jenen von [Weil08]. Darüber hinaus werden im Artikel neun Schritte zur Umsetzung angeführt, welche mit einer Requirement Analyse und dem Aufbau eines gemeinsamen Sicherheitsverständnisses zwischen Kunde und Dienstanbieter beginnen und sich bis hin zum Berichtswesen und der zyklischen Kontrolle der Wirksamkeit erstrecken.

[Kuhn07] Im Practice Guide [Kuhn07] werden sechs Schritte vorgestellt, wie anhand vom Access Management eine Security Policy erfolgreich umgesetzt werden kann. Die Maßnahmen von [Weil08], [Marq08] und [Kuhn07] werden in dieser Arbeit in Kapitel 5 zusammengefasst berücksichtigt.

[Semm09] Die Arbeit analysiert ein ganzheitliches Konzept für Informationssicherheit unter besonderer Berücksichtigung des Schwachpunktes Mensch. Personelle, technische, prozedurale und physische Maßnahmen werden angeführt und beleuchtet. Zur Unterstützung des Information Security Managements wird empfohlen, zusätzliche Prozesse zu implementieren, die sowohl für den Betrieb als auch zur Steigerung der Informationssicherheit relevant sind. Dabei wird die Bedeutung vom Incident Management, Problem Management, Release Management und Availability Management hervorgehoben. Im Gegensatz zu dieser Arbeit wird in [Semm09] ITIL als eine von mehreren Maßnahmen betrachtet, nicht aber als umspannendes Rahmenwerk eines systemischen Sicherheitsansatzes.

Um die wissenschaftliche Landschaft dieser Arbeit in Anlehnung an die vereinfachte Darstellung in Abbildung 4 abzudecken, müssen ebenso Artikel und Whitepapers betrachtet werden, die sich mit Social Engineering in den verschiedenen Bereichen – Mensch, Technik, Organisation – beschäftigen.

[HaPr09] In diesem Artikel wird ein Angriffsvektor aufgespannt, der definiert, wie ein Social Engineer sein Opfer durch Überzeugungstechniken manipuliert. Als Basis für die Angriffsmethoden werden psychologische Eigenschaften aufgezeigt, die fest im menschlichen Verhalten verankert sind. Als typische Taktiken werden Einschüchterung, Sympathie, Identitätsdiebstahl, Täuschung, Konfusion, Dumpster Diving, Phishing und Reverse Social Engineering angeführt. Der Artikel beschreibt auch eine Reihe an Gegenmaßnahmen, welche in den Bereichen der menschlichen, technischen und organisatorischen Sicherheit eingeordnet werden können. Eine gesamtheitliche Sicherheitsstrategie, die etwa auch die Wechselwirkung der vorgestellten Gegenmaßnahmen darstellt, ist nicht Inhalt des Artikels.

[Lari06] Die Arbeit definiert das Social Engineering Vertrauensmodell (Social Engineering Trust Model) und das Social Engineering Angriffsmodell (Social Engineering Attack Model). [Lari06] beschreibt im Social Engineering Vertrauensmodell, wie ein Social Engineer eine Vertrauensbasis zu einer Person aufbaut, von der er Informationen für einen tiefergehenden Social Engineering Angriff benötigt. Hierbei werden die zugrundeliegenden Eigenschaften menschlichen Verhaltens detaillierter beschrieben als in [HaPr09] und im Modell verankert. Im Social Engineering Angriffsmodell werden die verschiedenen Schritte der Informationsbeschaffung eines Social Engineers dargestellt.

[Unbe01] Der Autor fokussiert beim Schutz vor Social Engineering Angriffe primär auf die Notwendigkeit von Policies. Diese sollen unter anderem Regelungen zur Datenvernichtung gegen Dumpster Diving, physische Sicherheitsmaßnahmen gegen unbefugtes Betreten, Mitarbeiterausweise zur eindeutigen Identifikation usw. abdecken. Damit die Policies wirksam werden, müssen sie den Mitarbeitern durch

Sicherheitsschulungen bewusst werden. In [Unbe01] spricht der Autor von der Erziehung der Mitarbeiter vor der Gefahr durch Social Engineering Angriffen. Im Zentrum stehen hierbei menschliche Sicherheitsmaßnahmen.

[Kee08] Der Autor unterteilt Social Engineering Angriffe in jene, die übers Telefon, über das Internet, durch Dumpster Diving, durch Shoulder Surfing, durch Reverse Social Engineering und durch persönliche Überredung durchgeführt werden. Zu jeder Kategorie werden Gegenmaßnahmen anhand von Fallbeispielen erläutert, wobei der Fokus auf Prozeduren und Richtlinien liegt.

[ScMi08] Der Artikel argumentiert, dass die Social Engineering Schwachstelle nicht in der Technologie liegt, sondern im menschlichen Verhalten. Der Autor beschreibt, wie durch Schulungsmaßnahmen die Mitarbeiter Social Engineering Angriffe abblocken und sogar erkennen können, ähnlich einer Firewall.

[TaCl10] Schulungsprogramme zur Erhöhung des Sicherheitsbewusstseins finden vor allem im Arbeitsumfeld statt. Der Artikel beleuchtet den Zusammenhang zwischen dem Sicherheitsbewusstsein im beruflichen Kontext zu jenem im privaten. Herausgefunden wurde, dass Mitarbeiter zumeist sehr motiviert und interessiert an Sicherheitsschulungen sind. Nachgewiesen wurde ebenso, dass an die Mitarbeiter in der Arbeit vermittelten Sicherheitsmaßnahmen von diesen auch privat aufgegriffen wurden. Als eine Konsequenz dieses erfolgreichen Bereichswechsels schlagen die Autoren vor, nicht unternehmensspezifische, sondern umfassende Sicherheitsmaßnahmen zu vermitteln. Dadurch könnte eine unternehmens- und bereichsübergreifende Sicherheitskultur entstehen.

[Tian07] In der Arbeit wird referenzierend auf [DeSt85] festgehalten, dass Menschen sehr schlecht im Entlarven von Lügen sind. Der Prozentsatz entdeckter Unwahrheiten liegt lediglich bei 45% bis 65% bei einer statistischen Wahrscheinlichkeit von 50%. Zum Erkennen von Social Engineering Attacken wird eine Methode vorgestellt, die auf Bewertung der Kommunikation beruht. Hierbei werden verschiedene Kriterien herangezogen, wie etwa die Redezeit des Angreifers

im Vergleich zu der des Mitarbeiters, die Anzahl der Sprachpausen des Angreifers usw. Der Mitarbeiter soll dabei unterstützt werden, zu erkennen, ob es sich um Lügen handelt. Durch Experimente konnte der Autor nachweisen, dass diese Methode einen positiven Einfluss auf das Erkennen von Social Engineering Angriffen hat.

[NyHo07] Ubiquitous Computing wird in [NyHo07] als die nächste Entwicklungsgeneration von vernetzten Systemen angesehen. Neue Möglichkeiten bieten aber für einen Social Engineer auch neue Angriffsvektoren. Die Autoren identifizieren drei bekannte Social Engineering Methoden, die bei Ubiquitous Computing eine Rolle spielen – Diebstahl von mobilen Geräten, Shoulder Surfing und Network Monitoring. Als neu wird die Möglichkeit von Signal Hijacking angesehen, da durch Ubiquitous Computing mehr Geräte miteinander kommunizieren. Die neue Gefahr von Digital Dumpster Diving unterscheidet sich vom Dumpster Diving dadurch, dass nicht sensible Dokumente im Abfall gesucht werden, sondern der digitale Inhalt von weggeworfenen Geräten vom Social Engineer gesichtet wird. Denial of Service Attacken sind nicht mehr auf Provider gerichtet, sondern können auch gezielt gegen Menschen eingesetzt werden. Zuletzt identifizieren die Autoren eine neue Art von Phishing.

Systemische Sicherheit zeichnet sich durch eine Kombination von menschlichen, technischen und organisatorischen Sicherheitsmaßnahmen im prozessorientierten Kontext aus. Das multi-dimensionale Modell wird in [KeBe06] vorgestellt und diskutiert.

[Klai10] In [Klai10] werden aktuelle Entwicklungen der Informationssicherheit identifiziert und analysiert. Moderne Sicherheitsmodelle zeichnen sich demnach durch ein multidimensionales Konzept aus. Die einzelnen Domänen stehen in Wechselwirkung miteinander. Im Gegensatz zu traditionellen Sicherheitskonzepten werden zusätzliche Faktoren berücksichtigt, wie beispielsweise die Unternehmenskultur. In [Klai10] wird auf [KiBe06] als ein modernes Informationssicherheitsmodell verwiesen.

[KiBe06] Das im Artikel vorgestellte Systemic Security Management Model beinhaltet die drei Eckpfeiler traditioneller Modelle – „Menschen“ (Personal), „Prozesse“ und „Technologie“. Zusätzlich wird der vierte Eckpfeiler, jener der „Organisation, Design und Strategie“, hinzugefügt, wodurch ein drei dimensionales Modell in Form einer Pyramide entsteht.

[Mann08] In [Mann08] wird das Social Engineering Model of Protection beschrieben. Grundsätzlicher Gedanke ist, dass die schützenswerte Information von verschiedenen Verteidigungsringen umgeben ist. Ein Angreifer muss sämtliche überwinden, um Zugriff auf die Daten zu bekommen. Die Ringe sind unterschiedlichen Bereichen zugeordnet, was dem Ansatz eines systemischen Sicherheitsmodells entspricht. Das Social Engineering Model of Protection wird im Zuge dieser Arbeit um das systemische Modell von [KiBe06] ergänzt.

In der Arbeit soll analysiert werden, ob ITIL eine geeignete Methode gegen Social Engineering darstellt. Dazu muss auch gezeigt werden, dass ITIL als Rahmenwerk gegen Angriffe eines Social Engineers in eine unternehmensweite Information Security Governance integrierbar ist.

[WePo06] In dieser Arbeit werden verschiedene Definitionen von IT-Governance in der Literatur recherchiert, miteinander verglichen, Widersprüche identifiziert und eine gemeinsame Sichtweise erarbeitet.

[ZhYu11] Der Artikel analysiert die Faktoren von Information Security und deren interne Wechselwirkung zu Risiken. Dabei fokussieren die Autoren auf die Kontrollprozesse, den Schutz der Ressourcen und auf die Zielerfüllung der Sicherheitsvorgaben. Aufgespannt wird ein drei dimensionales Modell aus IT-Governance, Process-Resource-Security-Information Security und Management and Control System in IT-Governance.

[LePi10] Die konkrete Umsetzung von IT-Governance im Bankensektor wird in [LePi10] analysiert. Hierbei werden in einem ersten Schritt COBIT Prozesse identifiziert, welche die

Anforderungen von BASEL II erfüllen. Anschließend werden weitere Rahmenwerke, wie etwa RISK IT, VAL IT, ISO 27002 und ITIL, berücksichtigt. Ergebnis ist ein IT-Governance Modell für Banken.

[HeYe08] Als weiteres Anwendungsbeispiel wird in [HeYe08] COBIT bei einem universitären EAP System eingesetzt. Nach der Komponentenbeschreibung von IT-Governance werden die Realisierungsschritte erläutert. Ein EAP System einer Universität wird beschrieben und eine IT-Governance Strategie wird vorgeschlagen.

[Gette07] Am Fallbeispiel der United States Capitol Police wird die Einführung und Etablierung einer Unternehmensarchitektur und IT-Governance analysiert. Ein Prozess wird etabliert, der Technologie und Geschäftsanforderungen verbindet. Die Geschäftsanforderungen werden durch die Unternehmensziele und -prioritäten bestimmt.

Die Betrachtung der wissenschaftlichen Landschaft verdeutlicht die vielseitige Beleuchtung in verschiedenen Arbeiten der Forschungsbereiche IT-Security und Social Engineering. Neu in dieser Arbeit ist die Analyse von ITIL als Rahmenwerk eines systemischen Sicherheitsansatzes gegen Social Engineering. Dabei werden unter Berücksichtigung des aktuellen Forschungstands von IT-Security und Social Engineering im Best-Practice Rahmenwerk ITIL Sicherheitsmechanismen identifiziert, klassifiziert und in ein Sicherheitsmodell eingebettet.

## 1.5 Aufbau der Arbeit

Einleitend wird das Thema Sicherheit und Informationssicherheit beleuchtet. Die Grundlagen zur eigentlichen Analyse werden mit einer Einführung in die Konzepte von ITIL abgeschlossen.

Anschließend werden Maßnahmenempfehlungen gegen Social Engineering entwickelt. Das gewählte Vorgehensmodell basiert auf den klassischen Methoden des Engineerings und durchläuft die drei Schritte Analyse, Design und Konstruktion, welche sich im Aufbau der Arbeit wiederspiegeln.

Analysephase: Der erste Schritt der Analyse ist die Erläuterung der Begrifflichkeit des Social Engineering als klare Abgrenzung der Arbeit. Des Weiteren werden Angriffsmethoden und Techniken von Social Engineering identifiziert sowie der Angreifer und seine Angriffsmethoden analysiert, um daraus das Gefahrenpotential abzuleiten und darzustellen. Anschließend werden die Prinzipien von ITIL wiedergegeben und untersucht, welche Sicherheitsmechanismen unter welchen Voraussetzungen Social Engineering Attacken entgegenwirken. Hierbei wird unterschieden zwischen Mechanismen, welche Tätigkeiten von manipulierbaren Menschen auf technische Verfahren abbilden, Mechanismen, welche den Menschen unterstützen sollen, Social Engineering Angriffe zu erkennen und zu beheben, sowie Mechanismen zur Angriffsanalyse.

Design Phase: Eine Auflistung konkreter Maßnahmenempfehlungen zur Absicherung vor Attacken eines Social Engineers, welche in den Service Operation Prozessen von ITIL eingebettet werden können, wird in Form von Tabellen übersichtlich und wiederverwendbar wiedergegeben. Diese Tabellen stellen eine kompakte Zusammenfassung der erarbeiteten Maßnahmen basierend auf Best Practices, Guidelines, allgemein gültigen Normen und Grundsätzen sowie wissenschaftlichen Grundlagen dar.

Konstruktionsphase: Zur besseren Veranschaulichung werden in der Arbeit mehrere Fallbeispiele behandelt. In den Beispielen wurde ITIL auch zur Verstärkung der Sicherheit vor Social Engineering eingesetzt. Die Ergebnisse und Erfahrungen, die sich daraus ergeben haben, werden unter verschiedenen Gesichtspunkten analysiert und unterstreichen die Anwendbarkeit der in der Arbeit dargelegten Grundsätze.

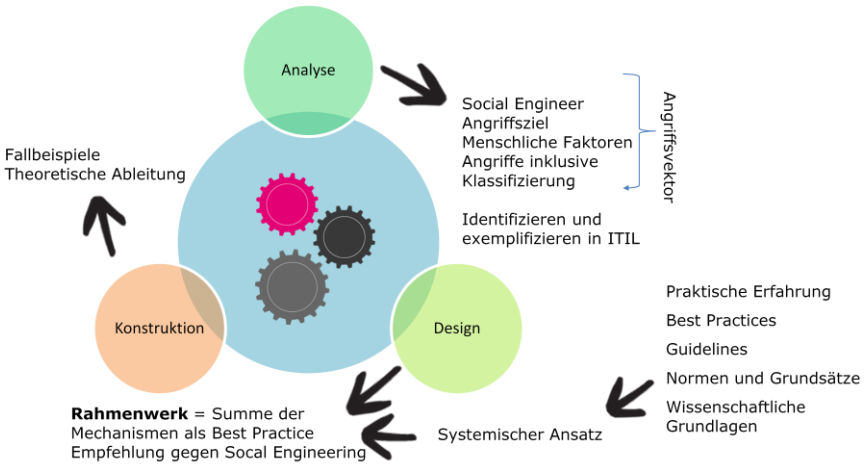



**Abbildung 5: Vorgehensmodell basierend auf Engineering Methoden**

Um den Kreislauf des Vorgehensmodells zu schließen, folgt nach der Konstruktionsphase wieder eine Analysephase. Hierbei wird gezeigt, dass die Best Practice Ansätze von ITIL sowohl die systematischen und organisatorischen als auch die menschlichen Sicherheitsmechanismen stärken und damit effektiv Social Engineering Attacken entgegenwirken.

Abschließend werden Social Engineering Angriffsmöglichkeiten identifiziert und analysiert, die durch ITIL nicht abgesichert werden. Zusätzlich wird die Möglichkeit analysiert, ob durch die Einführung von ITIL Prozessen in Unternehmen neue Social Engineering Angriffsvektoren entstehen. Dies wird durch die Methode einer klassischen Restrisikoanalyse umgesetzt.

# 2 Grundlagen

## 2.1 Sicherheit

Im deutschen Sprachgebrauch wird das Wort „Sicherheit“ im Wesentlichen mit zwei Dingen verbunden. Zum einen verbindet man damit Stabilität, also die Unempfindlichkeit eines Systems gegenüber Einflüssen, die nicht absichtlich herbeigeführt werden, wie zum Beispiel Feuer oder Fehleingaben des Benutzers. Zum anderen wird mit Sicherheit auch der Schutz gegen gezielte und böswillige Angriffe auf ein System bezeichnet. Diese beiden Bedeutungen werden im englischen Sprachgebrauch mit zwei verschiedenen Begriffen ausgedrückt: *safety* und *security*.

Die beiden Aspekte beeinflussen einander. So kann zum Beispiel ein Angreifer die Stabilität des Systems gefährden. Umgekehrt kann auch mangelnde Stabilität eines Systems erst einen Angriff möglich machen.

## 2.2 Systeme

Admiral Grace Hopper: „*Life was simple before World War II. After that, we had Systems.*“

Wir alle benutzen jeden Tag Maschinen und Systeme. Aber was zeichnet eigentlich Systeme gegenüber Maschinen aus? Wann spricht man von Maschinen, wann von Systemen und warum ist diese Unterscheidung relevant?

Ein Temperaturmessgerät ist eine Maschine, die es einem ermöglicht, die aktuelle Raumtemperatur zu messen. Integriert man diese Maschine in die Zentralheizung eines Hauses, so spricht man von einem System. Das Temperaturmessgerät misst die aktuelle Raumtemperatur und übermittelt sie einer Steuereinheit, welche die Leistung der Zentralheizung reguliert.

Das heißt, ein wesentliches Merkmal von Systemen gegenüber Maschinen sind nicht triviale Abhängigkeiten zwischen Maschinen und in weiterer Folge Systemen selbst. Systeme zeichnen sich durch komplexe Interaktionsmuster aus, die zur Schaffung immer größerer Systeme gebildet werden müssen [Schn01].

Betrachtet man das Internet, also die Vernetzung und Interaktion von Millionen Computern, so kann man von dem komplexesten Konstrukt

sprechen, welches je von Menschen entworfen wurde. Der Technologietrend zeigt eindeutig in Richtung einer umfassenden Informatisierung der Welt [FrLa03].

Je komplexer die Kommunikationsmuster und je vielfältiger die Akteure sind, umso öfter trifft noch ein weiteres Merkmal von Systemen in den Vordergrund. Unter emergenten Merkmalen versteht man, dass Systeme Dinge bewirken, die ursprünglich vom Entwickler nicht geplant wurden [Schn01]. So wurde zum Beispiel das Telefon von Alexander Graham Bell ursprünglich dazu konzipiert, um das Eintreffen eines Telegramms vorab anzukündigen. Er hatte nicht die Vorstellung, dass ein Telefon ein persönliches Kommunikationsmedium sein könnte und welche Auswirkungen es auf unsere heutige Gesellschaft hat.

Auch der Vorläufer des Internets wurde in den 60er-Jahren vom amerikanischen Verteidigungsministerium entwickelt, um Daten zwischen Computern trotz eines Atomangriffes austauschen zu können. Die heutigen Einsatzmöglichkeiten wie zum Beispiel E-Commerce, Telebanking, Voice over IP, Virtual Sex, Telearbeit, E-Voting, etc. haben die damaligen Benutzer und Entwickler nicht erahnen können.

Eine wichtige Eigenschaft von Systemen gegenüber Maschinen ist, dass sie Bugs haben. Das heißt, im Gegensatz zu einer Fehlfunktion, wo eine Maschine dann schlicht und einfach nicht mehr richtig funktioniert, verhält sich das System bei einem Bug auf eine bestimmte – möglicherweise unerklärliche oder einmalige – Weise falsch. Bei einem Bug könnte man von einem unerwünschten emergenten Merkmal sprechen. Maschinen gehen kaputt oder funktionieren nicht mehr, aber nur ein System kann einen Bug haben [Schn01].

## 2.3 Systeme und Sicherheit

Anhand der Merkmale von Systemen kann man leicht erkennen, warum es so schwierig, vielleicht mit den bisher bekannten Mitteln sogar unmöglich ist, Systeme sicher zu gestalten.

**Systeme sind komplex**: Statistisch gesehen schleicht sich alle 1000 Programmzeilen ein schwerer Fehler ein. Betrachtet man nun die Weiterentwicklung des Betriebssystems Windows, so bestand Windows 98 aus ca. 18 Millionen Codezeilen. Windows Vista hingegen hat ungefähr 60 Millionen Codezeilen. Die Tendenz zur Komplexität im Quellcode macht es unmöglich, ein fehlerfreies und sicheres Programm zu implementieren.

**Systeme interagieren**: Betrachten wir das vorige Beispiel mit dem Temperaturmessgerät und der Zentralheizung. Liefert nun das Messgerät auf Grund eines defekten Fühlers falsche Daten, so funktioniert die gesamte Zentralheizung nicht mehr richtig. Das heißt, wegen der starken Vernetzung und Interaktion zwischen vielen Komponenten kann sich ein Fehler einer kleinen, vermeintlich unbedeutenden Komponente rasch ausbreiten und schwerwiegende Folgen für das gesamte System haben.

**Systeme haben emergente Eigenschaften**: Bei der Entwicklung des Internets in den 60er-Jahren hat niemand die heutigen Anwendungsbereiche bedacht. Aus einem militärischen, vor Atomangriffen sicheren und vor allem abgeschlossenen Datennetzwerk ist das weltweit größte Kommunikationsnetz entstanden. So ist das Internet zum Beispiel nie für eCommerce Anwendungen konzipiert worden. Die damals getroffenen Designentscheidungen verursachen jetzt viele sicherheitstechnische Probleme.

**Systeme haben Bugs**: Einige Programmierschwächen im Microsoft Remote Procedure Call (RPC) Interface erlauben es Angreifern, auf das betroffene System ein Backdoor mit administrativen Rechten zu kreieren. Betroffen sind davon sämtliche Windows NT, Windows 2000, Windows XP und Windows Server 2003 Betriebssysteme [Cert03].

Angesichts dieser Tatsachen zeigt es sich, dass es mit den heutigen Mitteln unmöglich ist, ein System vollkommen abzusichern. Das ist aber auch gar nicht notwendig. Ein nicht vernetzter Heimcomputer, der nur selten zum Solitär spielen verwendet wird, muss ganz anderen Sicherheitsanforderungen genügen, als zum Beispiel ein Datenbankserver in einem großen Firmennetzwerk, der maximal eine Stunde im Jahr ausfallen darf und sehr sensible Daten verwaltet. Man muss also untersuchen, welche Sicherheitsbedürfnisse an Systeme gestellt werden. Diese werden vom Umfeld des Systems bestimmt.

## 2.4 Daten, Information und Wissen

Um in weiterer Folge Informationssicherheit näher beleuchten zu können, müssen zunächst die darin zugrundeliegenden Begrifflichkeiten „Daten“, „Information“ und „Wissen“ behandelt und voneinander abgegrenzt werden.

In der Literatur gibt es unterschiedlichste Ansätze zur Begriffsbestimmung. So werden in [Kams77] Daten und Information unterschieden durch das kontextlose Wesen von Daten. Information hingegen kennzeichnet ein

Verhältnis zwischen wechselwirkenden strukturierten Systemen. Sie bezieht sich auf die jeweiligen Besonderheiten der miteinander wechselwirkenden Strukturen, wenn dadurch ein neuer sogenannter Strukturbereich (in [Gelb03] als „neue Botschaft“ bezeichnet) entsteht.

In DIN ISO/IEC 2382 [ISO98] werden Daten als Gebilde aus Zeichen oder kontinuierliche Funktionen definiert, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen, vorrangig zum Zwecke der Verarbeitung und als deren Ergebnis.

Vereinfachend lässt sich festhalten, dass Informationen durch eine kontextbezogene Interpretation von Daten entstehen. Werden diese Informationen bewertet und mit weiteren Informationen vernetzt, entsteht nach [Diem08] Wissen. Dieser Sachverhalt wird in Abbildung 6 in Anlehnung an [FiSc05] dargestellt.

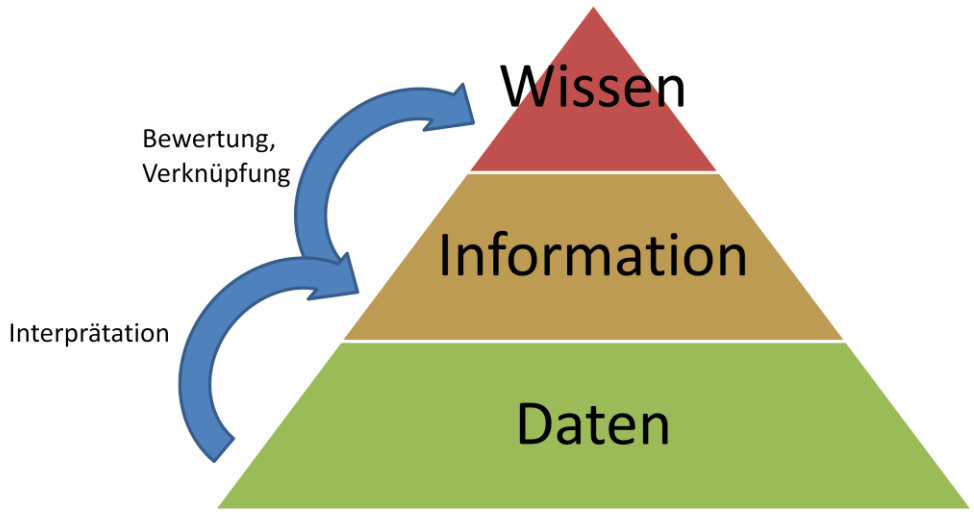



**Abbildung 6: Daten, Information, Wissen, in Anlehnung an [FiSc05]**

In [ReMu00] wird Wissen als eine bedeutungsvolle Vernetzung von Informationen bezeichnet. [Herb00] ergänzt dies um die Aussage, dass Wissen das Netz aus Kenntnissen, Fähigkeiten und Fertigkeiten, die jemand zum Lösen einer Aufgabe einsetzt, darstellt. Jedenfalls ist Wissen mehr als eine Sammlung von Daten oder Information. Wissen ist die Anwendung von kontext- und beziehungsspezifischer Information, welche die Voraussetzung für menschliches Planen und Handeln ist. Neues Wissen entsteht auch nicht primär durch zusätzliche Information, sondern durch Verkettung und Vernetzung von bestehendem Wissen, durch Bewertung, Entscheidungen

und Reflexion. Die folgende Tabelle fasst die Abgrenzung von Daten, Information und Wissen in Anlehnung an [Gelb03] zusammen.

| Daten | Information | Wissen |
|---|---|---|
| 0-dimensional | 1-dimensional | 2-dimensional |
| Angabe ohne Auswahl oder Verknüpfung | Resultiert aus Auswahl bzw. aus Verknüpfung | Kontext- und beziehungsspezifische Information<br><br>Menschliche Fähigkeit zu entscheiden und zu planen |
| Beispiel: Meise, blau | Beispiel: die neue Botschaft: „Alle Meisen sind blau“ | |

**Tabelle 1: Abgrenzung von Daten, Information und Wissen [Gelb03]**

Neben der philosophischen Sichtweise ist auch die rechtliche besonders zu beachten. Hierfür wird in der derzeit geltenden Fassung des Österreichischen Datenschutzgesetzes [Oest00] die Begrifflichkeit der Daten detailliert festgehalten, wobei im Speziellen personenbezogene und sensible Daten behandelt und eindeutig bestimmt werden.

„Daten" („personenbezogene Daten"): Angaben über Betroffene, deren Identität bestimmt oder bestimmbar 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.

„Sensible Daten" („besonders schutzwürdige Daten"): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.

## 2.5 Informationssicherheit

Sicherheitsdienste sind Funktionen, die ein System bereitstellen muss, um die Sicherheitsbedürfnisse seiner Benutzer zu entsprechen. Systeme, die Gebrauch von offenen und somit von jedermann zugänglichen Netzwerken

machen, müssen entsprechend [MRSI02] grundsätzlich für ein gewisses Maß an Vertraulichkeit, Integrität und Verfügbarkeit sorgen.

Betrachtet man die Entwicklung der im Internet bereitgestellten Dienste, so lässt sich ein starker Trend weg von Nutzung als reines Informationsinstrument hin zu kommerziellen Angeboten feststellen. Ob Home- Banking, Internet- Einkaufszentrum oder Online-Reservierungssystem, geschäftliche Transaktionen werden zunehmend über das Kommunikationsmedium abgewickelt und stellen über die genannten Grundbedrohungen hinaus weitere Sicherheitsanforderungen. [MRSI02]

Sicherheitsbedürfnisse werden zumeist als implizite Anforderungen an Systeme gesellt. Meist erst durch Verletzung einer dieser Anforderungen im laufenden Betrieb entsteht bei Anwendern und Entwicklern das Bewusstsein über deren Notwendigkeit.

### 2.5.1 Sicherheitsbedürfnisse

Folgend werden eine Reihe gängiger Sicherheitsbedürfnisse wie Verfügbarkeit, Integrität, Verbindlichkeit, Überprüfbarkeit, Vertraulichkeit und Anonymität vorgestellt, welche anschließend den Dimensionen von Informationssicherheit zugeordnet werden.

#### *Verfügbarkeit*

Für Benutzer ist es wichtig, dass wann immer sie eine bestimmte Anwendung brauchen, diese zur Verfügung steht und funktioniert. Sollte das nicht der Fall sein, so muss der Systemadministrator dafür sorgen, dass sie innerhalb einer bestimmten Zeit repariert ist. Die zur Verfügung stehende maximale Reparaturzeit ist zumeist bestimmt durch Wartungsverträge oder fixe Fristen, welche die Benutzer der Anwendung einhalten müssen.

Für Sicherheitsexperten heißt Verfügbarkeit auch Fehlertoleranz und Ausfallsicherheit. Der Ausfall eines Teilsystems sollte nicht das Gesamtsystem beeinflussen. Des Weiteren sollte bei einem Ausfall ein anderes System die Funktionalität des beschädigten Systems während dessen Reparaturzeit übernehmen. [BSI08]

Natürlich ist eine ausfallsichere Implementierung eines Systems sehr kostenintensiv. Daher ist für jede Anwendung besonders wichtig, die

Anforderungen an die Verfügbarkeit zu kennen, um daraus den tatsächlichen Schutzbedarf ableiten zu können. [BSI08]

### *Integrität*

Integrität bezeichnet die Korrektheit, Manipulationsfreiheit und Unversehrtheit von Daten und Informationen. Integrität wird teilweise von Sicherheitsmaßnahmen wie Checksummen, Einwegfunktionen und asymmetrischen Verschlüsselungsverfahren gewährleistet.

Oftmals wird Integrität mit dem Bereich der Authentifikation verwechselt. Während sich die Authentifikation mit dem Ursprung der Daten beschäftigt, also mit der Frage, wer diese Daten verfasst hat, behandelt die Integrität die Gültigkeit der Daten. Sie beschäftigt sich nur damit, ob die Daten nach der Erstellung verändert wurden. [Schn01]

Die Schutzbedürfnisse Verfügbarkeit, Vertraulichkeit und Integrität werden in der Literatur (vgl. [RaPf96], [ZSI89]) als die klassischen Schutzziele der Informationssicherheit genannt.

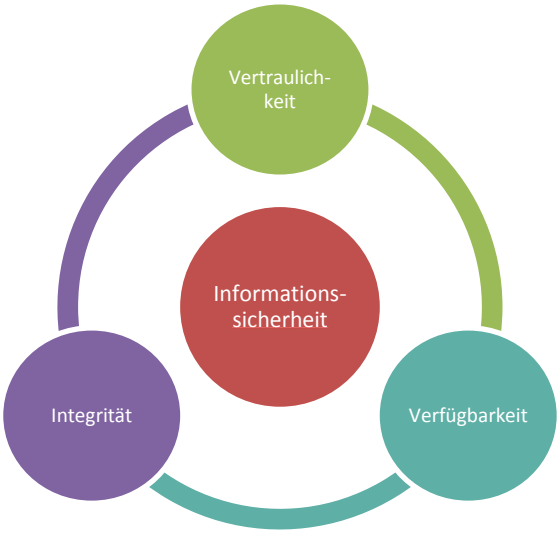



**Abbildung 7: Verfügbarkeit - Vertraulichkeit – Integrität [RaPf96] [ZSI89]**

Der Begriff der mehrseitigen Sicherheit (vgl. [Chau87], [RaPf96]) wurde geprägt, da der Begriff „Betroffener“ auf keinen Fall zu eng auf den eigentlichen Benutzer ausgelegt werden darf. IT-Sicherheit und deren abgeleitete Schutzbedürfnisse werden nicht nur von den Anwendern gefordert, sondern mit gleichem Recht auch von Entwicklern, Herstellern, Systembetreibern, von der Rechtsprechung und vielen anderen mehr, die

von der Verlässlichkeit und Beherrschbarkeit der Informations- und Kommunikationssysteme in vielfältiger Weise abhängig sind. [Diers01] Betroffen kann eine Person (natürliche oder juristische) sein, eine Personengruppe, ebenso aber auch ein anderes „System" im weiteren Sinn des Begriffs IT-System. Informationssicherheit muss deshalb in weiterer Folge mehrseitig, d.h. aus der Sicht der verschiedenen Gruppen von Betroffenen beleuchtet werden.

### *Verbindlichkeit*

Überall dort, wo juristische Rahmenbedingungen eine Rolle spielen, wie zum Beispiel bei der Aufgabe einer Bestellung oder Überweisung einer Rechnung, muss eine rechtsverbindliche Kommunikation sichergestellt werden. Solange man mit einem Medium wie Papier arbeitet, das den Inhalt eines Dokumentes untrennbar mit einer Unterschrift verbindet, ist die Rechtsverbindlichkeit weitestgehend sichergestellt und juristisch anerkannt. Der Unterschreibende erklärt sich mit dem Inhalt des Dokumentes einverstanden. Insbesondere im elektronischen Handel muss ein vergleichbarer Sicherheitsdienst zur Verfügung gestellt werden. Im Streitfall muss der Händler dem Käufer nachweisen können, dass nur er und kein anderer eine Bestellung in Auftrag gegeben hat. Andererseits darf der Händler bei Lieferschwierigkeiten auch nicht den Erhalt der Bestellung leugnen. Daraus leitet sich die Forderung nach Verfahren ab, die einen zweifelsfreien Zusammenhang zwischen den ursprünglichen Daten und der Person herstellen, die diese gesendet bzw. empfangen hat. [Raep01]

### *Überprüfbarkeit*

1497 wurde das Konzept der doppelten Buchführung von Luca Pacioli [Paci94] erstmals beschrieben. Es beruht darauf, dass sich jede Transaktion auf zwei oder mehr Konten auswirkt. Ein Konto wird mit einem Betrag belastet, der einem anderen Konto wiederum gutgeschrieben wird. Eine Transaktion ist daher ein Transfer zwischen zwei Konten mit unterschiedlichen Vorzeichen. Die Summe aller Konten muss immer Null ergeben.

Durch das System der doppelten Buchführung werden zwei wichtige Anforderungen erfüllt. Die beiden Bücher werden von verschiedenen Buchhaltern geführt. Durch routinemäßige Kontrolle der beiden Bücher können Betrugsversuche oder simple Rechenfehler aufgedeckt werden.

Bei Systemen ist das Sicherheitsbedürfnis der Überprüfbarkeit in vielen sensiblen Bereichen ebenfalls integriert. So haben Banken, Gefängnisse, Atomraketensilos, Flughäfen uvm. komplexe und umfassende Prüfanforderungen. Dabei ist die Prüfung von Computerdaten weitaus schwieriger als jene von Rechnungsbüchern, da es sehr leicht ist, Dateien zu verändern oder zu löschen. [Schn01]

### *Vertraulichkeit*

Unter Vertraulichkeit versteht man, dass nur ein eingeschränkter Personenkreis Zugriff auf bestimmte Daten hat. Diese Sicherheitsanforderung wird zumeist durch Dateizugriffsrechte gewährleistet. Dabei wird für jede Datei definiert, welcher Benutzer darauf zugreifen darf. Allen anderen Benutzer wird der Zugriff verwehrt.

Ein weiterer Schutzmechanismus für die Bewahrung der Vertraulichkeit stellt die Kryptographie dar. Vor allem während des Transfers von vertrauenswürdigen Daten über potentiell unsichere Leitungen wie zum Beispiel das Internet wird auf Transferprotokolle zurückgegriffen, die mittels kryptographischer Algorithmen die Daten vor Angreifern schützen. [Sing01]

Ein besonderer Stellenwert spielt die Vertraulichkeit bei personenbezogenen Daten, wie in Kapitel 2.4 spezifiziert. Während in den USA personenbezogene Daten den Unternehmen gehören, die diese gesammelt haben, ist der Umgang mit personenbezogenen Daten innerhalb der EU weitaus strenger geregelt. Siehe dazu [Euro95], [Franc97] und [Oest00]:

**Offenheit**: Es darf keine nicht öffentlich bekannten Computersysteme geben, in denen Individualdaten gespeichert werden.

**Individuelle Mitbestimmung**: Jeder darf alle über ihn gespeicherten Daten einsehen, kopieren und korrigieren.

**Umfangsbeschränkung**: Eine Organisation darf nur im Rahmen ihres Bedarfes Informationen über Personen speichern.

**Beschränkung von Gebrauch und Veröffentlichung**: Daten dürfen nur zu dem Zweck gebraucht und veröffentlicht werden, der bei der Erhebung explizit angegeben wurde.

**Haftung**: Die Organisation verpflichtet sich, die allgemeinen Prinzipien der Sicherheit anzuwenden und haftet für auftretende Missbräuche.

### *Anonymität*

Anonymität im Internet ist ein viel diskutiertes Thema. Ohne Anonymität wäre unser soziales Leben stark eingeschränkt.

Soziale Anonymität ermöglicht es Menschen, über Dinge zu sprechen, über die sie ansonsten nicht sprechen würden. Im Internet gibt es viele anonyme Selbsthilfegruppen und Diskussionsforen zu Krankheiten und Lebenskrisen. Auch die politische Anonymität darf nicht vernachlässigt werden. In einigen Ländern kann eine regierungsfeindliche Äußerung in einem Diskussionsforum lebensgefährlich sein. Unter dem Schutzmantel der Anonymität war es zum Beispiel Kosovaren und Serben während des Kosovokrieges 1999 möglich, Nachrichten über den Konflikt dem Rest der Welt zu senden. [Schn01]

Auf der andern Seite kann Anonymität ausgenützt werden, Personen zu belästigen, zu beleidigen oder zu bedrohen. Unter dem Schutz der Anonymität ist es viel schwieriger, kriminelle Machenschaften, wie zum Beispiel das Verbreiten von Viren, aufzudecken.

Schwierig wird der Aspekt der Anonymität bezüglich elektronischer Zahlungen. Während man im normalen Leben bei einem Bargeldeinkauf seine Anonymität gegenüber dem Verkäufer wahrt, ist das im Online-Bereich weitaus schwieriger. Bei einer Zahlung mit Kreditkarte erfährt der Verkäufer die Identität des Käufers. Des Weiteren könnte auch die Kreditkartenfirma eine Akte über die Kaufgewohnheiten des Kreditkarteninhabers anlegen. [Henni98]

### *Authentifikation*

Im täglichen Leben durchlaufen wir ständig Authentifikationsprozesse. Wenn wir jemanden anrufen und er sich mit seinem Namen meldet, vergleichen wir dessen Stimme mit jener, die wir in unserer Erinnerung gespeichert haben. So können wir herausfinden, ob wir tatsächlich mit der Person telefonieren, für die sie sich ausgegeben hat.

In ähnlicher Weise durchlaufen auch Computersysteme Authentifikationsprozesse. Wenn man sich an seinem Arbeitscomputer anmelden möchte, identifiziert man sich zuerst mit der Eingabe seines Benutzernamens, danach authentifiziert man sich durch die Eingabe des geheimen Passwortes, welches nur einem selbst bekannt sein sollte. [Schn01]

Passwortabfragen sind die gängigste Authentifikation. Das Einlesen von biometrischen Daten wie zum Beispiel von Fingerabdrücken wäre auch eine denkbare Variante, scheitert aber zumeist an den zusätzlichen Kosten für Lesegeräte und der zu häufig auftretenden falschen positiven oder negativen Authentifizierungen. Des Weiteren können Passwörter, die während des Datentransfers von einem Angreifer abgefangen worden und daher in Zukunft sicherheitstechnisch unbrauchbar sind, geändert werden, biometrische Daten hingegen nicht.

In [Diem08] wird in Anlehnung an [Diers01] eine strukturelle Einteilung der Schutzziele getroffen und visuell dargestellt. Hierbei werden die klassischen Schutzbedürfnisse – Vertraulichkeit, Integrität und Verfügbarkeit – dem Bereich der Verlässlichkeit (Sicherheit des Systems), die weiteren Schutzbedürfnisse – Verbindlichkeit, Überprüfbarkeit usw. – der Beherrschbarkeit unter Berücksichtigung der folgenden Abgrenzung zugeordnet. Die Einteilung spiegelt die Forderung der mehrseitigen Betrachtungsweise von Informationssicherheit und der zugrundeliegenden Schutzbedürfnisse wider.

**Verlässlichkeit** ist jene Sachlage, bei der weder die Systeme noch die mit ihnen verarbeiteten Daten und Informationen, noch die Datenverarbeitung (Funktionen und Prozesse) in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit unzulässig beeinträchtigt werden.

Unter **Beherrschbarkeit** (Sicherheit der Betroffenen) versteht man jene Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von Systemen nicht unzulässig beeinträchtigt werden.

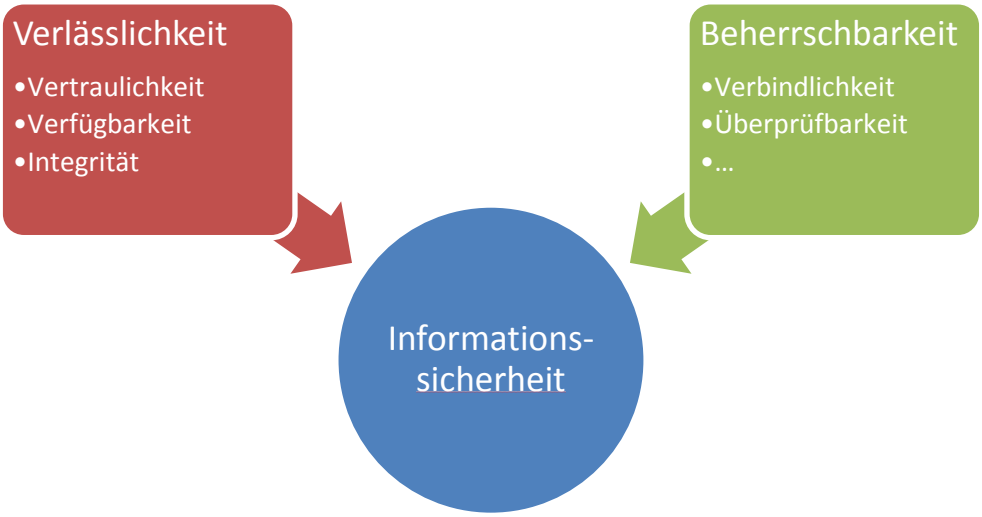



**Abbildung 8: Dimensionen von Informationssicherheit [Diem08]**

### 2.5.2 Standards für Informationssicherheit

Es gab bereits viele Bemühungen, Sicherheit zu messen und zu gewährleisten. Die Bewertungskriterien von Sicherheit hatten allerdings in verschiedenen Ländern unterschiedliche Zielsetzungen, wodurch es keine einheitlichen Standards gab. Die wichtigsten Kriterien waren die Trusted Computer System Evaluation Criteria (TCSEC) [US85], die vom National Security Center 1985 in den USA herausgegeben wurde und für Produktevaluation benutzt werden konnte. Bekannt wurde das Buch durch seinen markanten orangefärbigen Einband als „Orange Book“.

Das Orange Book zum Klassifizieren von verschiedenen Ebenen der Computersicherheit und der Möglichkeit zu bestimmen, ob ein bestimmtes System eine bestimmte Ebene erreicht, war bald veraltet. Es war nur zur Bewertung einzelner Systeme gedacht. Durch die zunehmende Vernetzung wurde es daher unbrauchbar. Des Weiteren war auch die klassifizierte Sicherheitsstufe eines bestimmten Systems stark von der Einsatzumgebung, der Konfiguration und den Rahmenbedingungen abhängig, wodurch keine objektive Aussage über alle Typen dieses Systems gemacht werden konnte.

Neben dem Orange Book gab es noch viele andere Versuche, Sicherheitskriterien für die Sicherheitsbewertung von Systemen und Produkten einzuführen. So gab es in Großbritannien das CESG

Memorandum NR. 3 (CESG3) [CESG89] und das „Grüne Buch“ (DTIEC) [DTI89]. In Deutschland wurde 1989 die erste Fassung eigener Sicherheitskriterien von der Zentralstelle für Sicherheit in der Informationstechnik (jetzt Bundesamt für Sicherheit in der Informationstechnik) veröffentlicht (ZSIEC) [BSI89]. In Frankreich wurde gleichzeitig das so genannte „Blau- weiß- rote Buch“ (SCSSI) entwickelt. [Robe93]

Innerhalb der EU wurde 1998 die Information Technology Security Evaluation Criteria (ITSEC) [BSI98] erstmals verabschiedet.

Die Common Criteria [CC06] sind eine Weiterentwicklung und Harmonisierung der europäischen ITSEC, des Orange Book (TCSEC), der Federal Criteria (FC) der USA sowie der kanadischen Kriterien (CTCPEC). Sie wurde im Dezember 1999 durch die internationale Standardisierungsorganisation (ISO) [ISO] als internationale Norm ISO/IEC 15408 [ISO07] veröffentlicht.

Neben der ISO/IEC 15408 Norm gibt es noch weitere Normen, welche im Bereich der Informationssicherheit eine wichtige Rolle spielen und berücksichtigt werden müssen. In ISO/IEC TR 15446:2004 Information technology – Security techniques – Guide for the production of Protection Profiles and Security Target [ISO04] wird die Erstellung von Schutzprofilen und Sicherheitszielen analog zu und anwendbar an den Common Criteria behandelt.

ISO/IEC TR 13335 [ISO04A] stellt ein Basiswerk für Sicherheitsmanagement dar und ist Ausgangspunkt und Referenz einer Reihe weiterer Dokumente zum Sicherheitsmanagement. Behandelt werden Konzepte und Modelle der Sicherheit, Techniken für das Risikomanagement, Techniken für das Sicherheitsmanagement, Auswahl von Sicherheitsmaßnahmen und Netzwerksicherheitsmanagement. [Ayal06]

Basierend auf den in Großbritannien entwickelten BS 15000, wurde der internationale Standard ISO/IEC 20000 [ISO05] zum Servicemanagement im Dezember 2005 veröffentlicht. Der Standard besteht aus zwei Teilen. Der erste Teil behandelt die Begriffsdefinitionen, der zweite Teil die Anforderungen an Servicemanagement und Informationssicherheitsmanagementsysteme (ISMS). Der Standard umfasst sämtliche Bereiche von der Planung und Umsetzung über den Betrieb, die Überwachung, Prüfung und Instandhaltung bis hin zur kontinuierlichen Verbesserung des Systems. Bei der Einführung eines ISMS unter Anwendung des Standards ist die Ausgestaltung abhängig von den

konkreten Bedürfnissen, Zielen, Sicherheitsanforderungen sowie der Größe und Struktur des Unternehmens. [Diem08] ISO/IEC 20000 ist kompatibel zu den ITIL Prozessen und Begrifflichkeiten, welche in Kapitel 3 näher beschrieben werden.

Die internationale Norm ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements [ISO05A] spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Angewendet werden kann die ISO/IEC 27001 Norm in verschiedenen Unternehmen unterschiedlicher Branchen, wie zum Beispiel staatlichen Institutionen und Behörden, in der Industrie und in kleinen bis großen Dienstleistungsunternehmen. ISO 27001 ist eine Spezifikation, „was“ durch ein Informationsmanagementsystem erfüllt werden muss, ganz im Gegensatz zum Grundschutzkatalog, welcher Maßnahmen zum „Wie“ auflistet. [Real08]

Das Bundesamt für Sicherheit in der Informationstechnik hat das Grundschutzhandbuch, welches seit Version 2005 auf Grundschutzkatalog umbenannt wurde, publiziert und im Sicherheitsmanagement etabliert. Beim Grundschutzkatalog handelt es sich um Baustein-, Maßnahmen- und Gefährdungskataloge, welche eine umfassende Sichtweise abdecken. Behandelt werden übergeordnete Aspekte, Infrastruktur, Systeme, Netze und Anwendungen. Durch die Auflistung von standardisierten zu erfüllenden Mindestkriterien bis mittleren Schutzbedarf stellt das Grundschutzhandbuch eine kosteneffektive und praktikable Methode zur Erstellung von Sicherheitsanalysen dar. [Ehri03] [Fran07]

[Voss09] stellt in Abbildung 9 die Verkettung und Verbindungen verschiedener angeführter und zusätzlicher Standards und Normen, wie etwa IDW PS 880 – Erteilung und Verwendung von Softwarebescheinigungen [IDW99] und IDW PS 330 – Abschlussprüfung bei Einsatz von Informationstechnologie [IDW02] vom Institut der Wirtschaftsprüfer in Deutschland, dem Landesdatenschutzgesetz (LDSG) und dem Bundesdatenschutzgesetz (BDSG), dar. Ersichtlich ist die Komplexität der Abhängigkeiten innerhalb der unterschiedlichen Normen und Standards. Grund hierfür ist, dass gesetzliche Bestimmungen die Einhaltung von genormten Audits und Prüfungen vorschreiben, welche wiederum auch auf technische Sicherheitsstandards zurückgreifen, woraus sich entsprechende Verkettungen ergeben.

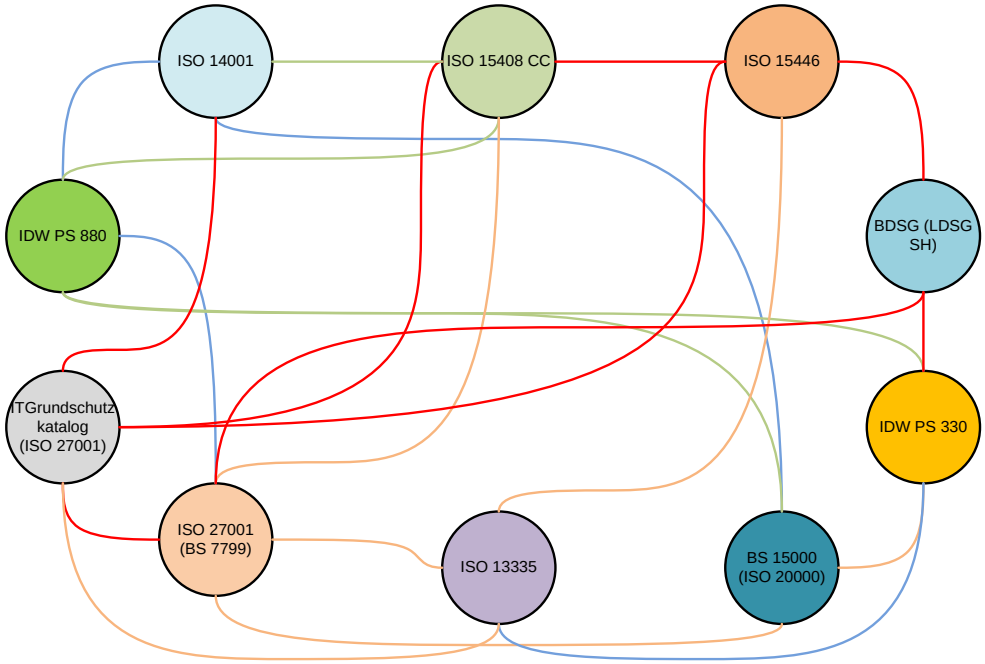



**Abbildung 9: Verkettung von Sicherheitsnormen und -standards [Voss09]**

# 3 Information Technology Infrastructure Library

Information Technology Infrastructure Library (ITIL) ist eine Sammlung an Konzepten und Empfehlungen, um Informationstechnologie (IT), Services, Development und Operations zu verknüpfen. Es handelt sich um ein Rahmenwerk, welches ein kundenorientiertes und kosteneffizientes Management von Services als Ziel hat. Die beinhalteten Methoden und Vorgehensweisen sind praxisorientiert und erprobt. Gerade die Anwendbarkeit und der Nutzen wurden wissenschaftlich in mehreren Arbeiten analysiert und festgestellt (siehe dazu [Kain08] [Hein08] [Vuci09]).

Laut [Kres05] ist ITIL ein „… herstellerunabhängige Sammlung von Best Practices, mit denen es Organisationen über einen prozessorientierten skalierbaren Ansatz ermöglicht wird, Effizienzsteigerungen innerhalb ihrer IT Prozesse zu erzielen und somit ihren Kunden einen gleichbleibenden Service zu liefern“.

[Elsa06] erweitert die Zielsetzung um die explizite Steigerung der Anwenderzufriedenheit. Des Weiteren wird genannt, dass eine höhere Professionalität des Unternehmens durch bessere Bewertung, Kontrolle und Steuerung der IT-Organisation erreicht wird. Hierbei spielen Messkriterien eine entscheidende Rolle, welche zur Bewertung und Steuerung herangezogen werden.

## 3.1 Geschichte und Entwicklung von ITIL

ITIL wurde entwickelt und federführend weiter ausgebaut vom britischen Office of Government Commerce (OGC) [OGC], welches aus der ehemaligen Regierungsstelle Central Computer and Telecommunication Agency (CCTA) hervorging. Die britische Regierung unter Margaret Thatcher war zu dem Zeitpunkt mit der Qualität der eingekauften Dienstleistungen nicht zufrieden, weshalb die damalige CCTA beauftragt wurde, Wege zur Kostenverringerung bei gleichzeitiger Qualitätssteigerung aufzuzeigen. Das Framework entstand in den 1980ern, als in Zusammenarbeit mit mehreren englischen Rechenzentren begonnen wurde, die Erfahrungen zu sammeln und zu dokumentieren. Ziel war auch, auf das rasante Wachstum der Informationstechnologie zu reagieren und in einem Nachschlagewerk die notwendigen Maßnahmen zusammenzufassen.

Nach mehreren Konsolidierungen der entstandenen einzelnen Dokumente wurde unter Government Information Technology Infrastructure Management Methology (GITMM, manchmal auch als GITIMM bezeichnet) eine Version 1989 veröffentlicht, welche als ITIL Version 1 (ITIL V1) angesehen werden kann. Im April 2001 wurde die CCTA in die OGC eingegliedert. Durch kontinuierliche Weiterentwicklung wurde nach ITIL V1 im Jahr 2006 ITIL V2 publiziert. Das ITIL V2 Framework beschreibt verschiede Prozesse, deren Inputs und Outputs, Zielsetzungen und ihr Zusammenwirken. Gegliedert ist das ITIL V2 Framework in die folgenden in Abbildung 10 dargestellten Bereiche.

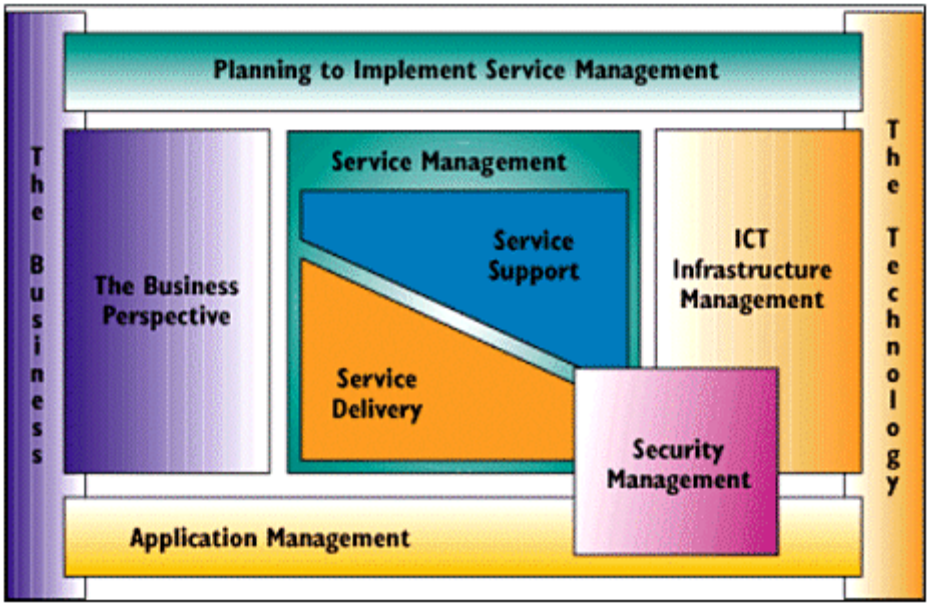



**Abbildung 10: ITIL V2 Framework [Dvwe05]**

ITIL V2 besteht im Kern aus sieben Modulen, die in [Dvwe05] beschrieben werden als:

- **Die geschäftliche Perspektive** (Business Perspective)
  Das Kernziel von Business Perspective ist es, eine gemeinsame Basis zwischen dem Kunden (Business) und dem IT-Service Anbieter (Provider) zu finden. Dem Kunden soll ein Verständnis für die IT-Services, welche maßgeblich den Business Prozess unterstützen, und deren Management vermittelt werden. Business Perspective kann das Business bei der Planung, Implementierung und Nutzung von qualitativ hochwertigen IT-Services informieren

und unterstützen, damit verbesserte Business Prozesse ermöglicht werden.

- **Unterstützung und Betrieb von Services** (Service Support)
  Die Aufgabe von Unterstützung und Betrieb ist die Erbringung der vereinbarten Serviceleistung. Hier sind alle operativen Prozesse abgebildet, wie beispielsweise Incident Management, Problem Management und Service Desk.
- **Planung und Lieferung von Services** (Service Delivery)
  Planung und Lieferung stellt die Schnittstelle der IT zum Kunden dar. Die Prozesse umfassen unter anderem die Planung und Implementierung neuer Services, was durch das Change Management und das Release Management abgebildet ist.
- **Management der Infrastruktur** (ICT Infrastructure Management)
  Das Management der Infrastruktur umfasst alle Aktivitäten und Maßnahmen zur Bereitstellung und Instandhaltung der Infrastruktur, entsprechend ihres Bestimmungszweckes.
- **Planung zur Einführung von Service Management** (Planning to Implement Service Management)
  Planning to Implement Service Management befasst sich mit der Planung, Einführung und fortlaufenden Verbesserung der ITIL-Management- Bereiche, bzw. der Prozesse. Die Umsetzung des ITIL Frameworks ist kein einmaliger Vorgang, sondern eine kontinuierlich fortzuführende Aufgabe.
- **Management der Anwendungen** (Application Management)
  Das Application Management stellt eine Roadmap zur Verfügung, die es ermöglicht, neue und bestehende Applikationen in einer Umgebung besser und zukunftsfähiger zu integrieren. Es beschreibt umfassend das Management für den gesamten Lebenszyklus einer Applikation (Software, Anwendung). Der Zyklus beinhaltet sowohl die Applikationsentwicklung (Application Development), als auch deren Nutzung (Service Management). Ziel ist es, in den beiden Teilphasen immer die Belange des gesamten Zyklus zu berücksichtigen, damit sicher betreibbare, stabile und veränderbare IT-Services aus den Applikationen generiert werden können.
- **Security Management**
  Informationssicherheit kann nur als unternehmensweites Konzept aufgebaut werden. Die Hauptaufgaben der Informationssicherheit bestehen in dem kontrollierten Zurverfügungstellen von Informationen und dem Schutz dieser vor unbefugtem Zugriff sowie dem Schutz der Infrastruktur vor unbefugtem Gebrauch.

Aufgrund steigender Verbreitung entwickelte sich ITIL immer mehr zum De-Facto Standard für IT Service Management. Hierbei flossen Konzepte, Methoden und Verfahren in den ISO 20000 Standard sowie in verschiedene Modelle, wie beispielsweise HP ITSM Reference Model (Hewlett Packard) [HP00], IT Process Model (IBM) [IBM01], Microsoft Operations Framework [MS08], ein.

Im Mai 2007 wurde in ITIL V3 eine komplett überarbeitete und neu strukturierte Version von ITIL veröffentlicht. Kern von ITIL V3 ist die Abbildung des gesamten Service Lifecycles. Hierzu finden sich die Prozesse von ITIL V2 in der neuen Version wieder, wurden aber um weitere ergänzt. Manche Prozesse von ITIL V2 wurden zur besseren Gliederung und Abgrenzung sowohl bei der Implementierung als auch beim Betrieb in mehrere Prozesse aufgegliedert. Beispielsweise wurde Incident Management aus ITIL V2 in Incident Management, Request Fulfillment, Access Management und Event Management in ITIL V3 neu strukturiert abgebildet. Die folgende Tabelle spiegelt die Abbildung der ITIL V2 Prozesslandschaft in ITIL V3 wider.

| ITIL V2 Prozess | ITIL V3 Prozesse |
|---|---|
| Availability Management | Availability Management |
| Capacity Management | Capacity Management |
| Financial Management | Financial Management |
| IT Service Continuity Management | IT Service Continuity Management |
| Service Level Management | Service Level Management<br>Service Catalog Management |
| Service Desk | Service Desk |
| Incident Management | Incident Management<br>Request Fulfillment<br>Access Management<br>Event Management |
| Problem Managment | Problem Managment |
| Change Management | Change Management |
| Release Management | Release Management<br>Deployment Management |
| Configuration Management | Configuration Management<br>Asset Management |
| Security Management | Security Management |

**Tabelle 2: ITIL V2 zu ITIL V3 Prozess Mapping**

Aktuell sind mehrere Organisationen mit der Pflege und Weiterentwicklung von ITIL involviert.

- Office of Government Commerce (OGC), als Eigentümer von ITIL
- IT Service Management Forum (itSMF) [itSMF], ein internationales Non-Profit Unternehmen, welches sich der Unterstützung und Weiterentwicklung von IT Service Management widmet
- APM Group [APMG], welche seit 2006 in Abstimmung mit OGC Zertifizierungs- und Akkreditierungsschemata für ITIL Examen definiert
- Examinierungsinstitutionen sind Institute, welche durch die APM Group bevollmächtigt sind, ITIL Examen für verschiedene Qualifikationsebenen abzuhalten.

## 3.2 Aufbau von IT Service Management

Das Service Management ist eine Sammlung an Services, welche den Kunden einen so genannten „Value“ (Wert) liefern. Der Value ist wiederum bestimmt durch „Utility“ (Zweckmäßigkeit), also was der Kunde haben will, und „Warranty“ (Einsatzgeeignetheit), also der Form der Erbringung.

Die Services in ITIL V3 sind entsprechend dem Service Lifecycle [OGC07L] gegliedert. Hierbei handelt es sich um eine Abbildung des Lebenszyklus von Services, welches in einem organisatorischen Modell eingebettet ist.


**Abbildung 11: ITIL Service Lifecycle [OGC07L]**

Das Service Lifecycle Model stellt dar, wie Service Management gemäß ITIL V3 funktionieren soll, wie die Komponenten untereinander in Verbindung stehen und welchen Einfluss Änderungen einzelner Komponenten auf das Gesamtsystem haben.

Das gesamte Service Lifecycle Model ist in die fünf Phasen – Service Strategie, Service Design, Service Transition, Service Operation und Continual Service Improvement – gegliedert, welche in weiterer Folge besprochen werden.

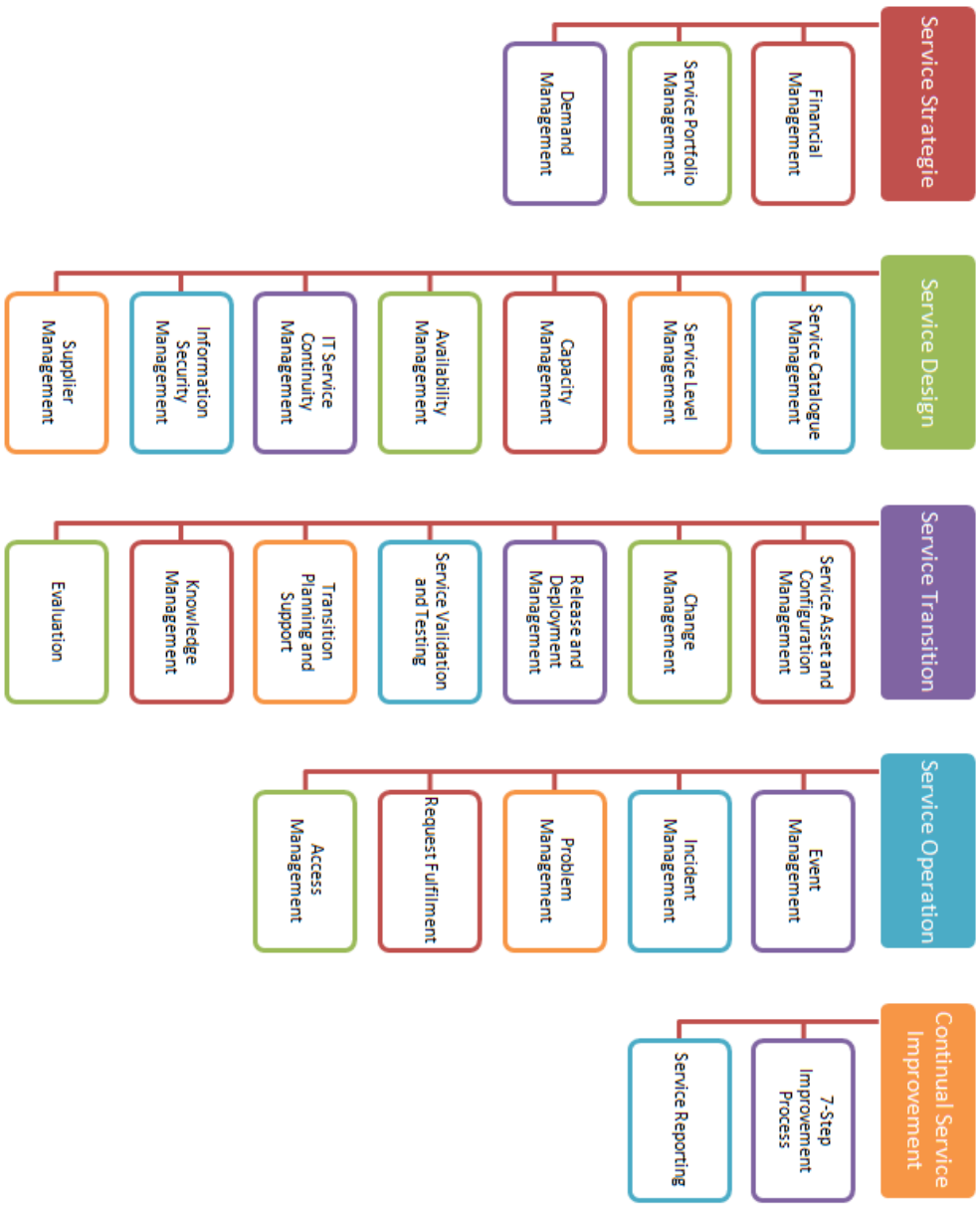



**Abbildung 12: ITIL Prozesslandschaft**

### 3.2.1 Service Strategy

Service Strategy liefert Leitlinien zum Design, zur Entwicklung und zur Implementierung von Service Management als strategische Ressource. [BoJo08S] Sie soll helfen, kunden- und marktorientierte Ziele und Erwartungen zu identifizieren und festzulegen, aber auch auf Gelegenheiten

adäquat reagieren zu können. Hierzu werden die Grundsätze des Marktfokus in das ITIL Framework eingebettet, also den Grundsatz zu wissen, wo und wie man im Wettbewerb steht, den Grundsatz der differenzierenden Fähigkeiten, also zu verstehen, welche unterscheidbare und profitable Assets geschaffen werden können, und den Grundsatz der Performance Anatomie, also dem Verständnis, Services als strategische Assets zu betrachten, welche kontinuierlicher Weiterentwicklung bedürfen.

Sind einem Unternehmen die Ziele bekannt, tritt man ein in die Phase der Service Strategie. Hierbei hilft das Modell der fünf P von Henry Mintzberg [Mint92] – Perspektive, Position, Plan, Ploy (List) und Pattern (Muster).


**Abbildung 13: Strategie der fünf P [Mint92]**

Der Plan beschreibt, welches Ziel konkret verfolgt wird. Daraus ergibt sich, dass eine Strategie vor dem Handeln existiert und dieses beeinflusst. Die Strategie ist in gewisser Weise eine List, seine Konkurrenz zu übertreffen. Vorgänge, die auf eine Strategie basieren, verursachen bestimmte Muster. Die Muster spiegeln die Kontinuität von Entscheidungen und Maßnahmen wider, die sich aus einer festgelegten Positionierung und einer verfolgten Perspektive ergeben.

Service Strategy umfasst die Prozesse des Financial Managements, des Service Portfolio Managements und des Demand Managements. Für eine

detaillierte Prozessbeschreibung sei auf [BoJo08S] und [OGC07S] verwiesen.

- **Financial Management**
  Das Financial Management ist dafür verantwortlich, dem Management jene Informationen bereitzustellen, welche für die Gewährleistung eines wirtschaftlichen und kosteneffektiven Service Delivery notwendig ist. Das Financial Management dient dazu, jegliche Ausgaben den Services zuzuordnen und zu rechtfertigen.
- **Service Portfolio Management**
  Das Service Portfolio Management beschreibt die Werte des Unternehmens. Es werden alle Services dargestellt und erläutert, wie diese den Anforderungen des Marktes entsprechen.
- **Demand Management**
  Das Demand Management ist verantwortlich für das Ausrichten des Anbots auf den Bedarf.

Betrachtet man die Darstellung des Service Lifecycles, so ist ein direktes Wirken von Service Strategy auf Service Design, Service Transition und Service Operation, sowie in weiterer Folge auf Continual Service Improvement ersichtlich.

### *3.2.2 Service Design*

Basierend auf Service Strategy entwickelt Service Design verschiedene Services zur Produktionsreife, wobei dies sowohl die Entwicklung neuer Services als auch die Modifikation bestehender Services inkludiert.

Werden neue Services eingeführt, so müssen eine Reihe von Prozessen durchlaufen werden. Beispielsweise müssen nach der Konzeptphase neue Services dem Service Portfolio hinzugefügt und die Anforderungen genau bestimmt werden. Sowohl das Capacity Management, das Availability Management, das IT Service Continuity Management als auch das Security Management müssen die Anforderungen analysieren und die Auswirkung der Integration in die bestehende IT Landschaft abschätzen. Gegebenenfalls müssen Investitionen getätigt werden, welche mit Financial Management abgestimmt und durch das Supplier Management beschafft werden müssen.

Bei Modifikationen an Services werden in der Regel die gleichen Prozesse wie bei der Integration eines neuen Service durchlaufen.

Das Service Design umfasst die Prozesse des Service Catalog Managements, Service Level Managements, Capacity Managements,

Availability Managements, IT Service Continuity Managements, Information Security Managements und Supplier Managements. Für eine detaillierte Prozessbeschreibung wird auf [Bon08D] und [OGC07D] verwiesen.

- **Service Catalogue Management**
  Die Dokumentation aller Services und deren Wechselwirkung ist Aufgabe des Service Catalogue Managements. Hierbei werden alle Anforderungen, technische und organisatorische Methoden zur Erfüllung, Preise, Lieferergebnisse, Zuständigkeiten uvm. von betriebenen Services erfasst.
- **Service Level Management**
  Ziel des Service Level Managements ist die Vereinbarung der zu erbringenden Anforderungen von Services mit dem Kunden. Entscheidend hierbei ist die Bestimmung von messbaren Erfüllungskriterien. Für diesen Prozess ist der Service Level Manager verantwortlich.
- **Capacity Management**
  Die Aufgabe des Capacity Management ist die unternehmensweite kosteneffektive und effiziente Sicherstellung der Nutzung von Kapazitäten. Notwendige Kapazitäten sollen ausreichend verfügbar sein, wenn sie gebraucht werden, andererseits sollen nicht unnötige Investitionen getätigt werden. Beides wird durch Überwachung der genutzten Kapazitäten, Trendanalysen und Kapazitätsplanung realisiert.
- **Availability Management**
  Das Availability Management soll sicherstellen, dass den Anforderungen bezüglich Verfügbarkeit entsprochen wird. Der Einsatz entsprechender Technologien und Verfahren soll der Gefahr von technischen Fehlern, wie zum Beispiel einem defekten Server, entgegenwirken, sodass die mit dem Kunden vereinbarten Service-Verfügbarkeiten nicht gefährdet sind.
- **IT Service Continuity Management**
  Im Falle eines Desasters muss der Betrieb nach einer gewissen Unterbrechungszeit wieder anlaufen. Das IT Service Continuity Management stellt sicher, dass selbst bei einem Desaster ein Wiederanlauf möglich ist.
- **Information Security Management**
  Information Security Management bildet die Sicherheitsstrategie des Unternehmens in Security Policies sowie Leitlinien zur Information Security ab und steuert und kontrolliert Sicherheitsprozesse.

- **Supplier Managements**
  Supplier Management ist für den Umgang mit Lieferanten, welche zur Erbringung von Services notwendig sind, verantwortlich.

### 3.2.3 Service Transition

Nachdem die Spezifikation von neuen Services oder von Modifikationen durch Service Design entwickelt wurde, muss diese durch Service Transition umgesetzt werden. Hierbei liegt der Schwerpunkt in der Umsetzung entsprechend den Anforderungen und der Erreichung der mit dem Kunden vereinbarten Qualität. Gleichzeitig darf die Umsetzung bestehende Services möglichst wenig durch Störungen, Wartungsfenster usw. beeinflussen.

Service Transition umfasst die Prozesse Transition Planning und Support, Change Management, Service Asset und Configuration Management, Release und Deployment Management, Service Validation und Test, Evaluation und Knowledge Management. Für eine detaillierte Prozessbeschreibung sei auf [BoJo08T] und [OGC07T] verwiesen.

- **Transition Planning and Support**
  Transition Planning and Support ist für die konkrete Planung und Steuerung von Umsetzungen verantwortlich. Der Prozess stellt sicher, dass die notwendigen Ressourcen verfügbar sind, dass die Standards und Richtlinien angewendet und klare und umfangreiche Pläne bereitgestellt werden.
- **Change Management**
  Change Management beurteilt die Auswirkungen von Umsetzungsvorhaben (Request for Change, abgekürzt als RfC) und gibt diese in Zuge des Change Management Prozesses frei (wodurch aus einem Request for Change ein Change wird) oder lehnt sie gegebenenfalls ab. Beurteilt werden unter anderem das Risiko, eine adäquate Planung und Umsetzungsstrategie, Konflikte mit anderen Services oder Changes.
- **Service Asset and Configuration Management**
  Service Asset and Configuration Management ist für die Dokumentation der IT Infrastruktur und der IT Services verantwortlich. Die Gesamtheit des Informationspools wird als Configuration Management Database (CMDB) bezeichnet.

- **Release und Deployment Management**
  Release und Deployment Management ist für das Umsetzen des Changes in Form von Releases verantwortlich. Hierbei werden erprobte Verfahren und Methoden zur Umsetzung eingesetzt, sodass zum einen bestehende Services möglichst wenig beeinflusst werden, zum anderen das Risiko von fehlgeschlagenen Releases möglichst gering ist.
- **Service Validation and Test**
  Service Validation and Test stellt sicher, dass Releases die Kundenerwartungen erfüllen, Services zweckmäßig und einsatzbereit sind und die Spezifikation erfüllen.
- **Evaluation**
  Die Evaluation ist jener Prozess, der die Bewertung durchführt, ob die vorhergesagten Leistungen den tatsächlichen Leistungen entsprechen. Der Kunde ist stets in den Prozess in Form von Abnahmen involviert.
- **Knowledge Management**
  Das Knowledge Management dokumentiert Erkenntnisse und Erfahrungen in einer eigenen Wissensdatenbank, die in ITIL als Service Knowledge Management System (SKMS) bezeichnet wird. Zur Unterscheidung von Asset und Configuration Management soll die folgende Graphik dienen. Sie basiert auf dem Data - Information - Knowledge - Wisdom Modell (DIKW Modell), welches auch oftmals als „Wisdom Hierachy“, „Knowledge Hierarchy“ oder „Information Hierarchy“ bezeichnet wird. Siehe hierzu [Rowl07] [Zins07]. Die Graphik zeigt die klare Abgrenzung zwischen Informationen, wie sie durch das Asset und Configuration Management und Erkenntnisse und Erfahrungen, wie sie durch das Knowledge Management erfasst werden. Die Erkenntnisse und Erfahrungen dienen allen anderen Prozessen als Grundlage für Verbesserungen (basierend auf Weisheit).

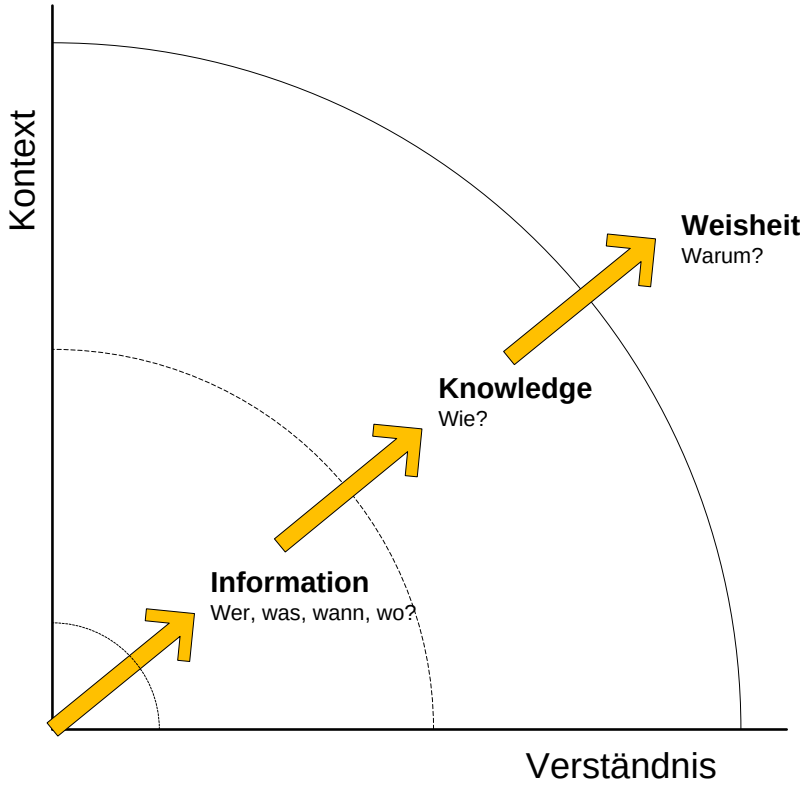



**Abbildung 14: Information - Knowledge - Weisheit, basierend auf [Rowl07] [Zins07]**

### *3.2.1 Service Operation*

Nach erfolgreichen Releases müssen Services betrieben werden. Der Betrieb von Services ist in ITIL im Bereich Service Operation abgebildet.

Service Operation beinhaltet die Prozesse Incident Management, Event Management, Request Fulfillment, Access Management und Problem Management. Diese Prozesse sind dafür verantwortlich, die Servicequalität und die -kosten zu optimieren. Für eine detaillierte Prozessbeschreibung wird auf [BoJo08O], [Kras06] und [OGC07O] verwiesen.

- **Incident Management**
  Das Incident Management ist für die Behandlung von Störungen verantwortlich.
- **Event Management**
  Störungen können nicht nur vom Kunden erkannt, sondern vielmehr durch automatisierte Überwachung der Services und Infrastruktur aufgezeigt werden. Event Management ist für die Erkennung und

Erstanalyse von Ereignissen (Events) als auch für die Bestimmung der richtigen Maßnahmen zur Behandlung verantwortlich.

- **Request Fulfillment**
  Standardanfragen, welche sehr häufig auftreten, werden durch den Request Fulfillment Prozess behandelt.
- **Access Management**
  Als eine besondere Art von Standardanfragen werden jene bezüglich Freigaben von Berechtigungen und Zugängen betrachtet. Diese werden in einem dezidierten Prozess behandelt. In vielen Unternehmen wird auch die Begrifflichkeit des Rights Managements oder des Identity Managements für das Access Management verwendet.
- **Problem Management**
  Während Incident Management Störungen schnellstmöglich beheben versucht, wird oftmals die eigentliche Fehlerursache nicht gefunden. So ist beispielsweise durch einen Reboot die Störung behoben, die eigentliche Ursache aber weiterhin unbekannt. Problem Management analysiert jene Störungen, die öfter aufgetreten sind oder besonders negative Auswirkungen hatten. Problem Management identifiziert Maßnahmen, wie diese Störungen zukünftig verhindert werden könnten.

### *3.2.2 Continual Service Improvement*

Um die Wettbewerbsfähigkeit eines Unternehmens zu steigern, muss neben der Effizienz auch die Prozessqualität verbessert werden. [JaFa07] Abteilungen müssen ihre Services kontinuierlich verbessern, um für das Business attraktiv zu bleiben. [Bon08C] Die fortwährende Verbesserung der Effektivität und Effizienz wird in ITIL durch Continual Service Improvement gewährleistet.

Continual Service Improvement umfasst die Prozesse 7 Step Improvement und Service Reporting. Für eine detaillierte Prozessbeschreibung sei auf [Bon08C] und [OGC07I] verwiesen.

- **7 Step Improvement (oder CSI Improvement Process)**
  Während man mit dem PDCA Rad Innovationszyklen lebt und die Qualität misst, beschreibt der Siebenschritt Verbesserungsprozess, wie gemessen und berichtet werden soll. Wenn der Service Level Manager etwas entdeckt, das verbessert werden kann, wird die

Analyse durch das Continual Service Improvement angestoßen. Das Ergebnis eines 7 Step Improvement Zyklus ist die Erstellung eines Service Improvement Plans (SIP), welcher zusammenfassende Informationen über Maßnahmen, mit denen die Servicequalität verbessert werden soll, beinhaltet.


**Abbildung 15: CSI Verbesserungsprozess [OGC07I]**

- **Service Reporting**
  Das Service Reporting des Continual Service Improvement ist businessfokusiert. Es dient nicht dazu, die Einhaltung von SLAs zu zeigen (hierfür siehe Service Level Management), sondern um zusammenzufassen, was vorgefallen ist, was zur Behebung unternommen wurde und was getan wurde, damit ähnliche Vorfälle keine oder akzeptabel geringe Auswirkungen auf das Business haben. Somit wird die vergangene, gegenwärtige und zukünftige Leistungsfähigkeit des Business dargestellt und für verschiedene Stakeholder veröffentlicht.

## 3.3 ITIL und andere Referenzmodelle

Basierend auf Analysen und Publikationen von ISACA [ISACA] lässt sich die folgende Pyramide an Referenzmodellen darstellen. Die Pyramide visualisiert den stufenförmigen Aufbau verschiedener Frameworks, Best Practice Guides und Normen aus der Sichtweise von Governance, Reifegradmodellen, Geschäftsmodellierungen und Projektmanagement, Security und Service Management sowie unternehmensinternen Prozessen.

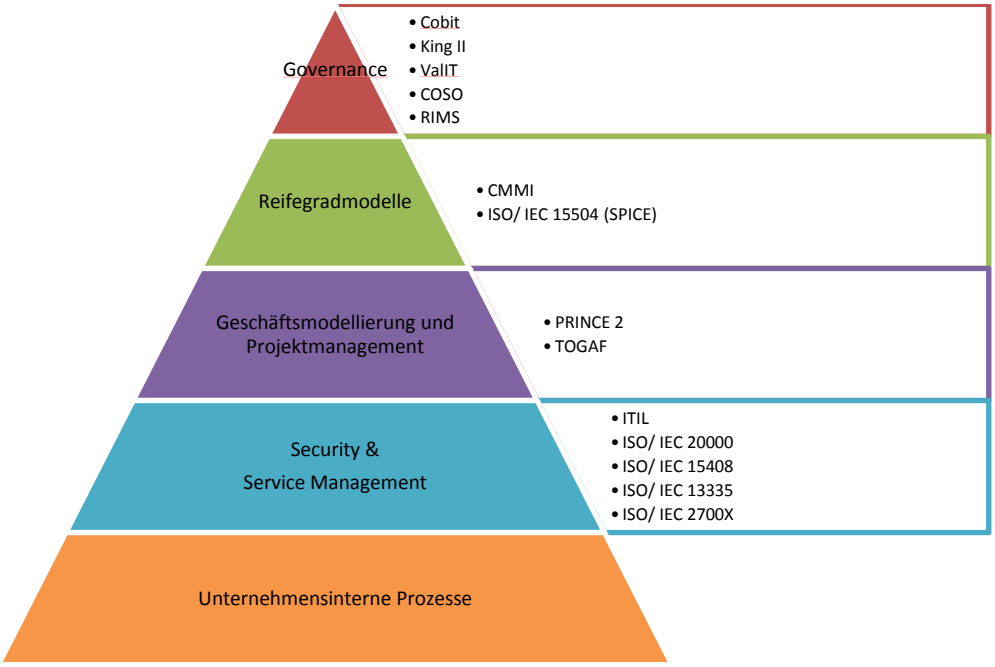



**Abbildung 16: Überblick Governance Frameworks, basierend auf [ISACA]**

COSO (Committee of Sponsoring Organizations of the Treadway Commission) [COSO] hat 1992 das COSO Modell publiziert, welches ein Kontrollmodell im Bereich der Finanzberichterstattung darstellt (COSO und Basel II siehe [ITGI07a], COSO und Sarbanes-Oxley siehe [FoZo06]). Das Modell wurde in den folgenden Jahren um Enterprise Risk Management (2004) sowie um Finanzberichterstattung von kleineren Aktiengesellschaften (2006) erweitert.

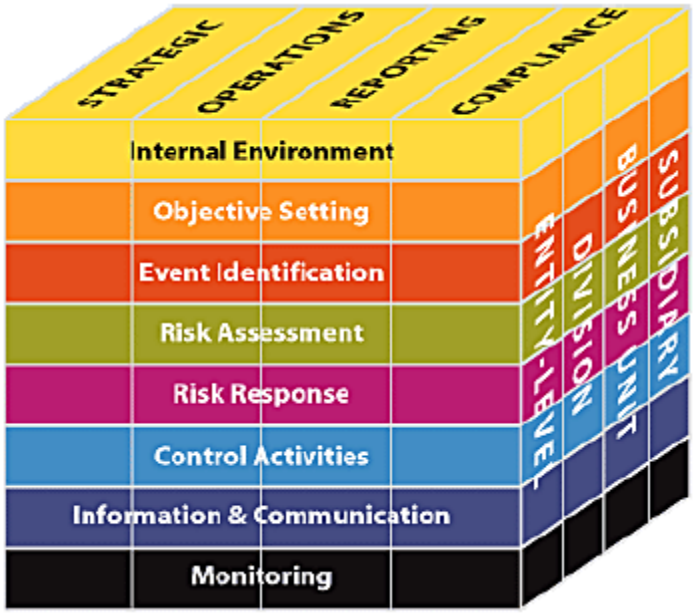



**Abbildung 17: COSO Würfel [COSO]**

Control Objectives for Information and Related Technology (COBIT) ist analog zu ITIL ein Best Practice Framework. welches auf COSO basiert und die Aufgaben der IT in 34 Prozessen und deren Control Objectives (Kontrollziele) gliedert. Das COBIT Governance Modell beschreibt in den Bereichen „Plan & Organize“, „Acquire & Implement“, „Delivery & Support“ und „Monitor & Evaluate“ die prozessorientierte Darstellung zur Bereitstellung von Information in einem Unternehmen. Die aktuelle Version 4.2 von COBIT ist unter [ITGI07] frei verfügbar. Die Verbindung zwischen COBIT und anderen Frameworks, wie ITIL, Prince2, ISO/IEC 27002 und weitere, kann in mehreren Publikationen von ISACA (siehe [ISACA10]) detailliert nachgelesen werden.

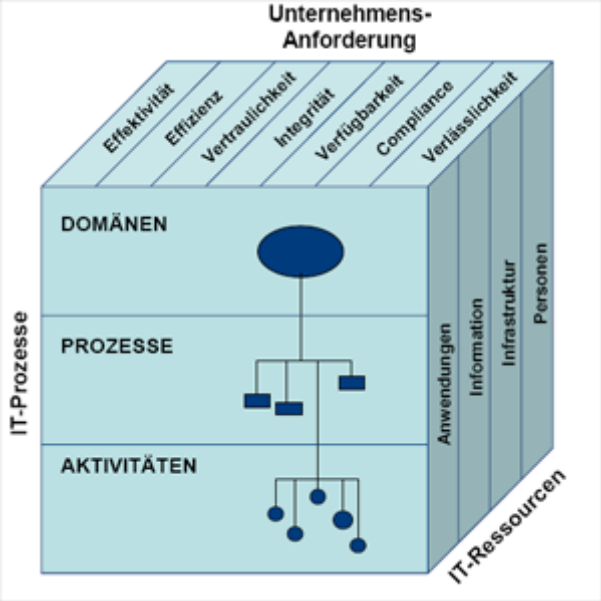



**Abbildung 18: COBIT Wüfel [ITGI07]**

Die so genannten King Reports wurden vom Department for National Treasury der Republik von Südafrika [NTRSA] erstellt und veröffentlicht. Die drei erschienenen Reports (King Report I veröffentlicht 1994, King Report II veröffentlicht 2002 und King Report III veröffentlicht 2009, siehe [SAICA09]) beschreiben die Governance Bedingungen für Unternehmen, die an der Börse von Südafrika notiert sind, haben aber ebenfalls allgemeine Gültigkeit.

Das durch das IT Governance Institute (ITGI) [ITGI] entwickelte Rahmenwerk ValIT stellt eine Erweiterung und Vervollständigung von COBIT dar. ValIT hat den Schwerpunkt in den Entscheidungsprozessen um IT Investitionen und deren Evaluation, während sich COBIT vielmehr auf die operative Ebene beschränkt. Die derzeit aktuellste Version von ValIT kann unter [ITGI08] bezogen werden.

Der Risk Management Standard (RIMS) entstand 2002 aus einer Zusammenarbeit zwischen dem Institute of Risk Management (IRM) [IRM], der Association of Insurance and Risk Managers (AIRMIC) [AIRMIC] und dem Nationalen Forum für Risk Management im öffentlichen Bereich (ALARM) [ALARM]. Der Standard kann unter [IRM03] frei heruntergeladen werden. Er beschreibt einen Risikomanagement Prozess und den Umgang mit finanziellen, strategischen und operativen Risiken und Gefahren.

Qualität muss geplant, gemessen und beobachtet werden. [NoMu03] Das Capacity Maturity Model (CMMI) ist ein am Software Engineering Institute (SEI) der Carnegie Mellon University Pittsburgh entwickeltes Reifegradmodell, welches Prozesse qualitativ misst, indem es ihnen Reifegrade zuweist. Das Modell besticht durch seine universelle Anwendbarkeit, beispielsweise als Benchmarking für Projektmanagement von Softwareprojekten [Scho08] oder als Assessment Methode für kleine Software- Unternehmen. [Andr09] Dadurch, dass es zulässig ist, auch alternative Praktiken zu verwenden, solange sie das gleiche Ziel wie die vorgeschlagenen Best Practices haben, wird die Flexibilität in der Anwendung des Modells erhöht. Die Verwendung von CMMI als Referenzmodell bietet langfristig die für kleine Unternehmen notwendige Flexibilität in Hinblick auf organisationsweite Anwendung von Prozessverbesserungen. [Andr09]

Konkurrierend zu CMMI wurde Software Process Improvement and Capability Determination (SPICE) ebenfalls als Reifegradmodell entworfen, kann allerdings keine Projekte, Abteilungen oder Unternehmen ganzheitlich bewerten. SPICE beziehungsweise ISO/IEC 15504 [ISO98] ist ein internationaler Standard.

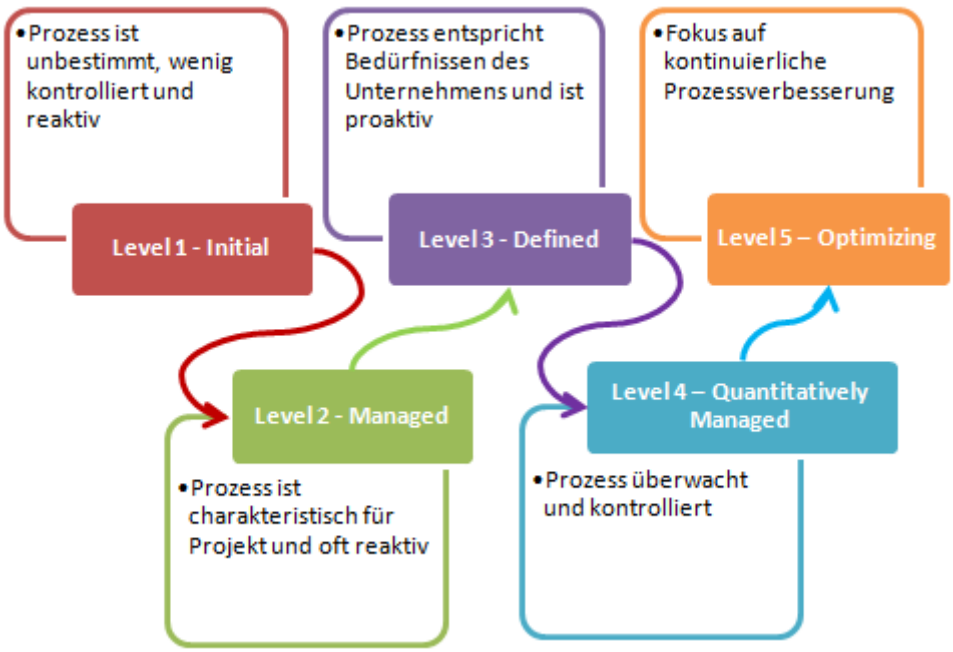



**Abbildung 19: CMMI Reifegradmodell**

Projects in Controlled Environments (Prince, seit neuer Version 1996 als Prince2 bezeichnet) ist ein strukturierter Projektmanagementansatz, welcher Management, Steuerung und Organisation von Projekten umfasst. Das Modell beschreibt die Koordination von Mitarbeitern und Aktivitäten sowie die Planung und Leitung von Projekten.

The Open Group Architecture Framework (TOGAF) ist ein offener Standard zur Etablierung von Enterprise Architekturen und kann unter [Open10] bezogen werden. Es handelt sich um einen umfassenden Ansatz für Entwurf, Planung, Implementierung und Wartung von Unternehmensarchitekturen.

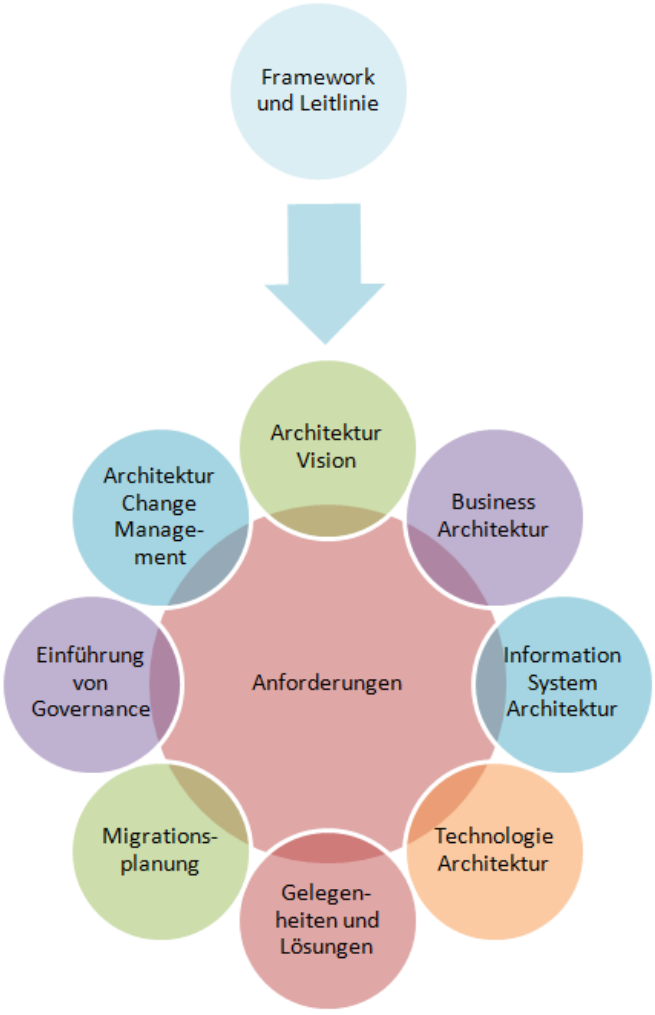



**Abbildung 20: TOGAF Architekturmodell [Open10]**

Neben ITIL gibt es eine Reihe an Security und Service Management Best Practices, welche in internationale Standards eingeflossen sind. Die

Common Criteria for Information Security (kurz als CC bezeichnet), welche mittlerweile zur Norm ISO/IEC 15408 erklärt wurden, beschreiben Kriterien zur Bewertung und Zertifizierung der Sicherheit von IT Systemen. Die Norm ISO/IEC TR 13335 umfasst eine Sammlung von technischen Kontrollen zum Management von Informationssicherheit. Der internationale Standard ISO/IEC 27001 ist eine umfassende Sammlung von Anforderungen für ein Information Security Management System. In ISO/IEC 27000 werden die Begrifflichkeiten definiert, ISO/IEC 27002 enthält inhaltlich den Leitfaden ISO/IEC 17799:2005. ISO/IEC 27003 gibt Leitfäden zur Umsetzung der ISO/IEC 27001 Norm wieder.

# 4 Bedrohungsanalyse – Risikofaktor Mensch

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder Systemen durch Aushorchen zu erlangen oder eine Person dazu zu bringen, eine gewisse Aktion zu setzen. Dabei werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autoritäten ausgenutzt, wodurch Mitarbeiter so manipuliert werden können, sodass sie unzuverlässig handeln. Besonders zu beachten ist, dass Social Engineering nichts mit Gewaltandrohung, Erpressung oder Ähnlichem zu tun hat. Es bedeutet vielmehr im weitesten Sinne das „Beeinflussen von menschlichen Verhalten mit Hilfe von Ingenieurmethoden“.

Social Engineering stellt eine besondere Herausforderung für Informationssicherheit dar, da technische Sicherheitsmaßnahmen durch menschliches Verhalten außer Kraft gesetzt werden.

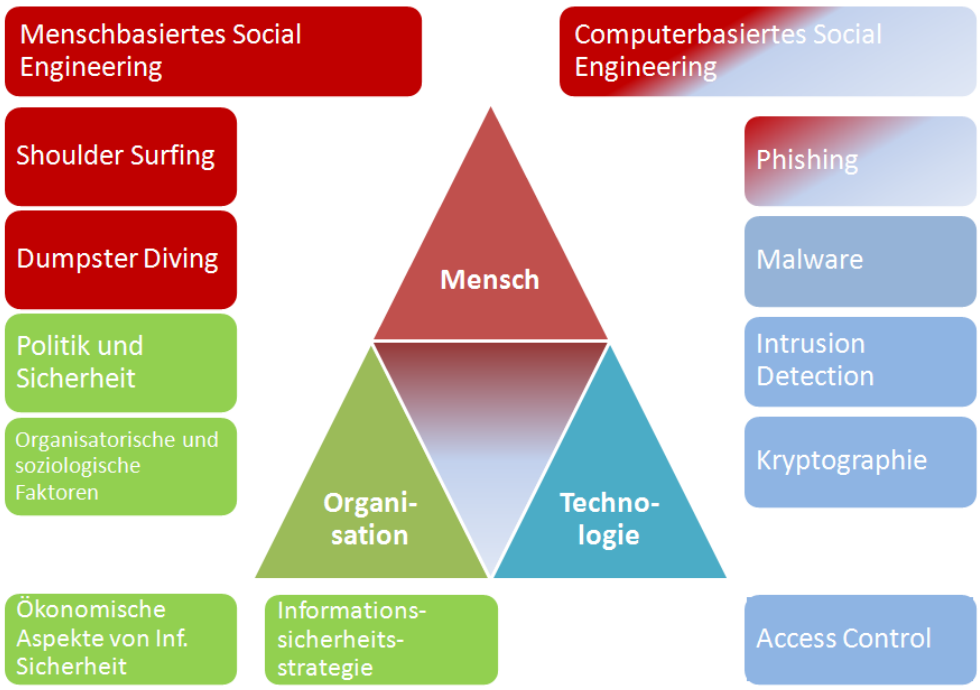



**Abbildung 21: Mensch – Organisation – Technologie**

Während ein Hacker ein technisches Sicherheitsloch ausnutzt, um in ein Computernetz einzudringen und nicht autorisierten Zugriff auf sensible

Informationen zu erlangen, nutzt der Social Engineer seine sozialen Kontakte.

## 4.1 Der Social Engineer

Ein Social Engineer ist in der Regel nicht an Zerstörung interessiert, sondern vielmehr am unberechtigten Zugang von Informationen. Der Social Engineer ist ein spezieller Hacker, der zum einen nicht Computersysteme angreift, sondern Menschen und zum anderen keine technischen Methoden anwendet, sondern sich vielmehr den Methoden der Psychologie und Kommunikationswissenschaft bedient.

Betrachtet man zunächst die Erfolgsfaktoren einer Social Engineering Attacke, so kann man daraus die Fähigkeiten eines Social Engineers ableiten.

Ein Social Engineer verfügt über hohe soziale Fähigkeiten, ist ein gewandter Redner, kann auf Menschen gut eingehen und überzeugend auftreten. Grundlegend für jeden Social Engineer ist die Begabung, sich Informationen im Vorfeld eines Angriffs auf vielfältigste Weise beschaffen zu können. Derartige Recherchen können zumal sehr lange dauern, mitunter Jahre, was Geduld und ein hohes Maß an Zielstrebigkeit voraussetzt.

Während eines Angriffs ist der Social Engineer in der Lage, spontan auf eine sich ändernde Situation reagieren zu können. Tritt der Social Engineer in direkten Kontakt mit dem Opfer, so ist ein hohes Maß an Selbstkontrolle Grundvoraussetzung für einen erfolgreichen Angriff.

Betrachtet man nun die psychologischen Eigenschaften eines Social Engineers, so wird von Robert Anton Wilson der Persönlichkeitstyp des Hackers als „Neophiliac“ bzw. „Neophile“ bezeichnet. Kennzeichnende Charaktereigenschaften sind:

- die Fähigkeit zur schnellen und spontanen Anpassung an extremen Veränderungen,
- die Ablehnung oder völlige Abscheu vor Tradition, eingefahrenen Mustern und Routine,
- eine Tendenz, schnell von alten Sachen gelangweilt zu sein,
- ein tiefes Verlangen, manchmal fast schon ein an Obsession grenzender Zwang, sich mit Neuem zu beschäftigen und Neues zu erfahren und

- ein korrespondierendes Verlangen, Neues zu erschaffen oder zu erreichen.

Daraus ergibt sich auch, dass entgegen dem weitläufigen Glauben, Hacker keinesfalls sogenannte „Fachidioten“ sind. Sie beschäftigen sich üblicherweise mit einer Vielzahl unterschiedlichster Themen, die ihre mentalen Fähigkeiten stimulieren. Die Themen, auf die sich Hacker spezialisieren, sind weit gefächert in verschiedensten Bereichen.

Entsprechend [Raym03] fallen die meisten Hacker in die INTJ- und INTP-Kategorie der Myers-Briggs Typologie für Persönlichkeiten. Der Myers-Briggs-Typindikator (MBTI) basiert auf einer Weiterentwicklung der Typologie von Carl Gustav Jung durch Katharine Briggs und Isabel Myers. Publiziert wurde MBIT von David Keirsey, wodurch er an Bekanntheit gewann. Eingesetzt wird die Einstufung zum Beispiel im Personalwesen. Siehe dazu [BrMc98], [Brig98] und [Brig95].

Folgend werden die beiden Persönlichkeitstypen kurz zusammengefasst:

Unter den Persönlichkeitstyp INTJ (Introverted, Intuitive, Thinking, Judging) fallen ungefähr 1% der Bevölkerung. Sie sind selbstbewusst (was manchmal auch als arrogant wahrgenommen wird) und willensstark. Ihnen fällt es leicht, Entscheidungen zu treffen. INTJ-Persönlichkeitstypen sind prinzipiell offen für die Aufnahme neuer Ideen und Gedanken, sie tendieren aber dazu, nur jene Ideen und Gedanken schlussendlich zu akzeptieren, die sie als effizient, passend und vorteilhaft für ihre eigenen Ziele ansehen. Sie sind Führungspersönlichkeiten, treten aber erst in Erscheinung, wenn ein Projekt ihrer Meinung nach Wert für diesen Schritt ist, bis dahin gelten sie als unauffällig. Man kann INTJ-Persönlichkeitstypen auch als Personen ansehen, deren Zugang zur Realität einem Schachspiel gleicht, immer auf der Suche nach möglichst erfolgsversprechenden Strategien und stets bemüht, gedankliche Notfallpläne zu haben. Sie sind perfektionistisch veranlagt und haben das innere Bedürfnis, sich in für sie interessante Themengebiete zu vertiefen, sind aber gleichzeitig sehr pragmatisch. Durch die Kombination von Vorstellungskraft und Zuverlässigkeit sind INTJ-Persönlichkeitstypen gut im Kreieren von Systemen. Viele arbeiten im wissenschaftlichen Bereich oder als Techniker.

Hacker werden auch dem INTP-Persönlichkeitstyp (Introverted, Intuitive, Thinking, Perceiving) zugeordnet. INTP-Persönlichkeitstypen sind nachdenklich, analytisch veranlagte Persönlichkeiten, die manchmal in Gedanken versinken und ihre Umgebung vergessen. Sie sind tendenziös sehr präzise in ihren Beschreibungen und sie erwarten dasselbe von ihrer

Umgebung. Logische Korrektheit ist sehr wichtig für INTP-Persönlichkeitstypen. Sie tendieren dazu, sehr tolerant und flexibel zu sein, zumindest solange ihre Prinzipien nicht verletzt werden. In diesem Fall jedoch neigen sie dazu, sehr geradeaus und unflexibel zu werden. Im Gegensatz zu INTJ-Persönlichkeitstypen sind INTP-Persönlichkeitstypen nicht sehr selbstbewusst und investieren viel Zeit in Selbstreflexion. Sie wollen im Allgemeinen keine Führungsposition einnehmen. Das entfernte Ziel eines INTP-Persönlichkeitstypen ist stets die Veränderung der Umgebung. Sie lieben komplexe Systeme und arbeiten oftmals im Bereich der Mathematik, Computer, Sprachen oder anderer Gebiete hoher Komplexität.

Weitere Informationen zur Persönlichkeit von Hackern, deren Profile und Ziele siehe unter [Gauv05], [Hone04] und [ChDu08].

## 4.2 Klassifizierung von Social Engineering

Grundsätzlich werden die folgenden drei Arten von Social Engineering unterschieden [Wole08]:

**Technology-based Social Engineering** (Technik-basiertes Social Engineering oder auch als Computer-basiertes Social Engineering bezeichnet): Die bekannteste unpersönlichste Form des Technology-based Social Engineering ist Phishing. Hierbei werden zum Beispiel Mails von fingierten vertrauenswürdigen Absendern an potentielle Opfer mit der Aufforderung einer Handlung gesendet. Oftmals wird in den Phishing Mails auf eine Webseite verwiesen, die täuschend ähnlich einer vertrauenswürdigen Seite nachempfunden ist. Der Besucher wird zur Eingabe von sensiblen Daten aufgefordert, welche direkt an den Social Engineer weitergeleitet werden.


**Von:** BAWAG-P.S.K. [mailto:OnlinePolice@bawag.com]
**Gesendet:** Freitag, 3. März 2006 14:35
**Betreff:** Sofortige ReActivation ihres BAWAG Online Kontos!

BAWAG

**Sehr geehrte Kundin,**
**Sehr geehrter Kunde,**

In unserem Land hat sich eine komplizierte Lage gebildet, die auf dem online-Banking Gebiet entstanden worden ist. Demzufolge sind wir gezwungen, die online-Konten von unseren Bankkunden zu kontrollieren, um die möglichen Eintagskonten festzustellen. Die sogenannten Eintagskonten werden von den Missetätern benutzt, um Geld zu waschen. Infolgedessen bitten wir Sie darum, den Vordruck, mit dem Sie sich auf unserer Web - Seite vertraut machen können, auszufüllen.

Die Konten, die bis zum **10.03.06** auf unsere Formblätter nicht eingetragen werden, werden bis zur Ermittlung ihrer Eröffnung und Benutzung sowohl von den Privatpersonen, als auch von den Firmenkunden gesperrt.

BITTE! DIE FORM MUß AUSGEFÜLLT WERDEN!

Wir bitten uns bei Ihnen um Entschuldigung dafür, daß wir Ihnen große Schwierigkeiten bereitet haben.
Wir hoffen, daß wir weiterhin gut zusammenarbeiten werden.

Mit freundlichen Grüßen
BAWAG

© BAWAG

**Abbildung 22: Phishing Mail Attacke 2006 gegen Kunden der BAWAG P.S.K.**

Ein weiteres Beispiel einer typischen Phishing Attacke ist der folgende Mailinhalt. Das Phishing Mail wurde am 13. Oktober 2009 mit diesem Inhalt empfangen. Lediglich die vom Social Engineer angeführte Internetadresse wurde verändert, damit nicht unbewusst eine weitere Verbreitung der Webseite passiert.

***Von**: Administrator*
***Gesendet**: Dienstag, 13. Oktober 2009 13:35*
***Betreff**: Bitte öffnen*

*Hallo Markus,*
*hier sind die Zugangsdaten. Wie versprochen. wir haben es endlich geschafft einen Online Poker Raum zu hacken.*
*Nie mehr bezahlen !!! Nach monatlicher Hackerei mit unserem Profi Hacker Team. Haben wir es endlich geschafft. Es war nicht einfach!!! Spiel einfach mit dem Geld anderer Leute ohne zu bezahlen. Lass dir die Gewinne auf dein Konto auszahlen. Hier sind die gehackten Zugangsdaten:*

*User Name: stawm-0882845, Passwort: Isycajodey*
*---*
*Kontostand dieses Kontos: 6.875 Euro*
*---*
*Bitte nicht weiter geben. Das ist Geheim.!!!!!!!*
*Kein Risiko und kein Geldausgeben.*
*---*
*Du muss einfach auf die Webseite gehen und die kostenlose Poker Software downloaden und dann starten. Danach kannst du dich direkt mit den gehackten Zugangsdaten einloggen und mit dem Geld anderer Spielen.*

*http://luckygames122.com/Poker/*
*Tipp: Bitte nicht übertreiben sonst fällst es auf. Und der Account wird gesperrt.*

*dein*
*Cyber Hacker Team*
*:-)*
*PS: Sag mir bescheid wie es gelaufen ist. Und gib mir was von der Kohle ab.*

Am häufigsten werden Webseiten von Zahlungssystemen, Bankinstituten, Auktions- und Verkaufsplattformen gefälscht [APWG09], um die Internet-Nutzer zur Bekanntgabe geheimer Zugangsdaten (wie z.B. PINs und TANs) zu bringen. Diese Daten werden dann in betrügerischer Absicht verwendet, um die Opfer zu schädigen.

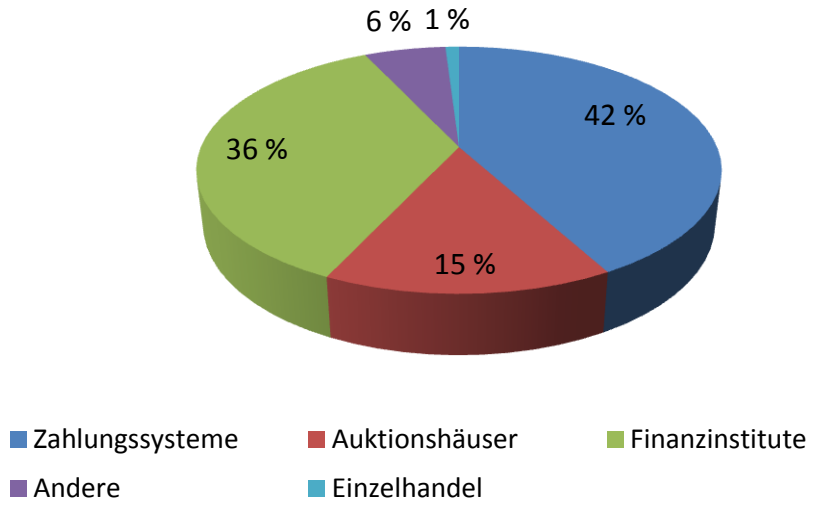



**Abbildung 23: Meist gefälschte Internetseiten 2009 [APWG09]**

Damit dem Opfer die Fälschung der Webseite nicht auffällt, wird nicht nur das Layout der echten Seite möglichst gut kopiert, sondern auch die URL nachgeahmt. Hierbei werden zumeist Subdomains oder ähnliche Schreibweisen verwendet. Beispiel hierfür wäre www.bawag.x.at oder www.bowag.net.

Der Phisher selbst macht sich strafbar, ist jedoch häufig nicht zu fassen. Das eigentliche Phishen wird vom Tatbestand des § 126c StGB [Oest10] (Missbrauch von Computerprogrammen oder Zugangsdaten) in ausreichendem Maße erfasst. Demnach macht sich strafbar, wer sich einen Zugangscode mit dem Vorsatz verschafft, dass dieser zur Begehung eines

betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) gebraucht wird.

Je nach Lage des Falles trägt der Kunde eines Finanzinstituts das Risiko, wenn er von der Bank darüber informiert wurde und die Phishing Attacke daher als solche hätte erkennen können. Die Bank haftet vor allem dann, wenn das Online-Banking System nicht dem Stand der Technik entspricht oder sie es unterlässt, Kunden vor möglichen Phishing Attacken zu warnen.

**Human-based Social Enginieering** (Mensch-basiertes Social Engineering): Beim Human- based Social Engineering kommuniziert der Social Engineer direkt mit dem Opfer. Das häufigste eingesetzte Kommunikationsmedium ist das Telefon. Der Angreifer nutzt wie auch bei Phishing Attacken menschliches Verhalten, um an die gewünschten Informationen zu gelangen, steht aber in Interaktion mit dem Opfer. Daraus ergibt sich zwangsläufig, dass Human- based Social Engineering Attacken sehr spezifisch und zielgerichtet sind.

Human- based Social Engineering ist fast immer verbunden mit Identitätsdiebstahl. Der Social Engineer gibt sich als eine andere Person, zum Beispiel als interner Mitarbeiter mit hoher Autorität, aus, um seine Ziele zu erreichen und einer etwaigen Strafverfolgung zu entgehen.

Aus strafrechtlicher Sicht ist die Art und Weise, mit der sich der Täter zum Beispiel Zugangsdaten verschafft, ohne Belang. Dies kann mittels getürkter E-Mails und exakt nachgebildeter Homepages geschehen, es ist aber ebenso gut möglich, dass sich der Täter keiner computerbasierten Hilfsmittel bedient und sich beispielsweise mittels persönlich adressierter und auf postalischem Weg übermittelter Schreiben an das Opfer wendet. Entscheidend für die strafrechtliche Relevanz ist in analoger Weise wie bei Phishing Attacken einzig und allein, dass der Täter mit dem Vorsatz handelt, die Daten später gewinnbringend zu verwerten.

Human- based Social Engineering inkludiert auch das sogenannte Dumpser Diving und Shoulder Sufing. Bei letzteren handelt es sich um jenen Angriff, bei dem direkt Überwachungsmethoden zum Einsatz kommen, um einen Mitarbeiter beim Eingeben sensibler Daten, wie zum Beispiel Zugangsdaten, zu beobachten. Dies kann ein einfacher Blick über die Schulter des Mitarbeiters, aber auch die Ausnutzung modernster Überwachungstechnologien bedeuten. Interessant hierzu sind sogenannte spy-resistant keyboards, siehe dazu [WiWa06] [RoRi04] und [DeKe05].

Dumpster Diving dient primär der Informationsgewinnung zur Vorbereitung des eigentlichen Angriffs. Es werden Informationen im Computermüll des Opfers gesucht, die zur Annahme einer fremden Identität, zum physischen Eindringen in einen Sicherheitsbereich oder als Informationsbasis für Beziehungsaufbauten während der folgenden Social Engineering Attacke hilfreich sind. Da sich Mitarbeiter nicht bewusst sind, welchen Informationswert der Müll für einen Angreifer haben kann, finden sich immer wieder unachtsam weggeworfene Ausdrucke von sensiblen Dokumenten, Mails oder Memos, Photographien, IDs und sogar Zugangsdaten darin. Falls es dem Angreifer gelingt, eine Arbeitsstelle, zum Beispiel als Reinigungskraft oder Praktikant, zu bekommen, kann er die Arbeitsplätze der Mitarbeiter in Mittags-, Kaffeepausen oder nach Feierabend genauer untersuchen. [Buch06]

**Reverse Social Engineering**: Die dritte Kategorie von Social Engineering Attacken stellt das sogenannte Reverse Social Engineering dar. Hierbei zielt der Angriff auf die Ausnutzung der menschlichen Eigenschaft ab, dass man Personen, die einem geholfen haben, zum einen besonderes Vertrauen schenkt, zum anderen man sich erkenntlich zeigen möchte.

Der Social Engineer kreiert eine Situation, in der sein Opfer Hilfestellung benötigt (Sabotage). Das Opfer muss so beeinflusst werden, dass es die Hilfe nichts ahnend beim Social Engineer sucht (Bewerbung), welcher freundlich und kompetent das scheinbare Problem löst (Unterstützung). Dadurch entsteht ein besonderes Vertrauensverhältnis zwischen Opfer und Social Engineer, welches dieser dann für den eigentlichen Angriff in Zuge der Problemlösung oder in späterer Folge ausnutzt.

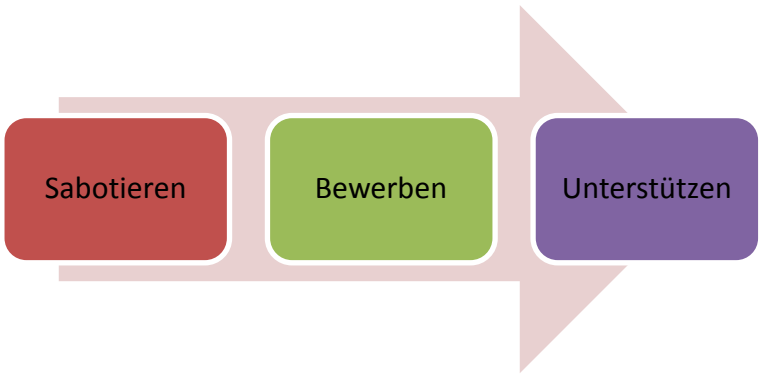



**Abbildung 24: Reverse Social Engineering Phasen [Nels06]**

Entsprechend [Nels06] wird Reverse Social Engineering durch die drei Phasen Sabotage, Bewerben und Unterstützen bestimmt. Hierbei ist mit der Begrifflichkeit „Sabotage“ nicht zwangsweise eine Zerstörung eines wirtschaftlichen Ablaufs gemeint, sondern allgemein das Bringen des Opfers in eine vermeintliche Notlage, aus welcher der Social Engineer in späterer Folge als „Retter“ heraushilft. Beispielsweise könnte ein Social Engineer gefälschte Mails (Mail- Spoofing) an eine Telearbeiterin schicken, welche den Anschein haben, dass sie von der Technikabteilung der Firma stammen. Mailinhalt ist eine Warnung, dass die Mail Client Einstellungen der Telearbeiterin falsch sind und daher gesendete Mails unter Umständen nicht zugestellt werden können und dass man doch bitte die Maileinstellungen richtigstellen solle. Zusätzlich werden Kontaktdaten (Name und Handy Nummer) angegeben, falls man hierfür Unterstützung braucht oder falls weitere Mails mit gleichen Warnungen empfangen werden. Ruft die Telearbeiterin diese Handy Nummer an, meldet sich ein freundlicher, kompetent wirkender und hilfsbereiter vermeintlicher Arbeitskollege, der sie telefonisch anleitet, einige Mail Client Einstellungen mit ihm gemeinsam durchzugehen und manche zu verändern. Schlussendlich scheint das Problem behoben. Der Social Engineer hat erfolgreich ein Vertrauensverhältnis zu seinem zukünftigen Opfer aufgebaut. Wenige Tage später wird er sie erneut kontaktieren und sie wird ihm bereitwillig einen Fernzugriff auf ihren PC freigeben.

Betrachtet man nun die drei Kategorien von Social Engineering – Human-based Social Engineering, Technology- based Social Engineering und Reverse Social Engineering – so stellt man fest, dass Reverse Social Engineering eine Unterkategorie von Human- based Social Engineering ist. Jede Reverse Social Engineering Attacke zählt auch als Human- based Social Engineering Attacke, nicht jedoch umgekehrt. Reverse Social Engineering zeichnet sich durch die Bewerbung des Social Engineers aus, was eine besonders tückische Manipulation des Opfers darstellt.

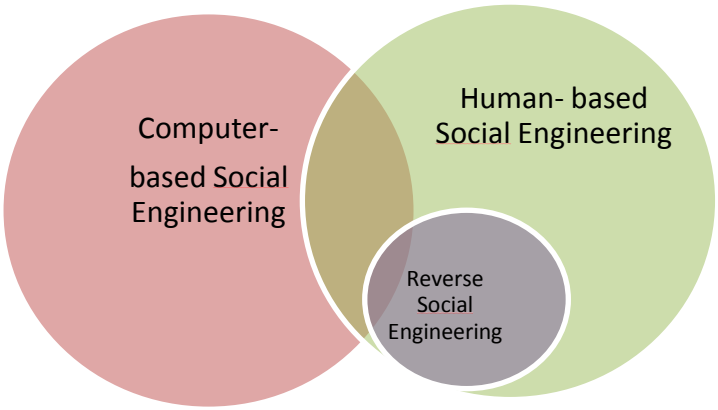



**Abbildung 25: Social Engineering Kategorien**

In Abbildung 25 werden die Social Engineering Kategorien visuell als Venn Diagramm dargestellt. Da es Attacken gibt, die nicht eindeutig nur einer Kategorie zugeordnet werden können, gibt es auch entsprechende Schnittflächen.

In dieser Arbeit liegt der Fokus auf Human- based Social Engineering Attacken, was somit auch Reverse Social Engineering Attacken beinhaltet.

## 4.3 Menschliche Faktoren von Social Engineering

Nach [Cial07], [Lari06] und [HaPr09] nützt ein Social Engineer die folgend erläuterten Konstanten menschlichen Verhaltens für die Beeinflussung fremder Personen schamlos aus. In einem Sicherheitskonzept stellen sie die „Achillesferse des Menschen“ dar. Menschliche Verhaltensweisen sowie die Wirkungsweise des Social Engineering Angriffs werden in diesem Kapitel beschrieben.

In der folgenden Tabelle werden die verschiedenen Faktoren menschlichen Verhaltens erläutert und gegenübergestellt.

| Verhalten | Beschreibung | Beispiel |
|---|---|---|
| Reziprozität | Man fühlt sich verpflichtet, Gefälligkeiten | Nach einer Gratisprobe kauft man eine Ware |

| | | |
|---|---|---|
| | „zurückzuzahlen“ | |
| Konsistenz | Wir sind bestrebt, in Übereinstimmung mit früherem Verhalten zu handeln | Eine Zusage kann man schwer zurücknehmen |
| Soziale Bewährtheit | Wir orientieren uns an andere | Produkte werden als Top Seller beworben |
| Sympathie | Sympathischen Menschen hilft man lieber | Attraktive Modells werden in der Werbung eingesetzt |
| Autorität | Anweisungen von Autoritäten werden weniger in Frage gestellt | Ein Arzt gibt seinen Patienten eine Anweisung |
| Knappheit | Knappe Ressourcen haben einen höheren Wert | Von einer Ware ist nur mehr ein Stück lagernd |

**Tabelle 3: Social Engineering und Faktoren menschlichen Verhaltens, basierend auf [Cial07], [Lari06] und [HaPr09]**

### 4.3.1 Reziprozität

Reziprozität, also das Prinzip der Gegenseitigkeit, bezeichnet das Gefühl, dass wir Gefälligkeiten „zurückzahlen“ müssen. Wenn uns jemand einen Gefallen tut, sind wir geneigt, diesen Gefallen zu erwidern. Es stellt unser Bemühen dar, dass wir anderen Personen nichts schuldig sein wollen, der Mensch ist also bemüht, erhaltene Leistungen zurückzugeben.

Aus evolutionstheoretischer Sicht haben Menschen im Laufe der Sozialevolution gelernt, anderen etwas zu schenken und konnten damit rechnen, dass das Geschenk etwas beim Gegenüber bewirkt, dass es also nicht völlig umsonst war. Das hat den Austausch von Ressourcen und Ideen gefördert. Es konnten sich Systeme gegenseitiger Unterstützung und des Handels entwickeln. Menschliche Gesellschaften haben einen deutlichen Wettbewerbsvorteil von der Reziprozitätsregel. [Cial07]

Aus soziologischer Sicht ist Reziprozität Basis zum Aufbau von Vertrauen und Beziehungen. Wer nicht dazu bereit ist, etwas zu geben bzw. zurückzugeben, gilt nicht als sympathisch, sondern wird als undankbar, egoistisch und geizig angesehen. Individuen versuchen, nicht in non-reziproken Beziehungsverhältnissen zu leben. Mangel an Reziprozität ist daher besonders problematisch, da er dem Streben nach Gleichgewicht als Grundmoment sozialer Beziehungen widerspricht. [Otto03]

Ein Social Engeneer nützt den Reziprozitätsfaktor, um Menschen dazu zu bringen, Wünsche und Anforderungen zu erfüllen, die sie ohne das Gefühl etwas schuldig zu sein, niemals nachkommen würden. Hierbei wurde in einen Experiment von Dennis Regan [Rega71] empirisch bewiesen, dass der Einfluss der Reziprozität stärker als das Sympathiegefühl ist. Es muss also keine besondere Sympathie zwischen den Social Engineer und dem Opfer existieren, wenn die Reziprozitätsregel ausgenutzt wird. Wird hingegen ohne Ausnutzung der Reziprozitätsregel direkt derselbe Wunsch oder die Anforderung geäußert, spielt Sympathie eine große und ausschlaggebende Rolle.

### 4.3.2 Konsistenz

Entsprechend der Konsistenztheorie von Klaus Grawe [Graw98] [Graw04] gibt es vier sogenannte Grundbedürfnisse, welche ein Mensch zu seinem Wohlergehen erfüllen muss. Bei den Grundbedürfnissen handelt es sich um den Wunsch nach Bindung, nach Selbstwerterhöhung, nach Kontrolle und nach Lustgewinn beziehungsweise Unlustvermeidung. Im Laufe des Lebens entwickelt jeder Mensch Strategien, diese evolutionären Bedürfnisse zu befriedigen. Die Strategien werden als motivationale Schemata gespeichert und können entweder der Annäherung und Erschaffung eines Zielzustandes dienen (Bedürfnisbefriedigung), oder aber der Vermeidung eines bestimmten, unerwünschten Zustandes (Schutz vor Verletzung der Bedürfnisse). [Frie05] Je ausgeglichener die Grundbedürfnisse sind und je kontinuierlich erfolgreich sich die motivationalen Schemata herausstellen, umso mehr erhöht sich die Konsistenz und desto gesünder ist der Organismus, beziehungsweise im umgekehrten Fall umso ungesünder ist der Organismus (siehe dazu [Frie05]).

Konsistenz ist auch ein wesentlicher Bestandteil des menschlichen Verhaltens. Permanent sind wir gezwungen, Entscheidungen zu treffen. Dabei sind wir bestrebt, einmal getroffene Entscheidungen nicht umzustoßen und uns in ähnlichen Situationen gleich zu verhalten. Diese Konsistenz in der Verhaltensweise wird als sympathisch empfunden.

Ein Social Engineer nützt dieses Verhalten aus, indem er seinen Angriff in frühere Entscheidungen seines Opfers einbettet. Hierbei gilt insbesondere das Sprichwort: „Wer A sagt, muss auch B sagen“. Der Social Engineer könnte die Strategie verfolgen, sein Opfer in eine Vielzahl von aufbauenden Entscheidungen nach und nach zu zwingen, die eine immer größere

Tragweite haben. Während die erste Anfrage noch harmlos war, steigert sich die Gefährlichkeit kontinuierlich. Das Opfer ist aufgrund des Konsistenzbedürfnisses sehr schwer in der Lage, eine Abfrage abzuweisen, wenn es mehrere ähnliche zuvor angenommen hat.

Ein ähnliches Verhalten findet man nicht nur im menschlichen Verhalten, sondern auch in sicherheitstechnischen Bereichen. Ein Intrusion Detection System, welches nicht nur nach fixen Mustern sucht, sondern neue Angriffsmethoden als Anomalien erkennen und verhindern versucht, basiert auf Erfahrung [Fars09]. Die Erfahrung ergibt sich aus der Auswertung von statistischen Daten über einen gewissen Zeitraum, wobei das Intrusion Detection System zu große Veränderungen (Schwellenwert) als einen Angriff einstuft. Wenn nun ein Angreifer in einer kontinuierlichen Attacke den Schwellenwert nie überschreitet, aber stets annähert, wird der Schwellenwert vom Intrusion Detection System über die statistische Heuristik langsam erhöht, bis eine Sicherheitslücke für den Angreifer entsteht.

### 4.3.3 Soziale Bewährtheit

In [Cial07] wird soziale Bewährtheit folgendermaßen definiert:

Wir betrachten ein Verhalten in einer gegebenen Situation in dem Maß als richtig, in dem wir dieses Verhalten bei anderen beobachten. Ob es darum geht, was mit einer leeren Popcornschachtel im Kino zu tun ist, wie schnell man auf einem bestimmten Straßenabschnitt fahren darf oder auf welche Weise man bei einem Abendessen mit Freunden das Hühnchen essen soll, stets ist uns bei der Beantwortung dieser Fragen das Verhalten anderer eine wichtige Orientierungshilfe.

Beispielweise nutzen viele Überzeugungsstrategien der Werbung (siehe dazu [Petr07]) das Prinzip der sozialen Bewährtheit. Typische Aussagen wie „30 Millionen Konsumenten können nicht irren“ sollen den Kunden suggerieren, dass es sich um ein gutes Produkt handelt und zu einer raschen Kaufentscheidung führen.

Grundsätzlich tritt das Prinzip der sozialen Bewährtheit in Situationen auf, in denen sich der Mensch unsicher fühlt. Man kann die Auswirkung einer Entscheidung nicht abschätzen, man fühlt sich unsicher, man fühlt sich nicht ausreichend informiert oder ist in einer besonders stressvollen Situation. Das alles führt zu dem Punkt, an dem man sich die Frage stellt, wie sich

wohl andere entscheiden würden. Hierbei gilt, dass man sich besonders an Vorbildern oder Personen orientiert, die einem besonders ähnlich sind. Cavett Roberts, Gründer der National Speakers Association [theNSA], prägte die Aussage: Da 95% der Menschen Nachahmer und nur 5% Vormacher sind, lassen sich Menschen mehr durch die Handlungen anderer Menschen überzeugen, als durch jedes andere Argument.

Ein Social Engineer nutzt das Prinzip der sozialen Bewährtheit, indem er dem Opfer gegenüber in einer stressigen Entscheidungssituation bewusst die Information zukommen lässt, wie andere Kollegen sich angeblich verhalten.

### *4.3.4 Sympathie*

Sympathie ist oftmals ein ganz entscheidender Erfolgsfaktor für einen Social Engineer, da man sympathischen Menschen bereitwilliger hilft beziehungsweise ihren Anweisungen eher folgt.

In der Sozialpsychologie wurden mehrere Einflussfaktoren identifiziert, welche einen Menschen für uns sympathisch oder unsympathisch erscheinen lassen. Die Einflussfaktoren wurden durch Experimente mit Versuchspersonen nachgewiesen:

**Ähnlichkeit, Sympathie und Interaktion** stehen in Wechselwirkung und in direktem Zusammenhang.

- Versuchspersonen, denen ein gemeinsames Zimmer zugewiesen wurde, wurden oft zu Freunden. [Newc61]
- Versuchspersonen bekamen eine vage Information über zwei Frauen. Mit einer davon erwarteten sie ein vertrauliches Gespräch zu führen. Diese Frau wird als sympathischer eingeschätzt. [DaBe87]
- Bei im Experiment gezeigten Personen beeinflusst die Häufigkeit des Sehens deren Beliebtheit. [Swap77]
- Die Vertrautheit mit Menschen oder anderen Reizen erhöht deren Akzeptanz. [Born89]

Im Wesentlichen bestimmen zwei Kreisläufe die Wechselwirkung. Je mehr man mit jemand interagiert, umso sympathischer wird uns diese Person und umso mehr Ähnlichkeiten verbinden wir mit der Person. Je mehr Ähnlichkeit vorhanden ist, umso häufiger interagieren wir mit jemandem.

Ähnlichkeiten entdeckt man durch Interaktion. Je mehr man interagiert, umso mehr Ähnlichkeiten findet man. Je ähnlicher uns Menschen sind,

umso sympathischer wirken sie auf uns, was wieder den Grad und die Häufigkeit der Interaktion steigert.

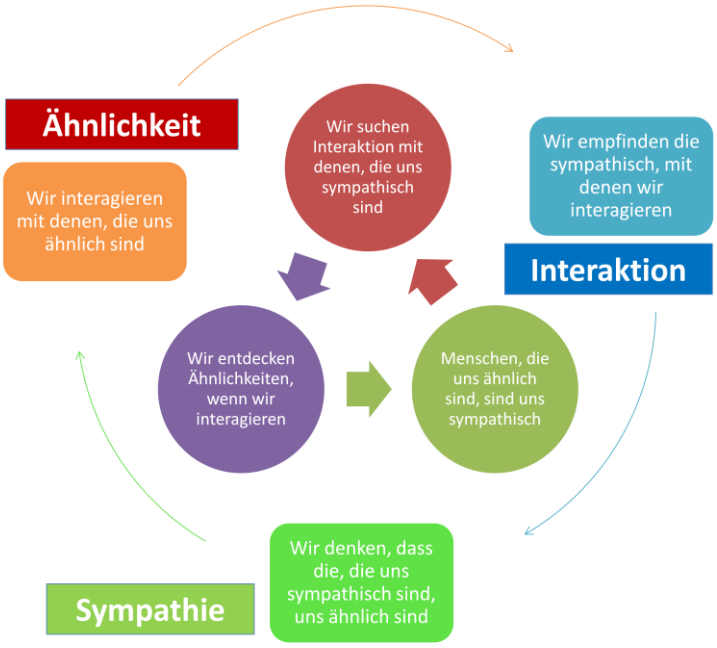



**Abbildung 26: Sympathie - Interaktion – Ähnlichkeit [Krol05]**

**Physische Attraktivität** wird von Evolutionspsychologen als Signal für Gesundheit, Jugend und Fruchtbarkeit angenommen. Sie nehmen auch an, dass die Evolution Frauen prädisponiert, männliche Züge zu bevorzugen, die die Fähigkeit signalisieren, Ressourcen zu erwerben und zu beschützen. [Buss89] [LiBa02]

- Schönen Menschen werden in der Regel weitere (soziale und intellektuelle) positive Eigenschaften zugeschrieben. [DBWB72] Gezeigt wurde dieser Umstand in einem Experiment, in dem Versuchspersonen weibliche Gesichter (Photographien) von unterschiedlicher Attraktivität bewerten sollten bezüglich Schönheit und den Ausprägungsgrad verschiedener Persönlichkeitsmerkmale (klug, gesellig, selbstsicher etc). [Cunn86]
- Je attraktiver eine Person ist, desto positiver wird sie bewertet. [LaKa00]
- Die Attraktivität hängt ab von:
    - der Feminität des Gesichts [RhZe01]
    - der Jugendlichkeit [BuKe98] [PeBe99]

- der Schlankheit [GaTo93]
- der Ehrlichkeit [Yarm00]
- dem Gehalt [HaBi94]

Sympathie ist auch durch die **Assoziation mit anderen Dingen** beeinflusst. Die Assoziationen können unterschiedlichster Natur sein. Lernt man beispielsweise eine Person in einer angenehmen Umgebung kennen, so ist das ein Einflussfaktor, ob man mit einer Person ein positives Gefühl verbindet. Hat die Person beim Kennenlernen eine unangenehme Botschaft überbracht, so bleibt dieser negative Eindruck haften. [Fels01] [Herk96]

Durch **Sympathie uns gegenüber** wirken Personen sympathischer. Wir mögen Personen, die uns sympathisch finden, aber auch umgekehrt meiden wir Personen, die uns unsympathisch finden. Erklären kann man dies leicht durch die Regel der Reziprozität.

### *4.3.5 Autorität*

Eine ganz besondere Situation, in der Autorität eine Rolle spielt, stellt das Gespräch zwischen Arzt und Patient dar. In einer Studie von [Tim08] wurden sprachliche Abläufe und Prozeduren innerhalb der Kommunikation identifiziert, womit ein Arzt den Patienten versucht zu beeinflussen.

In der Studie wird festgestellt, dass zumeist der Arzt die Patienten nicht ausreden lässt. Ausführungen des Patienten werden vom Arzt in der Regel unterbrochen, er hört dem Patienten nicht zu. Die Krankengeschichte und der Verlauf werden mittels knapper Ja-Nein-Fragen abgefragt. Bewusst erhöht der Arzt die Lautstärke der Stimme, als sich der Patient ablehnend zum Erhalt einer Spritze äußert. Gekonnt, an einen Vortrag auf der Universität erinnernd, erklärt der Arzt die Notwendigkeit der Behandlung, wobei er sich nicht scheut, viele Fachwörter und Wirkstoffe zu nennen, um seine Fachkompetenz klar zu unterstreichen. Der Patient wird verbal unter Druck gesetzt, doch der vorgeschlagenen Therapie einzuwilligen.

Als Gründe für die Machtausübung durch Ärzte macht [Tim08] vor allem Zeit- und Aufwandsersparnis aus. Es würde viel Zeit und Aufwand bedeuten, den Patienten effektiv zu beraten, ihnen ihre aktuelle Situation und die verschiedenen Optionen einer Behandlung zu erklären. Die Abwägung, welche Therapie die erfolgversprechendste ist, wird nicht gemeinsam mit dem Patienten erörtert, sondern allein vom Arzt entschieden. Es würde schlichtweg zu lange dauern, in Diskurs mit den Patienten zu

treten, weshalb er bewusst autoritär auftritt, sich rein an den Symptomen orientiert und die Wünsche des Patienten ausblendet. "Die heute oft geforderte kooperative Entscheidungsfindung findet oft nicht statt", fasst [Tim08] zusammen.

Autorität ist anerkannte, geachtete Macht, die zugleich bewundert und gefürchtet wird. [SoPa03] Entsprechend [Schu02] kann der Begriff der Autorität folgendermaßen definiert werden: Autorität ist das Ansehen und die Macht bei Personen aufgrund äußerer Befugnis und innerer Überlegenheit. Autorität bedeutet eine menschliche Möglichkeit, auf andere Menschen positiv einzuwirken. Man kann aber auch sagen: sozialer Einfluss, der entsteht, indem Personen, Gruppen oder Institutionen von anderen Personen in irgendeiner Hinsicht eine Überlegenheit zugesprochen wird und diese auch Anerkennung findet. [ZRAV60] versteht unter Autorität das maßgebende Ansehen einer Persönlichkeit, deren Charakter, persönliche Lebensführung und Leistung über jeden Zweifel erhaben sind und daher allgemein als Vorbild und Beispiel anerkannt werden.

Aus Sicht des Social Engineers ist gerade der Umstand, dass Entscheidungen und Weisungen von Personen höherer Autorität weniger in Frage gestellt werden, ein wesentlicher Erfolgsfaktor. Durch Identitätsdiebstahl nimmt der Social Engineer eine entsprechend autoritäre Rolle ein. Grundsätzlich gibt es unterschiedliche Arten von Autoritäten. Legitime Macht, meist im Sinne formaler, objektiver, zugeordneter Autorität wird als Amtsautorität bezeichnet. Funktional bedingte, informale Macht wird hingegen Sachautorität genannt. Hierunter zählen Autoritäten aufgrund hoher Sach- und Fachkenntnis, welche als Experten gelten. Eine besondere Art der Autorität ist jene, die sich aufgrund einer besonderen persönlichen Ausstrahlung ergibt, welche oftmals einfach nur als Charisma bezeichnet wird.

### 4.3.6 Knappheit

Das Knappheitsprinzip besagt, dass Informationen oder Ressourcen, die nicht für alle verfügbar sind, einen höheren Stellenwert für Menschen haben und als wertvoller angesehen werden, als jene, die für alle verfügbar sind. Informationen oder Ressourcen, die bedroht sind, knapp zu werden, haben einen noch höheren Stellenwert und gelten als noch wertvoller als jene, die immer schon knapp waren.

In einem Experiment von Worchel Stephens [Worc75] wurde das Urteil der Versuchspersonen über Kekssorten in Abhängigkeit von deren Verfügbarkeit untersucht. Die Versuchsanordnung war wie folgt:

Zwei Gruppen bewerteten verschiedene Kekssorten, wobei der einen ein großer Vorrat von allen Keksen zur Verfügung stand. Die andere Gruppe erhielt den gleichen Vorrat an Keksen mit Ausnahme von einer Sorte, von der sie nur sehr wenige Kekse erhielten.

Es zeigte sich, wenn die Knappheit von Anfang an bestand, dies wenig Einfluss auf die Urteile über die Kekse hatte. Waren die Kekse hingegen anfänglich in ausreichender Zahl vorhanden, wurden aber im Laufe des Experiments knapp, wurden die Kekse höher bewertet. Hierbei entstand nämlich entsprechend der Versuchsbedingung eine soziale Bedrohung, da andere Versuchspersonen angeblich auch noch Kekse brauchten. Die sogenannten Reaktanzeffekte, also eine Abwehrreaktion gegen innere oder äußere Einschränkungen, waren somit stärker, als wenn die Kekse in ausreichender Menge zur Verfügung standen.

Die Wahrnehmung, dass andere Versuchspersonen auch einen Anspruch auf die Kekse haben, genügt also zur Auslösung von Reaktanz.

In der Versuchsbedingung der nicht-sozialen Bedrohung, bei dem es angeblich zu einem Irrtum bei der Verteilung der Kekse kam, fielen die Reaktanzeffekte deutlich schwächer aus.

Das reaktante Verhalten, das aus dieser Haltung erwächst, besteht darin, die nunmehr verbotenen Handlungen – insgeheim oder offensichtlich – weiterhin auszuführen. Auf diese Weise möchte sich die betroffene Person diese Freiheiten gleichsam zurückerobern, auch wenn dies gegebenenfalls gar nicht mehr möglich ist. Typisch für die Reaktanz ist eine Aufwertung der eliminierten Alternative, das heißt gerade diejenigen Freiheitsgrade, die der Person genommen wurden, werden nun von dieser als besonders wichtig erlebt. Insbesondere kann die nun verbotene Handlungsmöglichkeit der Person zuvor völlig unwichtig gewesen sein. Im Extremfall hat die Person von dieser Handlungsmöglichkeit vor dem Eintreten der Beschränkung nie Gebrauch gemacht, übt die Handlung aber seit dem Eintreten der Einschränkung aus.

Ein Social Engineer nutzt bewusst das Prinzip der Knappheit. Er setzt das Opfer unter Druck, indem er die Zeit zur Entscheidungsfindung sehr kurz ansetzt. Des Weiteren betont er die negativen Konsequenzen bei einer Fehlentscheidung oder bei einer Verzögerung der Entscheidung, wodurch

vom Social Engineer aufgezeigte und angebotene Alternativen für das Opfer aufgrund des Reaktanzeffekts zwangsläufig wesentlich attraktiver wirken.

## 4.4 Social Engineering Techniken

Ein typischer Social Engineering Angriff durchläuft in Anlehnung an [Gartn02] basierend auf den Social Engineering Circle von [MiSi02] die folgenden vier Phasen – Informationsbeschaffung, Beziehungen aufbauen, Beziehungen ausnützen und Ausführung. Diese vier Phasen werden iterativ immer wieder durchlaufen, bis der Social Engineer sein Ziel erreicht hat.

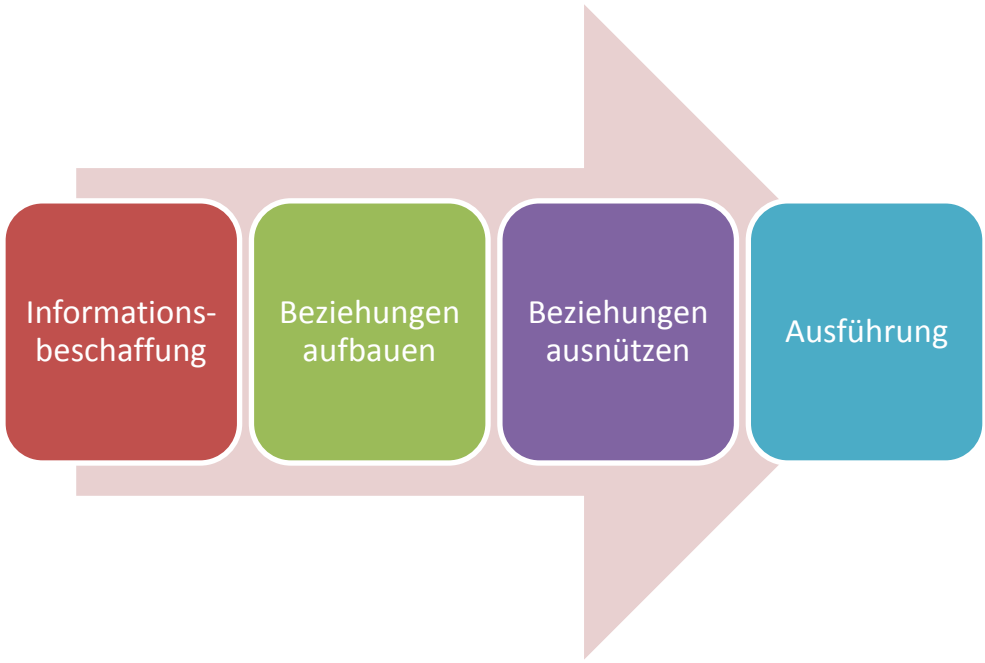



**Abbildung 27: Phasen einer Social Engineering Attacke [Gartn02]**

### *4.4.1 Informationsbeschaffung*

Die erste Phase ist die Informationsbeschaffung. Der Social Engineer verwendet eine Vielzahl unterschiedlicher Techniken, um Informationen über sein Angriffsziel zu sammeln. Hierbei werden zuerst die öffentlichen Informationen studiert, wie zum Beispiel den Internetauftritt einer Firma, Informationsprospekte, Mitarbeiter der Firma, Partnerfirmen usw. Anschließend werden Detailinformationen recherchiert. Möglichst umfassende Informationen über Mitarbeiter, deren soziale Netze, deren

Hobbies usw. werden zusammengetragen. Informationsquellen hierfür sind oftmals Webseiten zur Herstellung und Pflege sozialer Netzwerke, wie zum Beispiel StudiVZ, MySpace, Facebook, LinkedIn oder XING. Der Social Engineer kann durch Unterstützung mittels Tools, welche die Recherchetätigkeit automatisieren (siehe dazu [HuKo09]), sehr schnell und effizient Informationen zusammentragen. In [Hube09] wird ein derartiges Werkzeug detailliert analysiert und dessen Effektivität mittels Experimenten nachgewiesen.

Es wurden die folgenden fünf Organisationen ausgewählt:

- Organisation 1: eine internationale High Tech Firma
- Organisation 2: ein internationale Unternehmen
- Organisation 3: ein Finanzdienstleistungsinstitut
- Organisation 4: ein internationales Ingenieurbüro
- Organisation 5: ein internationaler Telekommunikationskonzern

Das Tool zur automatischen Informationssuche für einen späteren Social Engineering Angriff sollte männliche Singles finden, die in diesen Organisationen arbeiten.

In einem ersten Schritt durchsuchte das Tool ein soziales Netzwerk (Facebook) mittels der dort zur Verfügung gestellten Suchmasken. In zwei anschließenden Schritten wurden zuerst nur jene Personen weiter verfolgt, die Mitglieder in dem Netzwerk der Firma waren, danach nur mehr jene Mitglieder, die persönliche Daten zur Einsicht freigegeben hatten. Daraus wurden pro Organisation durchschnittlich acht Personen identifiziert, die mit sehr hoher Wahrscheinlichkeit in der jeweiligen Organisation arbeiten und männliche Singles sind. Die automatische Suche dauerte durchschnittlich 44 Minuten, bis man geeignete Zielperson für einen Social Engineering Angriff gefunden hatte.

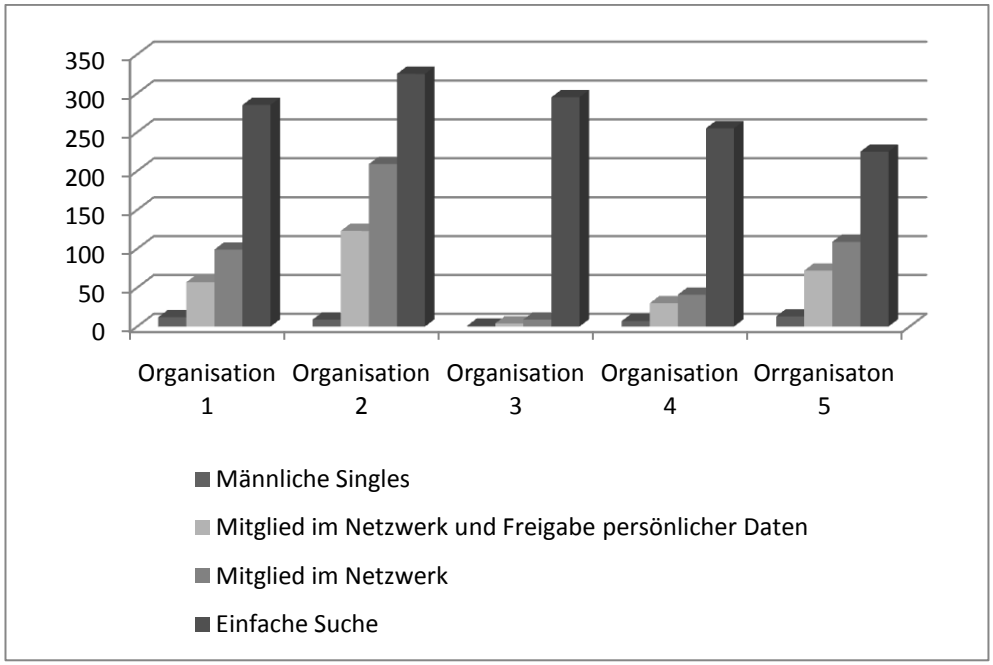



**Abbildung 28: Informationsbeschaffung durch automatisierte Zielpersonensuche [Hube09]**

Neben den sozialen Netzwerken gibt es eine unendliche Vielzahl unterschiedlicher anderer potentiell interessanter Informationsquellen für einen Social Engineer.

Damit der Social Engineer eine bestimmte Identität annehmen kann, muss er – zumindest für die Dauer des Angriffs – glaubhaft eine Expertenrolle einnehmen können. Er muss das entsprechende Fachvokabular im Vorfeld erlernen, die Unternehmenskultur und -strukturen begreifen und vieles mehr. Durch Kenntnis bestimmter Vorgänge in einer Organisation kann sich der Angreifer als Firmenmitglied ausgeben. Da er als Zugehöriger eingestuft wird, bekommt der Social Engineer einen Vertrauensbonus und Bedenken ihm gegenüber schwinden bei der Zielperson.

### *4.4.2 Beziehungen aufbauen*

Neben der Informationsbeschaffung ist eine weitere Grundvoraussetzung für einen erfolgreichen Social Engineering Angriff, Beziehungen aufzubauen. Hierbei bringt sich der Social Engineer in die richtige soziale Position. Beispielsweise macht er seine angenommene Identität der Zielperson bekannt, unterstützt das Opfer und baut ein Vertrauensverhältnis auf. Diese Phase kann innerhalb eines Telefonats durchlaufen werden, kann aber mitunter Wochen und Monate dauern.

Häufig übernimmt der Social Engineer eine der folgenden Rollen, über die er Verbindung zu seiner Zielperson aufbaut und Beziehungen errichtet:

- **Firmenmitglied**: Einem Kollegen, selbst wenn er einem unbekannt ist, schenkt man automatisch Vertrauen. Der Kollege benutzt das gleiche Vokabular, beklagt dieselben Dinge im Unternehmen, kämpft mit denselben Problemen und Ängsten – er wirkt damit sofort sympathisch. Wenn der Kollege noch dazu hilfesuchend in einer Notlage ist, so verstärkt sich der Effekt noch weiter und die Zielperson wird ohne Bedenken gerne helfen.
- **Mitglied einer vertrauenswürdigen Organisation, Autorität**: Am Mittwoch, den 9. Jänner 2008, betritt ein angeblicher Mitarbeiter der Firma AT Systems die BB&T Bank in Wheaton. Nachdem er dem Bankangestellten erklärt hat, dass er den üblichen AT Systems Mitarbeiter krankheitsbedingt vertritt, werden ihm US$ 850.000 zum sicheren Transport übergeben. Erst als am nächsten Tag wieder ein AT Systems Mitarbeiter die Bank betritt, wird der Schwindel erkannt. Stellt sich der Social Engineer glaubhaft als Mitglied einer bekannten, eventuell auch öffentlichen Institution vor, die zusätzlich noch mit Autorität versehen ist, vertraut ihm die Zielperson.
- **Wartungspersonal und Support**: Will der Social Engineer so wenig wie möglich auffallen, sich aber trotzdem sehr frei im Unternehmen bewegen, so bietet sich die Rolle eines Wartungsarbeiters oder einer Reinigungskraft an. Eine Reinigungskraft wird von den Mitarbeitern des Unternehmens kaum wahrgenommen und aufgrund der sozialen Stellung als ungefährlich eingestuft.

### 4.4.3 Beziehungen ausnutzen

Nachdem der Social Engineer eine Beziehung zur Zielperson aufgebaut hat und sich somit in eine gute soziale Position für einen Angriff gebracht hat, beginnt er, die Beziehungen auszunützen. Nach und nach schöpft er bestimmte Informationen ab, wie Urlaubszeiten der Mitarbeiter, Zugangsdaten, und vieles mehr, die ihn seinem Ziel näherbringen.

Er kann aber auch seine sozialen Fähigkeiten einsetzen, um Menschen so zu manipulieren, unrechtmäßige Handlungen durchzuführen, wie das Anlegen eines Benutzeraccounts, das Umsetzen eines Passworts oder das Verändern von Benutzerprivilegien.

Basis sowohl für die Informationsgewinnung als auch für das Initiieren unrechtmäßiger Handlungen sind die in Kapitel 4.3 vorgestellten Faktoren menschlichen Verhaltens wie Reziprozität, Sympathie, Autorität, Knappheit, soziale Bewährtheit und Konsistenz.

### 4.4.4 Ausführung

Hat der Social Engineer eine Zugriffsmöglichkeit auf sein eigentliches Ziel, so kommt es zur Ausführung des endgültigen Angriffs, um beispielsweise eine bestimmte Informationen zu stehlen, eine Webseite zu verunstalten oder sich Geld zu überweisen.

Der Sozialpsychologe und Profiler Max Kilger fasst die möglichen Ziele eines Social Engineers in [Hone04] zusammen und benennt sie entsprechend der Anfangsbuchstaben als MEECES (Money, Ego, Entertainment, Cause, Entrance into social groups, Status).

| # | Ziel | Beschreibung/ Beispiel |
|---|---|---|
| M | Geld | Gestohlene Kreditkartennummern, bezahlte Industriespionage und vieles mehr |
| E | Ego | Das Unmögliche möglich machen, einbrechen in als sicher geltende Institutionen oder eine persönliche Herausforderung meistern |
| E | Unterhaltung | Unterhaltung für einen gelangweilten Teenager, Kuriosität |
| C | Streitsachen | Rache, divergente politische oder ideologische Auffassungen |
| E | Zugehörigkeit | Zugehörigkeit zu elitären Hackergruppen und gegenseitiger Austausch von Fachwissen und Berichten |
| S | Status | Je schwieriger es ist, ein Ziel zu erreichen, umso reizvoller ist es |

**Tabelle 4: Ziele eines Social Engineers [Hone04]**

## 4.5 Social Engineering Vertrauens- und Angriffsmodell

In [Lari06] wird das in Abbildung 29 und Abbildung 30 dargestellte Social Engineering Vertrauensmodell (Social Engineering Trust Model) und das Social Engineering Angriffsmodell (Social Engineering Attack Model) beschrieben.

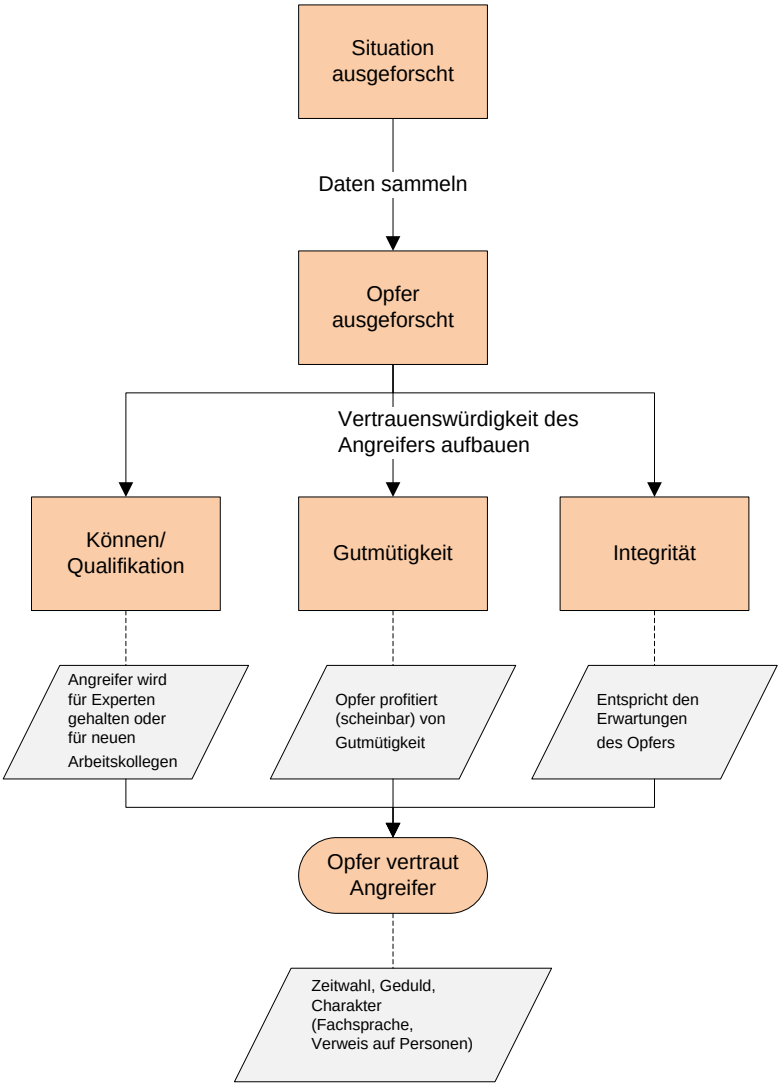



**Abbildung 29: Social Engineering Vertrauensmodell [Lari06]**

[Lari06] beschreibt im Social Engineering Vertrauensmodell, wie ein Social Engineer eine Vertrauensbasis zu einer Person aufbaut, von der er Informationen für einen tiefergehenden Social Engineering Angriff benötigt. Nach einer initialen Recherche nützt der Social Engineer verschiedene Techniken und menschliche Verhaltensweisen, wie sie auch in Kapitel 4.3

beschrieben werden, um eine Person davon zu überzeugen, vertrauenswürdig zu sein und dringend eine bestimmte Information zu benötigen.

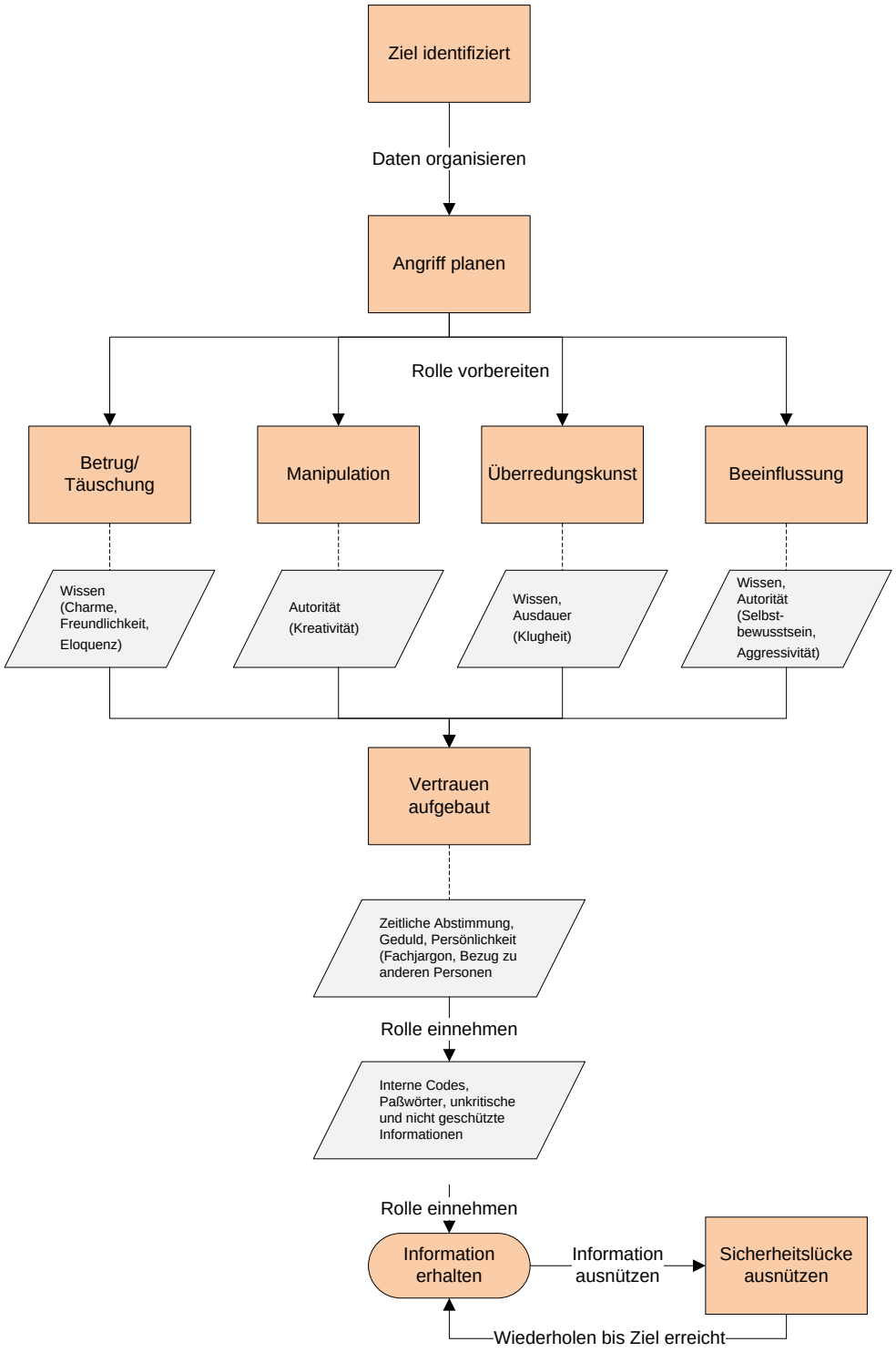



**Abbildung 30: Social Engineering Angriffsmodell [Lari06]**

Im Social Engineering Angriffsmodell nach [Lari06] werden die verschiedenen Schritte der Informationsbeschaffung eines Social Engineers dargestellt. Analog zum Vertrauensmodell nützt der Social Engineer seine Fähigkeiten, um Vertrauen aufzubauen und nach und nach Informationen zu sammeln, bis er sein Ziel erreicht hat. Das Modell verdeutlicht, dass ein Social Engineering Angriff üblicherweise nicht in einem Schritt durchgeführt wird, sondern viel Zeit und Aufwand in Anspruch nimmt. Durch gezielte Manipulationen, Täuschungen, Überreden und Beeinflussungen nähert sich der Angreifer Schritt für Schritt dem eigentlichen Ziel, was beispielsweise der Zugriff auf sensible Informationen, Industriespionage, Betrug, Identitätsdiebstahl oder einfache Zerstörung sein kann.

# 5 Identifikation von allgemeinen Sicherheitsgrundsätzen in Service Operation Prozessen

In den vorigen Kapiteln wurde ein Überblick von ITIL als Best Practice Guide für IT Service Management wiedergegeben. Anschließend wurde die Gefahr von Social Engineering Attacken dargestellt. Hierzu wurde gezeigt, welche menschlichen Verhaltensweisen ein Social Engineer für seinen Angriff ausnützt und welche Techniken angewandt werden.

Um die Wirksamkeit von ITIL gegen Angriffe eines Social Engineers zu verifizieren, werden nun in Anlehnung an [Schn01] und [Sunz88] in diesem Kapitel allgemeine Sicherheitsgrundsätze gegen Human- based Social Engineering Attacken in Service Operation Prozessen identifiziert. In den Artikeln [Kuhn07], [Marq08] und [Weil08] werden Maßnahmen angeführt, welche allgemein die Informationssicherheit in Unternehmen durch ITIL steigern. Diese werden in der folgenden Analyse im Kontext von Social Engineering berücksichtigt.

Die Sicherheitsgrundsätze Choke Points verwenden, Authentizität sicherstellen, gut planen und sich daran halten, Risiko durch Aufteilung verringern, gestaffelte Abwehr, Einfachheit, das schwächste Glied sichern und in Frage stellen sind wesentliche Eckpfeiler von Sicherheit. Gezeigt wird die allgemeine, historische und gegenwärtige Gültigkeit der Sicherheitsprinzipien durch Beispiele aus der Vergangenheit oder anderen Themenbereichen und Fachrichtungen, wie Medizin, Militärstrategie oder Rechtswissenschaft.

Anschließend wird erläutert, wie sich die Sicherheitsgrundsätze in den Best Practice Empfehlungen von ITIL wiederfinden und warum sie Human-based Social Engineering Angriffe erschweren, erkennen oder gänzlich verhindern. Aus diesem Kapitel wird der in Kapitel 7 zusammengefasste auf ITIL basierende Maßnahmenkatalog gegen Social Engineering abgeleitet.

## 5.1 Choke Points verwenden

Unter Choke Points versteht man Nadelöhre, durch die man Benutzer durchzwingt. Ähnlich wie bei Drehkreuzen in Bahnhöfen erhält man

dadurch einen besseren Überblick über die Geschehnisse sowie eine bessere Steuerungsmöglichkeit.

*Choke Points haben militärisch eine große Bedeutung. Eine natürliche Geländeeigenschaft, wie sie zum Beispiel bei Bergpässen gegeben ist, oder angelegte Bauwerke, wie zum Beispiel eine Brücke über einen Burggraben, sind selbst von wenigen, gut organisierten und entschlossenen Verteidigern gegen eine große Übermacht für lange Zeit zu halten. Der Angreifer kann aufgrund des Nadelöhrs nicht seine gesamte Schlagkraft ausspielen. Das bekannteste historische Beispiel hierfür ist die Schlacht bei den Thermopylen, ein Engpass zwischen Kallidromosgebirge und dem Golf von Malia, ca. 480 v. Chr. Der spartanische König Leonidas hielt mit wenig hundert Kriegern dem zahlenmäßig weit übermächtigen Heer, geführt von König Xerxes I, drei Tage lang stand und fügte den Angreifern schwerste Verluste zu. Man muss allerdings darauf achten, dass es keine Möglichkeit gibt, diese Choke Points zu umgehen. Dies wurde auch König Leonidas zum Verhängnis, da die persische Streitmacht einen Umgehungsweg nutzte und so das Nadelöhr zum Verhängnis für den Verteidiger selbst wurde, der leicht ohne jegliche Möglichkeit zur Flucht aufgerieben werden konnte.*

Das Sicherheitsprinzip von Choke Points wird auch in der IT genutzt. Stellt zum Beispiel eine Firewall die einzige Verbindung zwischen Firmennetzwerk und dem Internet dar, kann man sämtliche Zugriffe sehr gut steuern und protokollieren. An diesem zentralen Punkt lassen sich aus technischer und operativen Sicht effizient und effektiv Content Filter, Viren Prüfungen, URL- Filter, SMTP- Filter, SPAM Filter oder Intrusion Detection Systeme etablieren (siehe dazu [Schm03]).

Oftmals wird aber aus Bequemlichkeit, um von zu Hause aus arbeiten zu können, ein Modem an einen der Firmen Computer angeschlossen. Diese Einwahlmöglichkeit umgeht die Firewall und damit sämtliche Sicherheitssysteme. Angreifer suchen nach solchen offen gelassenen Hintertüren. [NoZe03]

Single Point of Contact (SpoC) ist gemäß den Grundprinzipien von ITIL der Service Desk. Hierbei spielt die Art und Weise der Kommunikationsaufnahme keine Rolle. Im Service Desk werden alle Anrufe, E-Mails, Faxe usw. von Kunden entgegengenommen und in Zuge des Incident Management Prozesses (Service Operation, Kapitel 3.2.1), des Request Fulfilment Prozesses (Service Operation, Kapitel 3.2.1) oder Change Management Prozesses (Service Transition, Kapitel 3.2.3)

bearbeitet. Der Service Desk ist auch zentrale Schnittstelle zu den anderen Prozessen, wie zum Beispiel Problem Management, Release Management, Change Management, Service Level Management, Capacity Management und Availability Management.


**Abbildung 31: Zentrale Eigenschaft des Service Desks**

Störungen (Incidents), Anfragen (Service Requests) und Änderungswünsche (Requests for Change) werden vom Service Desk aufgenommen und im Zuge des Incident Managements, des Request Fulfilments beziehungsweise des Change Managments (was in Service Transition eingeordnet ist) behandelt. Anzumerken ist, dass gemäß ITIL V2 ein Service Request ein spezieller Fall eines Incidents war und er wurde auch im Incident Management Prozess behandelt. Dies hat sich bei ITIL V3 zur besseren Unterscheidbarkeit zwischen Störungen und Anfragen geändert. Auch werden Service Requests im neu eingeführten Request Fulfilment Prozess behandelt und nicht mehr im Incident Management Prozess.

Sollten Störungen gehäuft auftreten oder sollte eine Störung von erheblicher Tragweite eintreten, wie zum Beispiel bei einer Service Level Agreement Verletzung aufgrund zu langer Ausfallszeit, so wird ein Problem Ticket (Problem) erfasst und im Problem Management analysiert. Prinzipiell kann aus jedem Prozess ein Problem Ticket für eine dezidierte intensive Analyse

erstellt werden. Sicherheitsvorfälle stellen eine spezielle Unterkategorie von Incidents dar und werden daher in ITIL als Security Incidents bezeichnet. Jeglicher Security Incident sollte jedenfalls nachgelagert über ein übergebenes Problem Ticket durch das Problem Management analysiert werden. Anfragen, die Einrichten oder Veränderung von Berechtigungen, Zugriffsrechten oder andere Benutzerdaten betreffen, werden im Access Management behandelt. In gewisser Weise ist es eine Spezialform des Request Fulfilment zur Behandlung dieser bestimmten Service Requests.

Die folgende Abbildung gibt einen vereinfachten Überblick über das Zusammenspiel der Prozesse und der Begrifflichkeiten.

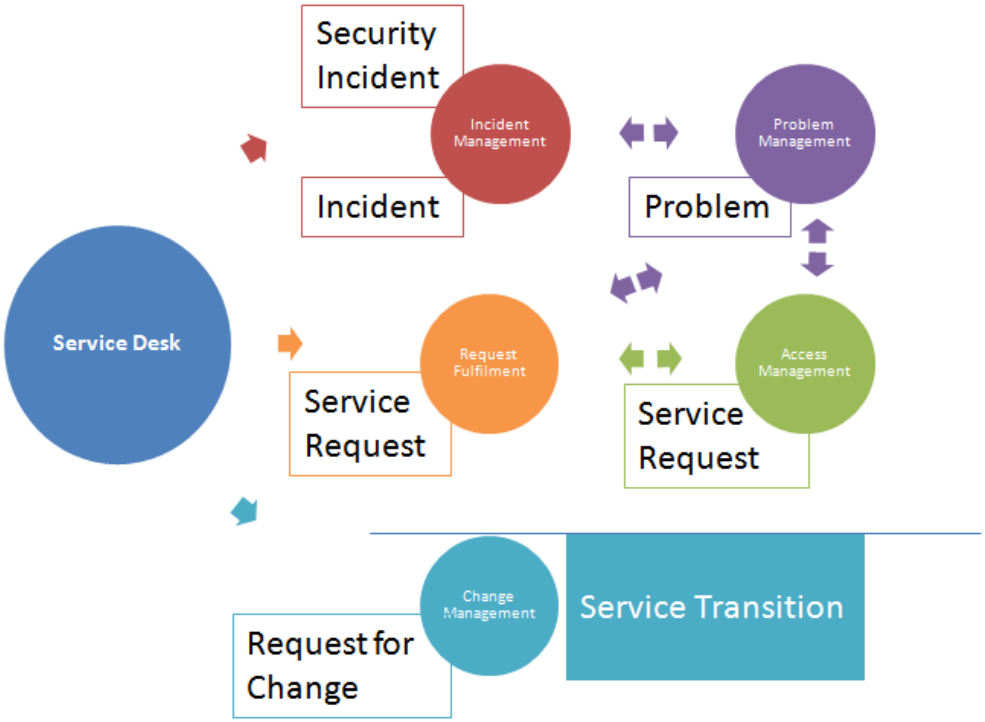



**Abbildung 32: Überblick Service Desk Schnittstellen (vereinfacht)**

Abbildung 32 ist unter anderem dahingehend vereinfacht, da ITIL eine Schnittstelle zwischen Change Management, Release und Deployment Management und Access Management vorsieht. In diesem Falle werden im Access Management nicht Service Requests, sondern Standard- Changes behandelt. Zwecks besserer Lesbarkeit werden sie in der Darstellung weggelassen. Standard- Changes werden in Kapitel 5.6 erläutert.

Jegliche Änderungen und die damit verbundenen Beeinträchtigungen der Services durch Wartungsarbeiten sind dem Service Desk bekannt. Auch hierbei fungiert der Service Desk sowohl firmenintern als auch extern als zentraler Kommunikationsknoten.

Grundsätzlich unterscheidet ITIL mehrere Arten von Service Desks. Kleine bis mittelgroße Unternehmen, die nur an einem Standort ihren Firmensitz haben, betreiben in der Regel einen **lokalen Service Desk**. Hierbei gibt es eine einheitliche Kontaktadresse für alle Anwender. Von einem **zentralen Service Desk** spricht man, wenn mehrere verteilte Organisationseinheiten einen gemeinsamen Service Desk nutzen.

Oftmals ist es sinnvoll, innerhalb des Service Desks eine oder mehrere Untergruppen zu bilden, die ausschließlich zur Behandlung spezifischer Incidents zuständig sind, wodurch nach ITIL so genannte **spezialisierte Service Desk Gruppen** entstehen. Beispielsweise werden alle Windows Arbeitsplätze betreffenden Anfragen nur von einer dafür geschulten Spezialistengruppe behandelt. Die Untergruppe ist aber Teil des Service Desks und unterliegt somit der Fortschrittsüberwachung und den Eskalationsmechanismen des Service Desks.

Ist ein Unternehmen auf mehrere Standorte verteilt, so werden oftmals so genannte **verteilte Service Desks** (in ITIL V3 als Spezialform des lokalen Service Desks angesehen) eingesetzt. Jeder Service Desk hat einen wohl definierten Kundenkreis, die jeweils eine einheitliche Kontaktadresse nutzen. Die verteilten Service Desks arbeiten unabhängig voneinander. Sollten sie gleiche oder ähnliche Services betreuen, empfiehlt es sich, ein gemeinsames Service Knowledge Management System und Configuration Management Datenbank zu etablieren und zu nutzen. Der Vorteil von lokalen Service Desks liegt in der gegebenen physischen Nähe zum Kunden. Des Weiteren können durch den Betrieb lokaler Service Desks etwaige Konflikte aufgrund kultureller Unterschiede oder sprachlicher Barrieren vermieden werden.

Durch moderne Telekommunikations- und Netzwerktechnologien ist es möglich, mehrere lokale Service Supports zu einem so genannten **virtuellen Service Desk** zusammenzuschließen. Hierbei existiert für alle Kunden eine einheitliche Kontaktadresse, die je nach Uhrzeit der Anfrage an einen anderen lokalen Service Desk weitergeleitet wird, womit man einen Rund-um-die-Uhr-Support durch effiziente Nutzung der verschiedenen lokalen Service Desks, welche in unterschiedlichen Ländern und Zeitzonen sind, gewährleistet. Ein derartiger Service Desk wird im ITIL Rahmenwerk für so

genannte 24-hour follow the Sun Services empfohlen. Selbstverständlich profitiert der virtuelle Service Desk nicht von den Vorteilen des lokalen Service Desks bezüglich Berücksichtigung kultureller Unterschiede, örtlicher Nähe zum Kunden oder einer gemeinsamen Muttersprache.

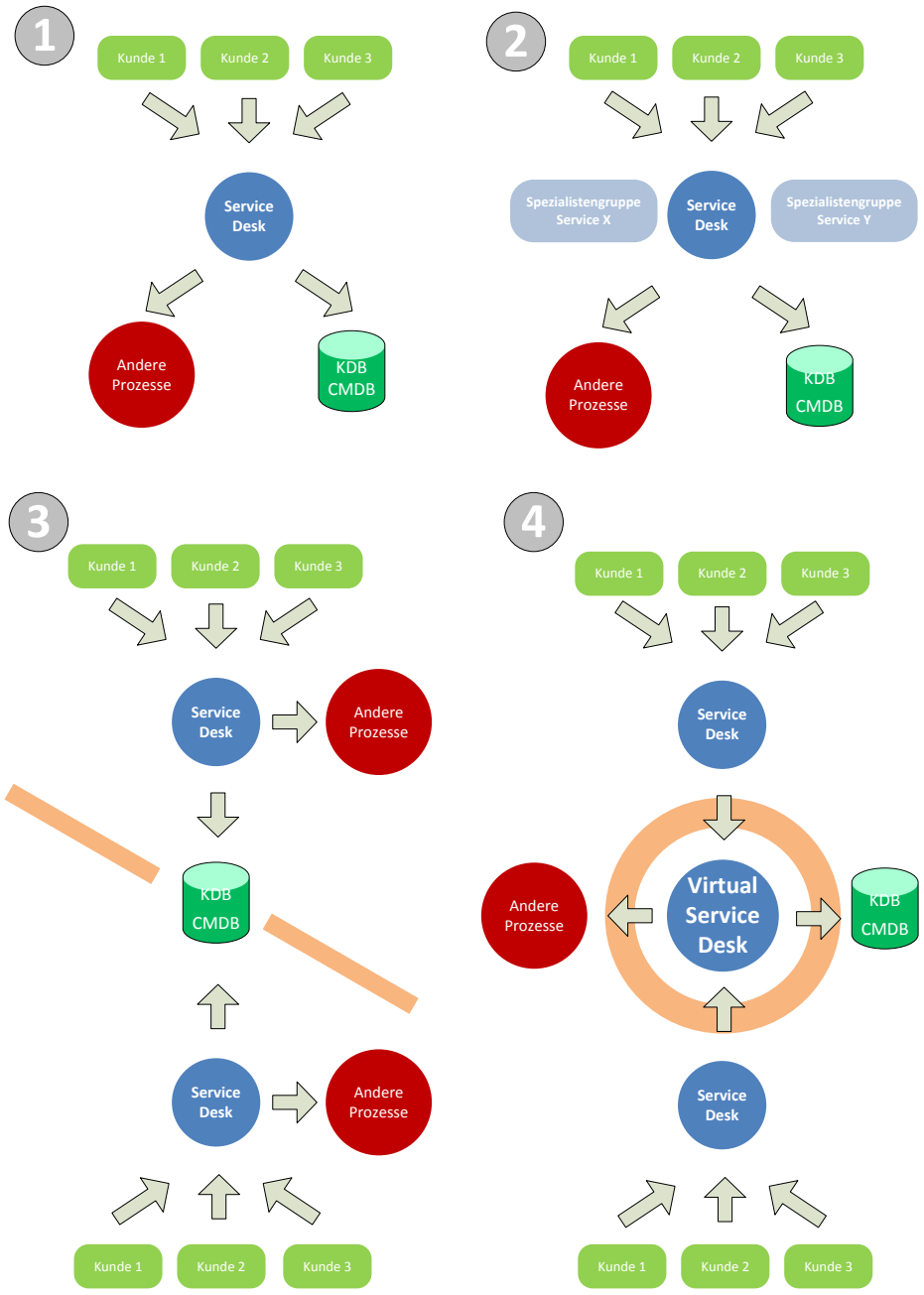



**Abbildung 33: Zentraler Service Desk (1)/ Spezialisierte Service Desk Gruppen (2) / Verteilter Service Desk (3)/ Virtueller Service Desk (4) [OGC07O]**

Der Service Desk stellt somit ein bewusst eingerichtetes Nadelöhr dar, über das jegliche Anfragen und Störungen eingebracht, erfasst und verfolgt werden. Die folgend identifizierten Sicherheitsmerkmale und Mechanismen können an dieser einen Stelle etabliert werden und schützen damit das gesamte Unternehmen. Dies erfüllt nicht nur das Kriterium der ökonomischen Effizient, sondern ist auch Grundvoraussetzung zum effektiven Erkennen und Behandeln von Human- based Social Engineering Attacken.

## 5.2 Authentizität sicherstellen

*Am 8. Februar 1587 wurde Maria Stuart, Königin von Schottland, nach einer Verurteilung wegen Verschwörung enthauptet. Ein Jahr zuvor hatte eine Gruppe von Katholiken geplant, die protestantische englische Königin Elisabeth I. zu ermorden und an ihrer Stelle Maria Stuart an die Macht zu bringen. Um die Verschwörung abzustimmen, wurden Maria Stuart geheime verschlüsselte Botschaften in ihr und aus ihrem Gefängnis geschmuggelt. Zum Unglück der Verschwörer wurde die geheime Kommunikation entdeckt. Da die Verschlüsselung gebrochen wurde, war damit nicht nur der Inhalt der Nachrichten dem Sicherheitsminister der Englischen Königin Elisabeth I. bekannt, er konnte auch den Inhalt ergänzen. Durch manipulierte Botschaften, die scheinbar von Maria Stuart stammten, verrieten die Drahtzieher ihre Identität. Maria Stuart selbst antwortete auf einen manipulierten Brief und ihre Unterschrift führte zu ihrer Verurteilung und Hinrichtung.*

Ein wesentlicher Bestandteil einer Social Engineer Attacke stellt der Diebstahl einer Identität dar. Der Angreifer nimmt die Identität eines internen Mitarbeiters an und versucht, den Service Desk Mitarbeiter durch Ausnützung der in Kapitel 4.3 angeführten Möglichkeiten zu manipulieren.

Die entscheidende Frage ist, wie kann der Service Desk Mitarbeiter die Identität des Kunden prüfen und wie sicher muss diese Überprüfung sein (im Englischen würde man dieses Sicherheitsprinzip als „Check at the Gates“ bezeichnen). Grundsätzlich gilt, keine Identitätsprüfung ist absolut sicher. Beispielsweise können Knochenmarksspenden den genetischen Fingerabdruck verfälschen [KoCh95] und die Gefahr von Verunreinigungen oder menschlicher Schlamperei kann nie ausgeschlossen werden. In Deutschland wurde der so genannte „Phantomkiller“, dessen Genmaterial

man an 39 Tatorten fand, zwei Jahre lang von mehreren Sonderkommissionen der Polizei gejagt, bevor man eine Verunreinigung der Spurensicherung feststellte (siehe dazu [Press09]).

Offensichtlich ist auch, dass nicht jedes Verfahren zur Identitätsbestimmung im Service Desk herangezogen werden kann. Faktoren wie Kosten des Verfahrens, Dauer der Ergebnisermittlung als auch Grundvoraussetzungen zur Durchführung des Verfahrens stehen der Sicherheit des Verfahrens gegenüber.

Eine wesentliche Forderung von ITIL ist die Erfassung jeglicher Störungen und Anfragen in einem entsprechenden Tool durch den Service Desk Mitarbeiter (siehe dazu [itSMF02] und [OGC07O]). Es muss sozusagen ein Ticket im Ticket Tool erstellt werden.

In dieser Arbeit wird unter der Begrifflichkeit eines Tickets ein erfasster Incident, Standard-Change, Service Request, ein erfasstes Problem, usw. gemeint. Das Tool zur Eingabe und Verwaltung von Tickets wird als Ticket Tool bezeichnet.

Die Erfassung von Tickets muss aufgrund verschiedener, in ITIL fest verankerter Mechanismen und Prinzipien geschehen:

- Eine nachträgliche Erfassung ist zumeist nicht vollständig, oftmals sogar nicht korrekt.
- Man kann nur die Bearbeitung von erfassten Störungen und Anfragen überwachen.
- Erfasste Incidents, Service Requests und deren Lösungsmethode sind für die Bearbeitung neuer ähnlicher Anfragen hilfreich.
- Die Erfassung von Incidents und Service Requests ist notwendig zur Erkennung von Häufigkeiten. Sie dienen dem Problem Management für eine detaillierte Ursachenforschung.
- Incidents und Service Requests können in Zuge ihrer Bearbeitung von verschiedenen Mitarbeitern behandelt werden. Die selbe Anfrage oder Störung soll aber auch nicht von mehreren Mitarbeitern gleichzeitig unabhängig voneinander behandelt werden. Die Erfassung jeglicher Anfragen ist also Voraussetzung für eine koordinierte Bearbeitung.
- Die Erfassung jeglicher Störungen und Anfragen ist für das Service Level Management essentiell notwendig. So sind die Anzahl der Störungen, deren Auswirkungen und die Störungsdauer entscheidende Qualitätskriterien eines Services und finden sich

typischerweise in Service Level Agreements wieder. Analog gilt dies auch für die Bearbeitung von Anfragen.

Die eingesetzte mögliche Authentifikationsmethode ist von dem gewählten Kommunikationskanal des Kunden abhängig. Eine Möglichkeit ist, Anfragen nur in Anwesenheit des Kunden selbst entgegenzunehmen oder zu bearbeiten. Typische Authentifikationsmerkmale sind in diesem Fall körperliche Merkmale des Kunden, beispielsweise Gesichtserkennung, Fingerabdruck, Unterschrifts- oder Iriserkennung. Für jegliche Anfrage allerdings immer die persönliche Anwesenheit des Kunden vorauszusetzen, ist in der Regel allerdings unmöglich. International agierende Unternehmen mit über die Welt verstreuten Kunden, die Bearbeitung von zeitkritischen Anfragen und schlichtweg der Kostenfaktor der zeitaufwändigen Verfahren bedingen alternative Authentifikationsmethoden. Nichtsdestotrotz sollte bei besonders kritischen Anfragen die persönliche Anwesenheit des Kunden und die damit verbundenen Authentifikationsmöglichkeiten verpflichtet werden.

Wenn Anfragen und Störungen in Tickets erfasst werden müssen, so ist denkbar, dass der Kunde genau dieses Tool nutzt, um die Anfrage selbst direkt einzugeben. ITIL bezeichnet dies als Möglichkeiten zur Selbsthilfe (engl. „Self-Help Capabilities“). [OGC07O] Hierzu muss sich der Kunde in einem im Intranet oder Extranet verfügbaren Portal authentifizieren.

Die klassische Methode zur Authentifikation ist die Eingabe eines Benutzernamens (Identifikation) und eines Passwortes, welches nur der echte Benutzer weiß (Authentifikation). Um den Anwender einerseits von der Flut von Kontodaten zu befreien und es andererseits zu ermöglichen, dass die verschiedenen Services aus den einzelnen Sicherheitsdomänen zusammenwirken können, ohne dass der Anwender unzählige Male aufgefordert wird, einen seiner Benutzernamen und Passwörter anzugeben, werden sogenannte Single Sign-On Lösungen eingeführt. [Roes02] beschreibt verschiedene Single Sign- On Verfahren zur Authentifikation über das Netzwerk.

Eine andere Möglichkeit stellt beispielsweise die elektronische Unterschrift mittels einer Bürgerkarte [OeBK] dar. Wenn sich ein Anwender anmelden möchte, wird zuerst die Personenbindung von der Bürgerkarte ausgelesen (Identifikation), anschließend muss eine Anmeldebestätigung mit dem Privaten Schlüssel der Bürgerkarte unterschrieben werden. Eine detaillierte Beschreibung zur Authentifikation mittels Bürgerkarte ist in [Zwat06] beschrieben. Die derzeit häufigste Ausprägung der Bürgerkarte ist eine

Smart-Card, wie sie beispielsweise Studentenkarten, Bankomatkarten oder die e-card der österreichischen Sozialversicherung darstellen. Die Bürgerkartenfunktionalität kann aber auch auf einem Personalausweis oder Kundenausweis einer Firma abgebildet werden. Grundsätzlich hat man sich hierbei nicht auf eine konkrete Technologie festgelegt, weshalb häufig der Begriff „Konzept Bürgerkarte“ verwendet wird. Das E-Government-Gesetz [Oest09a] hebt bei seiner Definition die Technologieneutralität und die Unabhängigkeit von technischen Komponenten hervor.

Einen weiteren Kommunikationskanal stellt E-Mail dar. Ein Kunde schreibt seine Anforderung oder schildert die eingetretene Störung in einem Mail und schickt sie an eine E-Mail Adresse des Service Desks. Das E-Mail Konto ist nicht einer Person zugeordnet, sondern es handelt sich um eine funktionale Mail Box, auf die alle Mitglieder des Service Desks zugreifen.

Aktuelle E-Mail-Programme bieten bereits integrierte Signaturfunktionen nach den vorgeschriebenen Standards. In den meisten Fällen wird der Standard S/MIME eingesetzt. [Ayni08]

Ein verpflichtender Rückruf stellt eine weitere Erhöhung der Sicherheit bezüglich Authentizität dar. Hierbei ist entscheidend, dass keinesfalls etwaige Kontaktdaten herangezogen werden, die im Mail angeführt werden, sondern aus einer vertrauenswürdigen Quelle stammen. Hierzu bietet sich das Tool zur Erfassung aller Anfragen und Störungen selbst an.

Ähnlich der Authentifizierung von Mails sind auch Anfragen per Telefon mit äußerster Vorsicht zu behandeln.

Die Authentizität des Anrufers kann mit einer gewissen Sicherheit durch Überprüfen der Rufnummer sichergestellt werden. Hierbei basiert die Sicherheit auf einem Faktor, dem Besitz beziehungsweise dem Zugang zu einem Handy oder Festnetztelefon.

Zusätzlich bieten sich Kontrollfragen oder die Nennung eines Losungswortes an, wodurch eine Zwei-Faktor Sicherheit gegeben ist, nämlich Besitz und Wissen.

Wichtig bei der Erfassung von telefonischen Anfragen ist eine gute Toolunterstützung. Es empfiehlt sich jedenfalls, die Telefonanlage mit dem Tickettool zu koppeln, sodass die Rufnummer des Anrufers hergenommen werden kann, um automatisch aus einer Personendatenbank den Anrufer zu identifizieren. Der Service Desk Mitarbeiter bekommt also sofort die wichtigsten Daten des Anrufers eingeblendet und kann über den ersten

Faktor, dem Besitz des Handys, den Anrufer authentifizieren. Zusätzlich könnte dem Service Desk Mitarbeiter ein Losungswort im Tool angezeigt werden, welches der Kunde nennen muss.

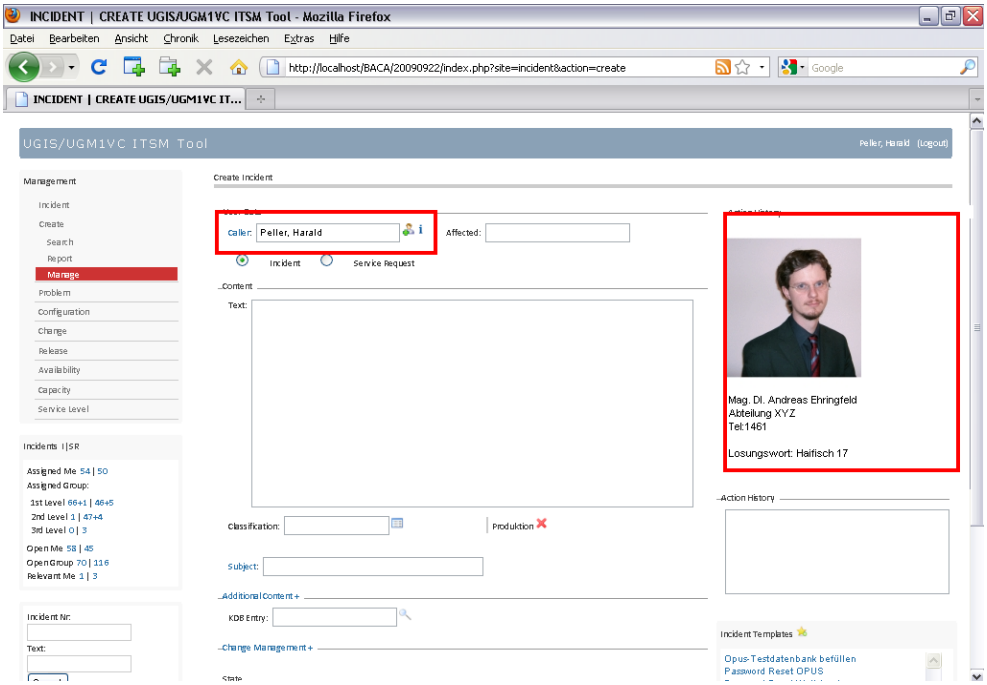



**Abbildung 34: ITIL Tool: Detailinformationen des Kunden darstellen**

Weitere Informationen des identifizierten Anrufers können ebenfalls für den Service Desk Mitarbeiter hilfreich sein, einen möglichen Human- based Social Engineering Angriff zu erkennen. Darunter fallen beispielsweise die Anzeige des Bildes zur Widererkennung, die Abteilungszugehörigkeit und Position im Unternehmen mit besonderer Hervorhebung, ob der identifizierte Anrufer ein externer oder ein interner Mitarbeiter ist. Eine besonders wertvolle Information ergibt sich aus einer möglichen Vernetzung mit dem Personalmanagementsystem des Unternehmens. So kann angezeigt werden, ob der Mitarbeiter krankgemeldet ist. All diese zusätzlichen Informationen unterstützen die Arbeit des Service Desk Mitarbeiters und erschweren es einem Social Engineer, sich als eine andere Person auszugeben.

Eine ganz besondere Form der Authentifizierung ist ein SecurID Key-Token. Hierbei handelt es sich um ein Sicherheitssystem der Firma RSA Security, welches oftmals zur Authentifizierung gegenüber VPN- Servern oder Firewalls verwendet wird.

Der SecurID Key-Token, erhältlich als Schlüsselanhänger oder im Kreditkarten-Format, zeigt eine alle 60 Sekunden wechselnde 4- bis 8-stellige Zahl an. Diese Zahl wird im Key-Token generiert und ist das Produkt eines AES Algorithmus, der sie aus einem Zeitindex und einem geheimen Schlüssel (Länge: 128 bit) des jeweiligen Key-Tokens berechnet. Der Schlüssel wird bei der Fertigung des Tokens mit einem echten Zufallszahlengenerator erzeugt und in dieses eingebettet. Er ist nur dem Authentication Manager bekannt, niemandem sonst.

Der Anrufer müsste zur Authentifizierung die 4- bis 8-stellige Zahl, den „SecurID-Code“, dem Service Desk Mitarbeiter nennen, welcher die Zahlenkombination über das Tickettool abfragt, wo es dann mit dem im Server für diesen speziellen Benutzer nach gleichen Kriterien erzeugten Code verglichen wird. Stimmen die Codes überein, ist der Anrufer authentifiziert.

Ein weiterer Authentifizierungsfaktor stellt der Wechsel auf ein anderes Kommunikationsmedium mit einen anderen Authentifizierungsmechanismus dar. Beispielweise müssten telefonisch angenommene Anfrage durch ein Mail bestätigt werden. Hierbei ist vorausgesetzt, dass sich der Benutzer authentifizieren muss, um Zugriff auf seine Mailbox zu erhalten. Damit das Verfahren praktikabel ist, müsste es weitestgehend über das Tickettool automatisiert unterstützt werden. Mit dem Erstellen des Tickets könnte ein E-Mail an die in der Datenbank hinterlegte E-Mail Adresse des Kunden geschickt werden. Erst durch Klicken auf einem im E-Mail enthaltenen Hyperlink, wird die Anfrage authentifiziert und das Ticket zur Bearbeitung freigegeben. Der Hyperlink muss so gestaltet werden, dass er ein generiertes Einmal- Passwort enthält, also eine Kennung, welche nur für diesen einen Autorisierungsvorgang gültig ist.

Allgemein gilt, dass durch die Forderung von ITIL, alle Anfragen erfassen zu müssen (siehe dazu [itSMF02]), eine Vielzahl an Authentifikationsmechanismen prinzipiell technisch möglich, aber durch die Toolunterstützung auch praktikabel sind. Eine Abwägung, welches Authentifikationsverfahren gewählt wird, ist keine grundsätzliche Entscheidung, es empfiehlt sich vielmehr, mehrere Authentifikationsmechanismen zu nutzen, abhängig von der Art der Anfrage. Grundsätzlich müssen die Service Desk Mitarbeiter entsprechend den Vorgaben von ITIL durch ein Tool unterstützt werden. Dieses Tool sollte dazu genutzt werden, zusätzliche Informationen über den identifizierten Anrufer sofort bei der Ticketerstellung darzustellen, welche

es für einen Social Engineer wesentlich erschweren, eine fremde Identität anzunehmen.

## 5.3 Gut planen und sich daran halten

Daniel H. Hill: *„…der Angriff der neun Brigaden Magruders nach Sonnenuntergang. Unglücklicherweise griffen sie nicht gemeinsam an, und wurden einzeln geschlagen.... Das war kein Krieg - das war Mord.“*

*Mit diesen Worten beschrieb Daniel H. Hill die Schlacht am Malvern Hill. Sie fand am 1. Juli 1862 statt und war die letzte der Sieben-Tage-Schlacht im amerikanischen Bürgerkrieg. General Lee wollte die letzte Möglichkeit nutzen, der feindlichen Unionsarmee eine empfindliche Niederlage zuzufügen, bevor sie im Schutz von Kanonenbooten über den James entkommen würde. Er schätzte die Föderationsarmee als demotiviert und demoralisiert ein. Sein Angriffsplan beruhte darauf, dass durch Artilleriebeschuss die feindlichen Stellungen sturmreif geschossen werden sollten, bevor ein kombinierter Angriff mehrerer militärischer Verbände den Feind auf dem Hügel im Sturm aufreiben sollte. Der Schlachtverlauf endete verheerend für General Lee. Tatsächlich war die feindliche Armee hoch motiviert und kampfbereit. Mangelnde Ortskenntnis und fehlerhafte Karten führten dazu, dass die militärischen Verbände von General Lee nicht entsprechend der Planung in Stellung gebracht werden konnten. So verzögerten unwegsame Straßen und versumpftes Gelände die Truppenbewegungen. Eine Division marschierte zunächst in die falsche Richtung. Die Artillerie konnte nicht in ausreichender Zahl in Stellung gebracht werden und wurde von der feindlichen Artillerie vernichtet. Fehlmeldungen führten dazu, dass General Lee eine völlig falsche Einschätzung vom Kampfverlauf hatte. Lees Operationsplan war schwierig zu koordinieren, seine Untergebenen waren seinen Führungsstil immer noch nicht gewohnt. Der Stab war nicht eingespielt und setzte die komplizierten Anweisungen Lees ungenügend um. Das alles führte zu einer Reihe von unkoordinierten Angriffen einzelner Truppen, welche vom Feind erfolgreich abgewehrt werden konnten und der Angriffsschwung der Konföderierten wurde gebrochen.*

Ein Social Engineer kann unkoordiniertes Vorgehen in Betrieben sehr gut für seinen Angriff nutzen. Individuelles Vorgehen, keine Abstimmung unter

den Mitarbeitern, undurchschaubare Verfahren und Vorgaben, aber auch Überarbeitung der Mitarbeiter, das Ignorieren und Liegenlassen von Kundenanfragen und ein insgesamt chaotisches Verhalten der Mitarbeiter sind nicht nur aus betrieblicher Sicht eine Katastrophe, sie erleichtern oder ermöglichen sogar erst Social Engineering Attacken.

Entsprechend [Ehri07] muss ein Betrieb unter anderem folgende Anforderungen erfüllen, um nicht aus organisatorischer Sicht in einem „täglichen Überlebenskampf“ und aufgrund der damit verbundenen Ohnmacht des Managements in der „Hoffnung der Selbstorganisation“ zu enden:

- Ein IT Betrieb ist ein kontinuierliches Teamwork.
- Ein IT Betrieb muss strukturiert ablaufen.
- Ein IT Betrieb muss serviceorientiert sein.
- Ein IT Betrieb muss transparent sein.

Ein Unternehmen ist bemüht, Visionen, Zielsetzungen und Politik umzusetzen. Damit die Vielzahl an Zielen, Vorgaben, Rahmenbedingungen und Einflussfaktoren strukturiert behandelt werden, verwendet das IT Service Management eine prozessorientierte Herangehensweise. Basis jeder Überlegung ist die Bestimmung der Ausgangslage. Anschließend wird die Zielsetzung definiert und das Delta zwischen Ist- und Sollzustand analysiert. Das Resultat dieser Überlegungen ist ein Maßnahmenplan. Essentiell ist die Identifikation von Möglichkeiten, den Grad der Zielvorgabenerfüllung zu ermitteln. Bei einem zyklischen Durchlauf dieser Fragestellungen erreicht man ein Prozessverbesserungsmodell.

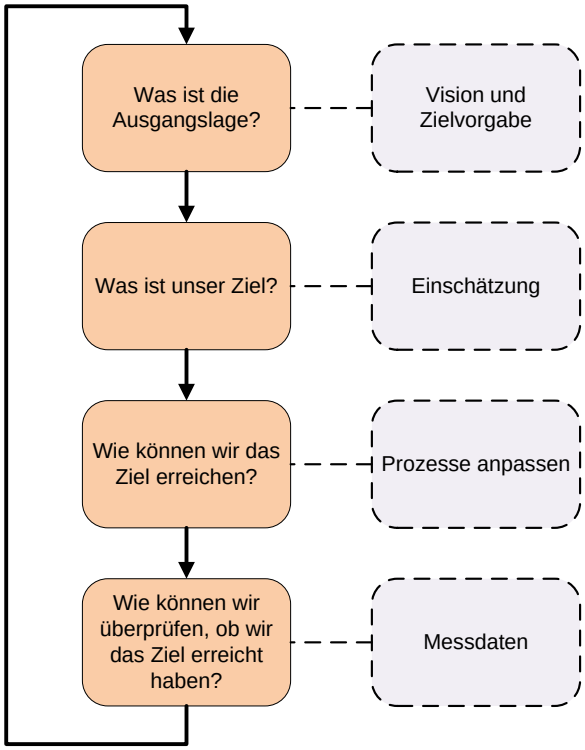



**Abbildung 35: ITSM - Prozessverbesserungsmodell [itSMF02]**

Isoliert man in der Betrachtungsweise des Prozessverbesserungsmodells den Schritt des Erreichens der Zielvorgabe, so leiten sich daraus eine Reihe von Aktivitäten ab. Diese Aktivitäten müssen in eine bestimmte Reihenfolge gebracht werden, um von einen gegebenen Ist- Zustand einen Soll- Zustand zu erreichen. Entsprechend [itSMF02] ist ein Prozess eine logisch zusammenhängende Reihe von Aktivitäten zur Erreichung eines vorab definierten Ziels. Um das Ergebnis der Aktivitäten zu verdeutlichen, wird es mit Qualitätseigenschaften und Normen verknüpft.

Das Resultat des Prozesses sind nicht nur das erreichte Ergebnis, sondern auch Messpunkte zur Bestimmung der Qualität des Produktes oder des Services.

Normen sind dazu da, die Umsetzung der Unternehmenspolitik festzulegen. Es entspricht der Abbildung visionärer Vorgaben in strategische Überlegungen, die sich in der Taktik widerspiegeln. Entspricht ein Prozess den Normen, so bedeutet dies, dass die Taktik der Strategie zur Erfüllung der Vision entspricht, was als effektiv bezeichnet wird. Sind die Aktivitäten auch kostengünstig, so spricht man von effizienten Prozessen.

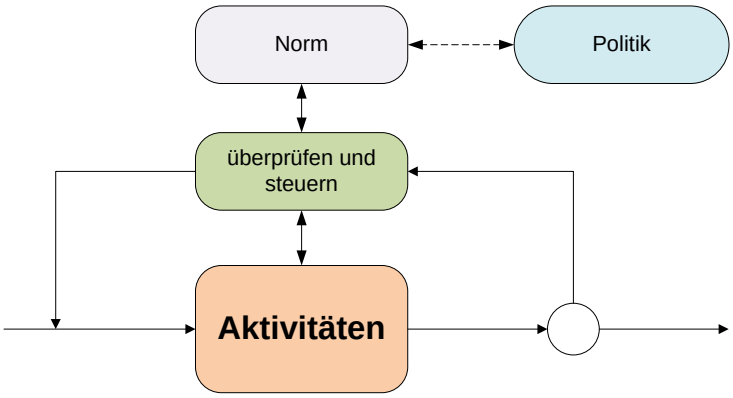



**Abbildung 36: Prozess [itSMF02]**

Grundsätzlich unterscheidet ITIL entsprechend dem generischen Prozessmodell nach [itSMF02] zwischen Prozessdurchführung, Prozessprüfung und Prozessbedingungen. Jeder Prozess wird isoliert zur Bestimmung der Qualität betrachtet, indem die Erfüllung der Zielvorgaben geprüft wird. Der Process Owner ist für das Ergebnis seines Prozesses und somit die Einhaltung der geforderten Qualitätsanforderung verantwortlich. Dazu kontrolliert er das Ergebnis seines Prozesses anhand von Leistungsindikatoren im Verhältnis zu den vereinbarten Normen. Zusätzlich organisiert er die Verknüpfung mit anderen Prozessen, um die reibungslose Zusammenarbeit zwischen den Prozessen zu gewährleisten.

Der Process Manager ist für die Planung und Durchführung eines Prozesses verantwortlich. Zusätzlich hat er die Aufgabe, dem Process Owner laufend zu berichten. Um das Ziel eines effektiven und effizienten Prozesses zu erreichen, benötigt der Process Manager eine Möglichkeit zur Überwachung und Bewertung seines Prozesses. Eine bekannte Methode für Organisationen, ist der Einsatz einer Balanced Score Card (BSC), welche auch für den Einsatz der ITIL Prozesse empfohlen wird.

Der Process Executor ist für die Durchführung bestimmter Prozessaktivitäten verantwortlich. Dieser muss dem Process Manager regelmäßig berichten. [Kain08]

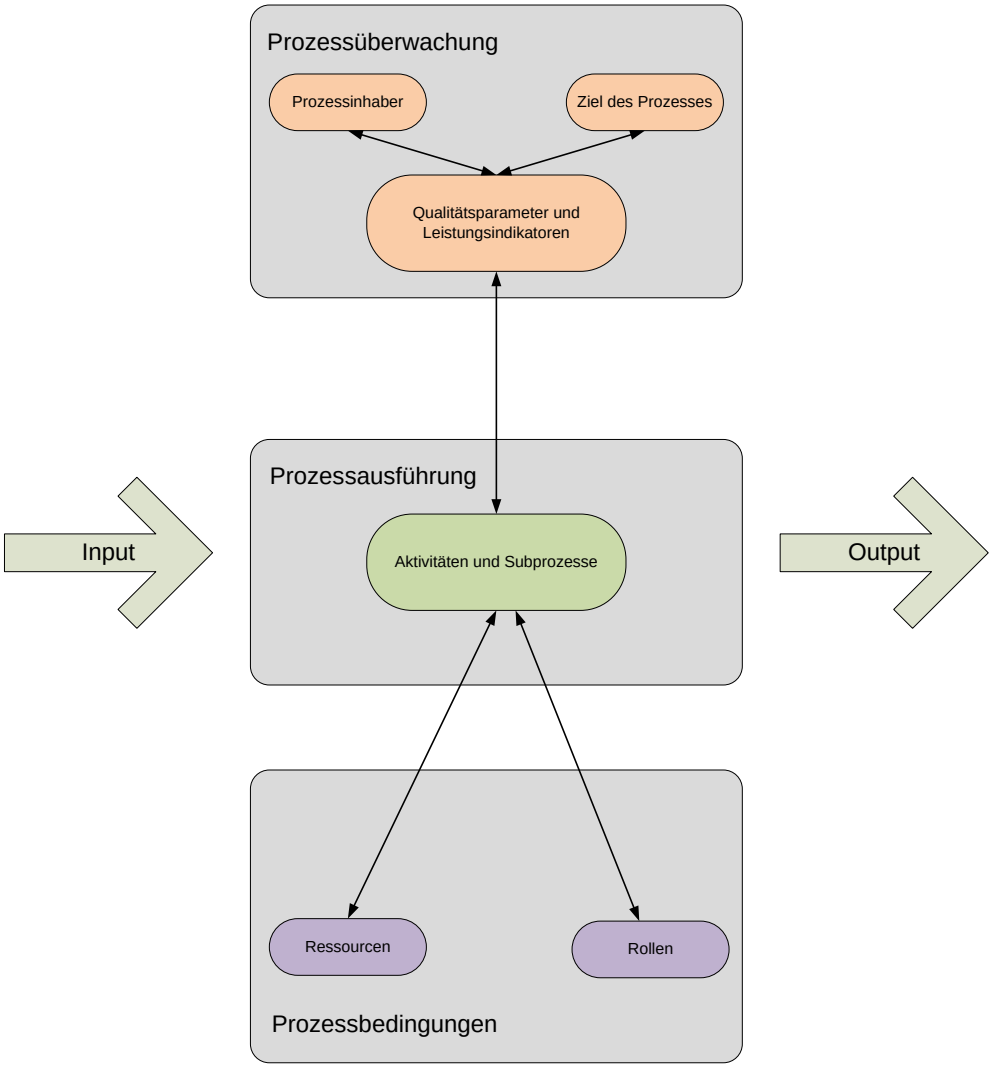



**Abbildung 37: Generisches ITIL Prozessmodell [itSMF02]**

Betrachtet man nun beispielsweise den Incident Management Prozess, so durchläuft dieser die folgenden wohldefinierten Prozessschritte, wie in Abbildung 37 dargestellt:

- Incident annehmen und erfassen
- Klassifizieren, kategorisieren, priorisieren und unterstützen
- Prüfung, ob Service Request oder Incident vorliegt
- Prüfung auf bekanntes Störungsmuster
- Analyse und Diagnose
- Beheben und wiederherstellen
- Prüfung, ob Incident erfolgreich gelöst wurde
- Incident abschließen

Zuerst wird der Incident vom 1st Level Mitarbeiter aufgenommen und erfasst.

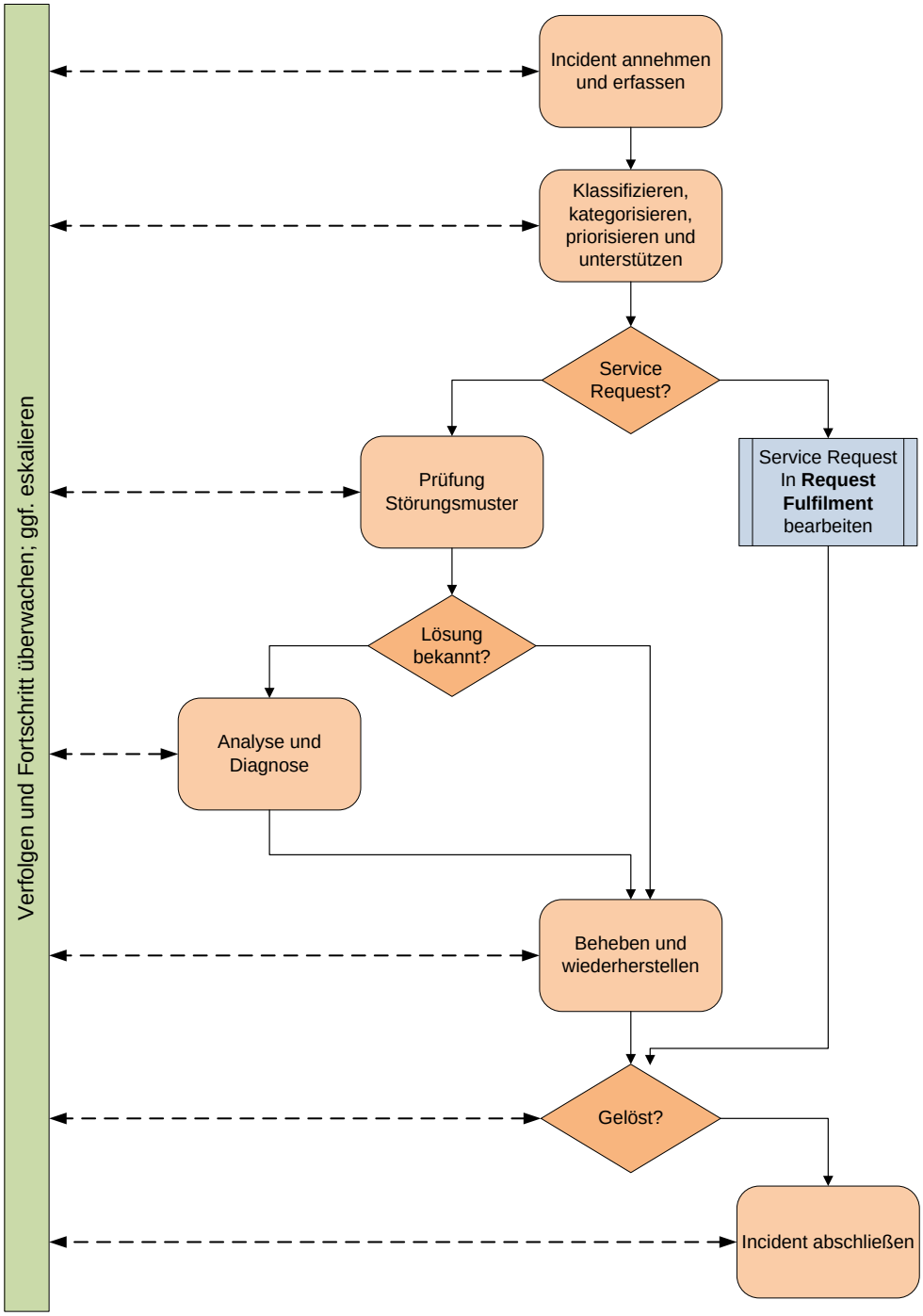



**Abbildung 38: ITIL Incident Management Prozess**

Hierbei wird der Anrufer erfasst und der vorliegende Sachverhalt beschrieben. Der Anrufer muss nicht zwangsläufig die betroffene Person sein. Gegebenenfalls wird daher diese ebenfalls im Ticket Tool eingetragen. Nachdem der Incident erfasst wurde, muss er klassifiziert, kategorisiert und priorisiert werden. Die Priorisierung bestimmt einerseits, mit welchen Ressourcen am Incident gearbeitet werden muss, als auch die Reihenfolge der Bearbeitung mehrerer Incidents. Die Priorisierung selbst erfolgt nach einer mehrstufigen Skala, die zumeist unternehmensweit definiert wird. Sie wird vom 1st Level Mitarbeiter entsprechend der folgenden Bewertung durchgeführt:

- Wer ist betroffen?
- Wie viele sind betroffen?
- Welcher Schaden entsteht bis wann bei Nichtnearbeitung?
- Welche Bearbeitungszeit ist in den Service Levels definiert?
- Wie komplex ist die Bearbeitung? Was ist die erwartete Bearbeitungszeit?
- Sind die Schritte zur Bearbeitung bekannt?
- Benötigt man zusätzliche Ressourcen zur Bearbeitung?

Da die Priorisierung vom 1st Level Mitarbeiter durchgeführt wird und entsprechend ITIL kein Heruntersetzen einer Priorisierung im Laufe der Bearbeitung des Incidents erfolgen sollte (siehe dazu [BoMa06] [Buhl05]), ist dieser Schritt ausgesprochen bedeutend. Er setzt eine hohe Qualifizierung des 1st Level Mitarbeiters voraus, welche in den folgenden Analysen detailliert behandelt wird.

Die Kategorisierung entspricht einer Zuordnung des Incidents zu hinterlegten Schlagwörtern. Diese dienen der schnellen Einordnung des Incidents, wenn ein Mitarbeiter das Ticket öffnet und sich auf einen Blick einen groben Überblick verschaffen möchte. Des Weiteren sind damit sowohl effiziente Suchen als auch Reports und Auswertungen möglich. Die Notwendigkeit von Reports und Auswertungen als Bestandteil eines Sicherheitskonzepts gegen Human- based Social Engineering Attacken wird in den folgenden Kapiteln analysiert.

Mit der Erfassung des Incidents beginnt bereits die erste Unterstützung durch den 1st Level Mitarbeiter. Durch gezielte Fragen wird das Anliegen identifiziert und abgegrenzt. Anschließend an die Priorisierung, Klassifizierung und Kategorisierung entscheidet der 1st Level Mitarbeiter, ob es sich um einen Incident oder um einen Service Request handelt.

Im Falle eines Incidents wird im nächsten Schritt geprüft, ob es sich um ein bekanntes Störungsmuster handelt und ob es für diese Störung eine dokumentierte Lösung gibt. Wird diese in dem Service Knowledge Management System gefunden, so wird die Störung anhand dieser Lösungsschritte behandelt. Anschließend wird in [itSMF02] empfohlen, das Incident Ticket mit den dokumentierten Lösungsschritten im Ticket Tool zu verknüpfen. Somit stehen hilfreiche Informationen zur Behebung der Störung zur Verfügung. Dies hat den Vorteil, dass nachvollziehbar ist, wie diese Störung behoben wurde, dient aber auch als Hilfestellung für die Behebung weiterer ähnlicher Störungen.

Tritt eine Störung zum ersten Mal auf, so existiert zumeist kein Eintrag im Service Knowledge Management System. In diesen Fall muss der Mitarbeiter den Incident näher analysieren und eine Diagnose stellen. Hierbei kann es vorkommen, dass der 1st Level Mitarbeiter nicht das notwendige Spezialwissen hat, weshalb er das Störungsticket einen 2nd Level Mitarbeiter zuweist. Insbesondere gilt, dass sich alle Mitarbeiter eines Levels über ihre Rechte und Pflichten bewusst sind. [Buhl05] Hierzu gehören Vereinbarungen über die Aufgaben der jeweiligen Parteien, welche oftmals in so genannten Operation Level Agreements (OLA) verankert sind. Der Mechanismus der Zuweisung zwischen einem 1st Level Mitarbeiter und einem 2nd Level Mitarbeiter wird als funktionale Eskalation bezeichnet. [OGC05S] Hintergrund ist, dass in einem Unternehmen Mitarbeiter unterschiedlicher Funktionen verschiedenen Bereichen zugeordnet werden. Während 1st Level Mitarbeiter jene Personen im Service Desk sind, besteht das 2nd Level Support Team zumeist aus Administratoren, Netzwerkspezialisten, Anwendungsbetreuern usw. In den meisten Fällen sind 3rd Level Mitarbeiter externe Know-how-Träger. Diese Einteilung ist allerdings nicht fest vorgeschrieben, weshalb eine granularere Einteilung in mehr als drei Levels sinnhaft sein kann und den Prinzipien von ITIL keinesfalls widerspricht.

Vom 1st, 2nd und 3rd Level Mitarbeiter wird versucht, die Störung zu beheben. Führen die Maßnahmen des Mitarbeiters dazu, dass der Incident erfolgreich behoben wird, so kann das Ticket abgeschlossen werden. Dieser Schritt inkludiert auch die vollständige Dokumentation des Behebungsweges im Service Knowledge Management System (SKMS). Der Incident gilt somit als gelöst, wodurch das Ticket mit all seinen Lösungsdetails im SKMS erscheint, um zukünftige, gleichartige Störungen bereits im Schritt „Prüfung Störungsmuster“ zu beheben, wodurch zeit- und ressourcenaufwändige Analysen vermieden werden. Aus sicherheitstechnischer Sicht hat dies zusätzlich den Vorteil, dass

transparente und einheitliche Aktivitäten bei der Behebung von Störungen durchlaufen werden.

Wie in [Kain08] und [OGC07S] aufgezeigt, bildet die Configuration Management Database (CMDB) ein wichtiges Instrument zur Gewinnung und Speicherung von alten oder neuen Informationen über die IT-Infrastruktur. Die Configuration Management Database bietet die Grundlage bei der Analyse der Störungen. SKMS und CMDB sind somit entscheidende Elemente bei der Bearbeitung von Incidents.

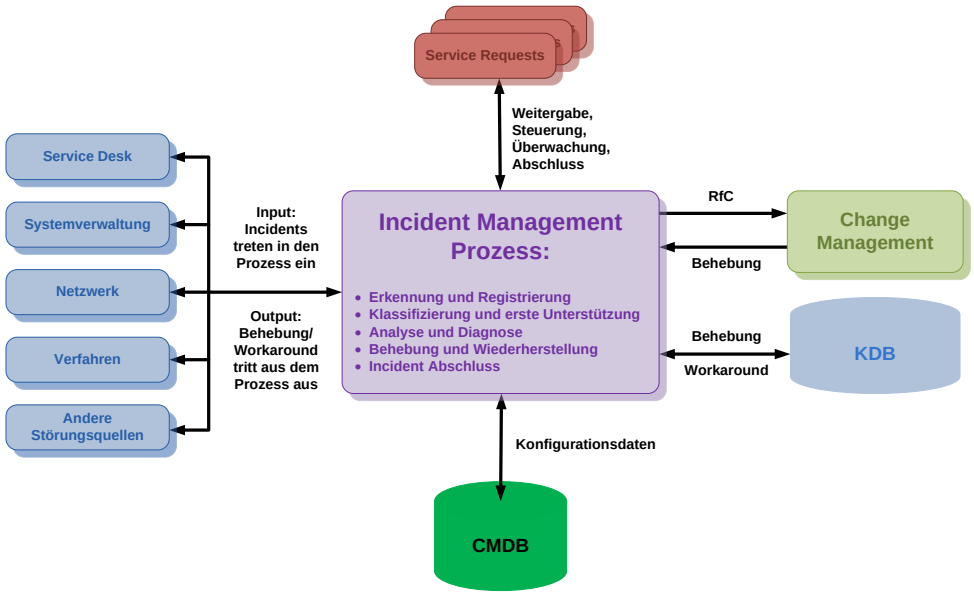



**Abbildung 39: Incident Management Prozessabhängigkeiten [itSMF02]**

Für eine geplante, strukturierte und vorgegebene Vorgehensweise, wie sie aus sicherheitstechnischer Sicht gegen Social Engineering notwendig ist, ist neben den definierten Prozessschritten und den bestimmten Akteuren auch die Spezifikation etwaiger Schnittstellen essentiell. Diese sind durch die Übergabe an andere Prozesse entsprechend ITIL gegeben.

Störungstickets werden durch das Incident Management erfasst und versucht zu beheben. Sind Systemänderungen für die Behebung von Störungen notwendig, so werden diese durch das Change Management beurteilt und gegebenenfalls zur Umsetzung im Release Management freigegeben. Das Release Management ist dafür verantwortlich, Änderungen strukturiert, effizient und effektiv umzusetzen. Hierbei wird besonders auf eine möglichst störungsfreie Umsetzung mit möglichst geringem Risiko für

den Betrieb geachtet. Das Configuration Management bietet die Basis sowohl für die Störungsanalyse in Zuge des Incident Managements, als auch für die Bewertung der Auswirkungen der Änderungswünsche in Zuge des Change Managements. Sie ist integraler Bestandteil des Release Management Prozesses, sodass die Configuration Management Database stets aktuell gehalten wird.

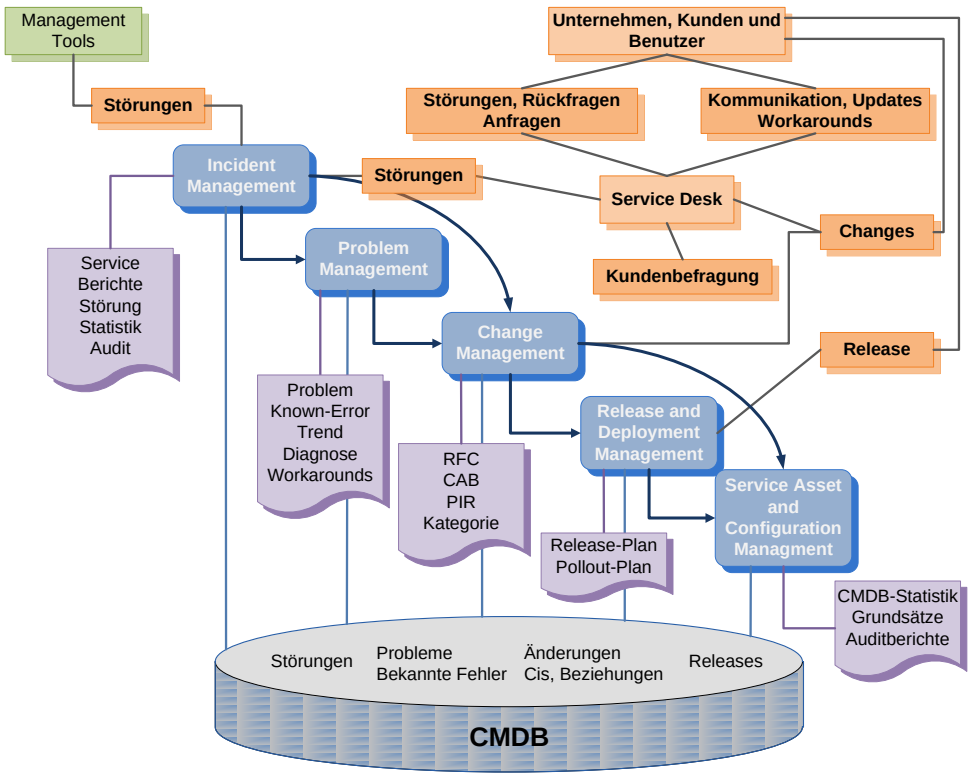



**Abbildung 40: Incident Management Schnittstellen [itSMF02]**

Eine weitere Schnittstelle ergibt sich zum und vom Problem Management. Tritt die gleiche Art einer Störung immer wieder auf, so sind die Lösungsansätze des Incident Managements nicht nachhaltig genug. Eine detaillierte Analyse für eine effektive Lösung wird aus dem Incident Management aus angestoßen und durch das Problem Management behandelt. Tritt eine besonders schwerwiegender Incident auf, beispielsweise wenn dieser eine Vertragsverletzung zwischen Dienstleister und Kunde mit sich zieht oder wenn es sich um einen schweren sicherheitskritischer Vorfall handelt, so sollte dieser jedenfalls durch das Problem Management analysiert werden. Das Problem Management ist aber nicht nur reaktiv, sondern auch proaktiv. So werden nicht nur eingetretene

Probleme behandelt, sondern auch mögliche. Das Problem Management untersucht die eigentliche Ursache und sucht nach Möglichkeiten, das Problem dauerhaft zu lösen. Ein Ergebnis des Problem Managements kann eine bessere Lösungsstrategie sein, welche im Service Knowledge Management System dokumentiert wird und die Basis weiterer Störungsbehebungen im Incident Management darstellt. Verbesserungsvorschläge werden durch das Problem Management in Form von Request for Changes an das Change Management zur weiteren Bewertung und Autorisierung geschickt.

Eine besondere Schnittstelle ist jene zwischen Incident Management und Information Security Management. Sicherheitsrelevante Incidents werden als Security Incidents markiert. Sie sind somit für das Information Security Management leicht identifizierbar und werden von ihnen besonders geprüft.

Anhand des Incident Management Prozesses wurde gezeigt, dass die in ITIL definierte Herangehensweise zur Behandlung von Incidents wohldefiniert ist. Dies gilt in analoger Weise für Service Requests, die in Zuge des Request Fulfilments oder des Access Managements behandelt werden. Ein derartiges Vorgehensmodell erschwert es Social Engineering Angreifern ganz entscheidend. Dadurch ist es nämlich einem Social Engineer theoretisch nicht mehr möglich, den Mitarbeiter beispielsweise durch Knappheit, Autorität oder Sympathie in seinen Handlungen zu beeinflussen, da die Aktivitäten, Akteure und Schnittstellen genau definiert sind. Diese Sicherheit ist in der Praxis aber erst dann gegeben, wenn sichergestellt ist, dass sich die Mitarbeiter an die Prozesse halten. Daraus ergibt sich, dass weitere Maßnahmen und der Einsatz von Technologie notwendig sind. Diese werden in weiterer Folge vorgestellt. Erst in dieser Kombination gewinnt das in ITIL verankerte Sicherheitsprinzip gegen Social Engineering an realer Effektivität.

## 5.4 Risiko durch Aufteilung verringern

Johann Wolfgang von Goethe: *„Entzwei und gebiete! Tüchtig Wort. – Verein und leite! Besserer Hort.“*

*Outsourcing, als eine besondere Art der Aufteilung, kann als Instrument zur Risikominimierung angewandt werden. Yury Zaytsev, Head Global IT bei Swiss Re, sieht Outsourcing als Möglichkeit Unsicherheit abzubauen und Risiken zu minimieren. Swiss Re beschränkt das Outsourcing ausschließlich auf nicht strategische Bereiche, wie zum Beispiel das Testen von Software.*

[Chur06] *Eine Risikominimierung ergibt sich aus der Reduktion des gebundenen Kapitals in einem Bereich mit volatiler Nachfrage.* [LiTs09]

*Die Anforderung, Software zu testen, tritt unregelmäßig auf, zugleich sind die Tätigkeiten des Testens sehr arbeitsintensiv. Da eine Vielzahl von externen Dienstanbietern sowohl das Know-how besitzen, als auch über genügend personelle Kapazitäten verfügen, hat sich Swiss Re für das Outsourcing des Softwaretestens entschieden. Dem gegenüber wären die hohen Kosten einer internen Testabteilung gestanden, welche groß genug sein müsste, um die Anforderungen bei Spitzenlast zu erfüllen, gleichzeitig wären somit aber viele Ressourcen während der testfreien Zeit unproduktiv gebunden und müssten finanziert werden.*

*Risikominimierung findet man in der Finanzbranche durch die so genannte Risikostreuung beziehungsweise Diversifikation. Hierbei wird das Vermögen auf unterschiedliche Anlagenformen und Finanzprodukte aufgeteilt, um das Risiko der Kapitalanlage in ihrer Gesamtheit zu vermindern (siehe dazu beispielsweise* [Schu97] *und* [Feik08]*).*

*Ein anderes Beispiel von Risikominimierung durch Aufteilung findet man in der Rechtsprechung. Um sicherzustellen, dass die Rechtsprechung nicht von einer einzelnen, fehlbaren Person und deren Einschätzung und Bewertung der Sachlage abhängig ist, wurden Geschworenengerichte eingeführt. Hierbei sind Geschworene ganz oder zum Teil bei der Entscheidung beteiligt. Grundgedanke hierbei ist, dass die Bewertung der Sachlage durch mehrere Personen durchgeführt werden sollte, um der Fehlbarkeit einer Einzelperson durch eine objektivere Bewertung einer Gruppe entgegenzuwirken. Der Richter bewertet in einem Geschworenenverfahren nur mehr die Rechtslage.*

*Eine Studie von* [KaZe66] *belegt, dass die Richter, die in Strafprozessen Geschworenengerichten vorsaßen, in 25 Prozent der Fälle mit dem Urteil der Geschworenen nicht übereinstimmten. Jüngere Beobachtungen (siehe dazu* [ArMe02] *und* [DeCl01]*) kritisieren das Geschworenenprinzip, wobei sie vor allem die Fähigkeiten der Geschworenen in Frage stellen, bei komplexerem Beweismaterial den Überblick zu behalten und zu einem emotionsfreien Urteil zu finden.*

Gerade dieser Umstand spiegelt die Schwierigkeit bei der Aufteilung von Aufgaben auf mehrere Personen wider. Die Berücksichtigung von Kompetenzen ist ein entscheidender Faktor bei der Verteilung von Risiko,

sodass nicht neue Angriffsvektoren für einen Social Engineer entstehen. Das Sicherheitsprinzip der Risikominimierung durch Verteilung ist nur dann effektiv gegeben, wenn die Gesamtsicherheit von der erfolgreichen Korrumpierung aller Einzelkomponenten abhängig ist. Des Weiteren muss der Sicherheitsgrad aller Einzelkomponenten mindestens dem Sicherheitsgrad des ursprünglichen Gesamtsystems vor der Aufteilung entsprechen (in Anlehnung an den Verteilungseffekt entsprechend [BSI08]).

Sucht man das Sicherheitsprinzip der Risikominimierung durch Aufteilung (engl. „Compartmentalize“), so findet man es in den Empfehlungen von ITIL in mehreren Stellen wieder. Ein ganz entscheidender Schutzmechanismus vor Social Engineering Attacken stellt die Zuständigkeitsmatrix dar, wie sie in ITIL verankert ist (siehe dazu [OGC07S] [IBM08]).

Wie im vorigen Abschnitt dargestellt, ist das Incident Management in mehreren Support Levels gestaffelt. Der Service Desk fungiert als Singe Point of Contact und ist der 1st Level Support. Anfragen, die im Service Desk nicht behoben werden können, werden an entsprechende Spezialisten weitergeleitet. Hierbei hilft eine Zuständigkeitsmatrix als Unterstützung, an wen welche Incidents weitergeleitet werden sollten. So wird ein Operating System (OS) spezifischer Incident (zum Beispiel: Windows Printer Spooler Error) an das Operating System Team des Unternehmens, als 2nd Level Support, weitergeleitet. Wenn auch hier nicht die notwendige Qualifikation vorhanden ist, so wird das Incident Ticket an Externe als 3rd Level, wie zum Beispiel Microsoft Support, weitergeleitet.

| 1st Level | 2nd Level | 3rd Level |
|---|---|---|
| **Service Desk** | 2nd Level Support Applikationen | Softwarelieferanten |
| | | Programmierer |
| | | Consultants |
| | 2nd Level Support Operation Systems | Externe OS Spezialisten |
| | | Microsoft |
| | | RedHat |
| | | SuSe |
| | | SUN |
| | | … |
| | | Consultants |
| | 2nd Level Support Netzwerk und Telekommunikation | Externe Spezialisten |
| | | Hersteller und Lieferanten |
| | | Consultants |

| | | |
|---|---|---|
| | 2nd Level Support Infrastruktur | DELL |
| | | IBM |
| | | HP |
| | | APC |
| | | … |

**Tabelle 5: Incident Management Support Levels**

Gerade der Mechanismus der fachlichen Eskalation von einem Support Level zum nächsten stellt eine wichtige Sicherungsmaßnahme gegen Attacken eines Social Engineers dar. Ein Angreifer kann somit schwieriger mit der Methode der Knappheit eine Überforderung beim bearbeitenden Mitarbeiter erzeugen.

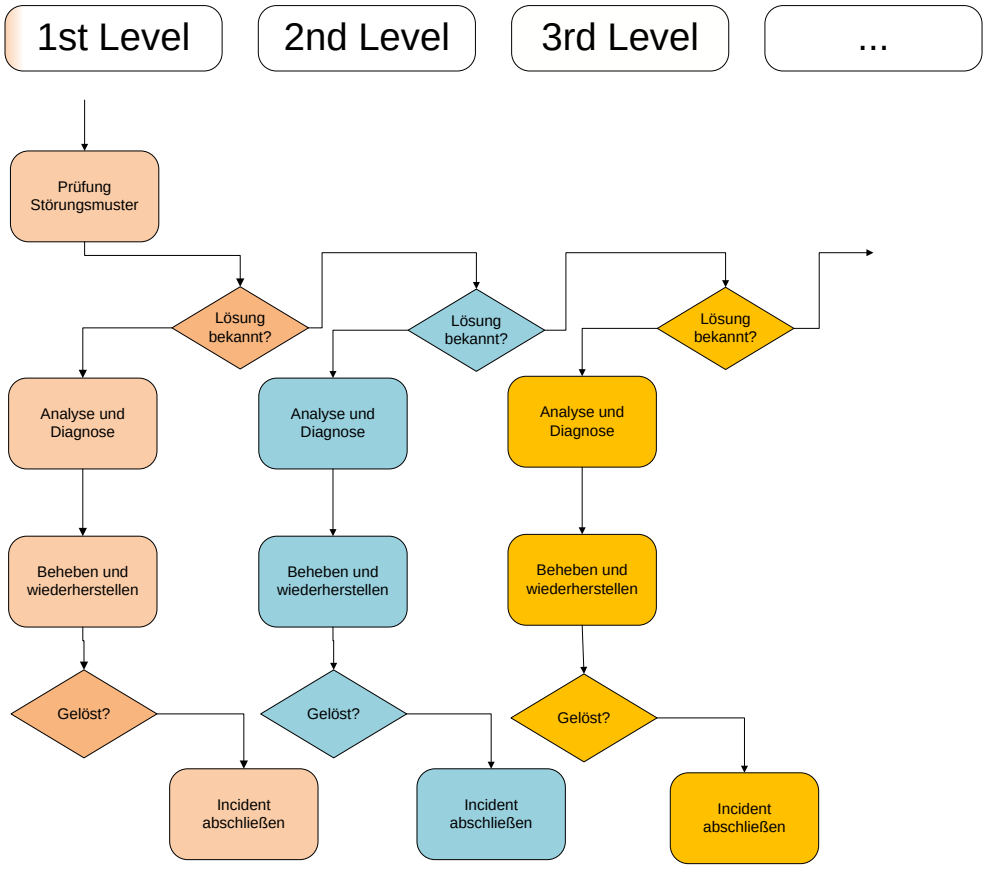



**Abbildung 41: Incident Management Support Levels**

Das Principle of Least Privilege (PoLP) besagt, dass Komponenten, Anwender oder Systeme nur mit jenen Privilegien arbeiten dürfen, die sie tatsächlich zur Erfüllung ihrer Aufgaben benötigen. Hierbei spricht man

auch von einer Minimalausstattung (siehe dazu [Whit03] [BaGe05] und für weiterführende Literatur [Deit90] [SaSc09]).

So braucht beispielsweise ein 1st Level Mitarbeiter keine administrativen Rechte auf Netzwerkkomponenten wie Switches und Router. Für einen 1st Level Mitarbeiter genügen einfache Analysewerkzeuge wie „ping“ und „traceroute“, um die Funktionsweise zu prüfen. Da der 1st Level Mitarbeiter keinerlei administrative Rechte auf die Netzwerkkomponenten hat, kann er im erkannten Fehlerfall nur das Netzwerk- und Telekommunikationsteam als 2nd Level Support verständigen. Dieses verfügt über die erweiterten Privilegien, aber auch die Qualifikation für eine detaillierte und fundierte Analyse. Der 2nd Level Support kann wesentlich besser die Auswirkung und Folgen der Handlungen abschätzen. Daraus ergibt sich logischerweise zum einen eine geringere Chance für den Social Engineer, den Mitarbeiter zu einer unrechtmäßigen Handlung zu bewegen, zum anderen aber auch ein erhöhtes Risiko, dass die Absichten des Social Engineers durch den höher qualifizierten Mitarbeiter erkannt werden.

Kann ein Einbrecher die Alarmanlage eines gesicherten Grundstückes nicht überlisten, so könnte er bewusst mehrere Alarme auslösen. Nachdem die Sicherheitsfirma zum wiederholten Male zum Grundstück geeilt ist, aber nichts feststellen konnte, gehen die Mitarbeiter der Sicherheitsfirma von einer Fehlfunktion der Alarmanlage aus. Die Alarmanlage wird vorübergehend abgedreht, um weitere störende Fehlalarme zu vermeiden. Nun kann der Einbrecher ungestört das Grundstück betreten.

Das Beispiel soll verdeutlichen, dass auch in Krisensituationen Sicherheitsmechanismen aufrecht erhalten bleiben müssen. ITIL spiegelt dies im IT-Betrieb durch die besondere Behandlung von Major Incidents wider. Hierbei handelt es sich um derart kritische Störungen, dass die Behandlung nach dem vorgestellten Prozess nicht möglich ist. Im Sinne des Sicherheitsprinzips, etwas gut zu planen und sich daran zu halten, existiert auch zur Behandlung von Major Incidents ein definierter Prozess, welcher sich durch kürzere Durchlaufzeit und höherer Bearbeitungspriorität auszeichnet. Ein Major Incident Team wird vom Major Incident dynamisch abhängig unter der Leitung des Incident Managers zusammengestellt. Hierbei erfüllt das Team das Sicherheitsprinzip der Risikominimierung durch Aufteilung.

Es wurde gezeigt, dass eine Aufteilung der Betriebsmannschaft nach Expertise in Kombination mit dem Mechanismus der fachlichen Eskalation und dem Principle of Least Privilege das Sicherheitsniveau entscheidend

erhöhen kann, um Human- based Social Engineering Attacken entgegenzuwirken. Sowohl klar definierte Zuständigkeiten als auch Schnittstellen stellen eine Basis für Sicherheit dar. Besonders zu beachten ist, dass beim Auftreten besonderer Ereignisse, wie beispielsweise Major Incidents, die Prinzipien der Sicherheit gegen Social Engineering Attacken weiter befolgt werden.

Das Restrisiko kann weiter minimiert werden, indem nicht nur eine Aufteilung vorgenommen wird, sondern indem man auch unterschiedliche Verfahren, Technologien oder Sicherheitsmechanismen kombiniert. Dadurch ist sichergestellt, dass ein Angreifer nicht mit den gleichen Methoden beziehungsweise mit der Ausnutzung gleicher Schwachstellen alle verteilten Komponenten einzeln nacheinander bezwingen kann.

## 5.5 Gestaffelte Abwehr

*Die Burg Hochosterwitz wurde erstmals im Jahr 860 urkundlich erwähnt. Sie gilt als Wahrzeichen des Bundeslandes Kärnten in Österreich. Um einen besonderen Schutz vor Angreifern und Belagerern zu bieten, wurden gestaffelte Abwehrmaßnahmen eingesetzt. Die Burg steht auf einem Dolomitfelsen und ist über einen mittelsteilen Aufstieg erreichbar. Der Aufstieg ist durch vierzehn Tore gesichert, die ein Angreifer nacheinander überwinden muss. Die Tore sind an strategischen Punkten positioniert, sodass sie gut verteidigt werden konnten. Zusätzlich sorgen Zugbrücken sowie künstliche und natürliche Engpässe für weitere Hindernisse. Die Gesamtsicherheit war durch die Kombination all dieser Sicherheitsmaßnahmen gegeben. Wurde von einem Angreifer ein Tor überwunden, so zog sich der Verteidiger in den nächsten von insgesamt vierzehn Verteidigungsringen zurück.*

Auf analoge Weise wird der Schutz von einem Verbund gestaltet. Der Angreifer ist dadurch gezwungen, jede einzelne Verteidigungslinie zu durchbrechen, was nicht nur sehr viel Zeit benötigt, sondern auch ein gefächertes Expertenwissen des Angreifers voraussetzt. Jede Verteidigungslinie sollte allerdings unterschiedliche Systeme einsetzen. Zwei gleiche hintereinander gestaffelte Firewall Systeme mit identischer Konfiguration sind sinnlos, da der Angreifer mit derselben Methode beide durchdringen kann. Sicherheit gewährleistet man durch einen gestaffelten Einsatz verschiedener Technologien, die miteinander sinnvoll kombiniert

werden. Firewall Systeme, Intrusion Detection Systeme (IDS), der Einsatz kryptographische Konzepte, Guarddogs uvm. sind die geeigneten Werkzeuge, um einen Verbund zu sichern. [NoZe03]

Im Bereich des Service Managements stellt die Zuständigkeitsmatrix die Basis für klare Aufgabenteilungen dar, welche mit entsprechenden Rechten und Privilegien hinterlegt sind. Diese Aufgabenteilung sollte für ein besonderes Sicherheitsprinzip genutzt werden, nämlich jenes der Funktionstrennung (engl. „Segregation of Duties“, „Segregation of Roles“), wodurch eine gestaffelte Abwehr (engl. „Defense in Depth“) erreicht wird. Hierbei wird in dieser Arbeit zwischen einer funktionalen Aufgliederung auf mehrere Personen zur Erfüllung einer Aufgabe und dem in späterer Folge vorgestellten Aufbau eines internen Kontrollsystems (IKT) unterschieden.

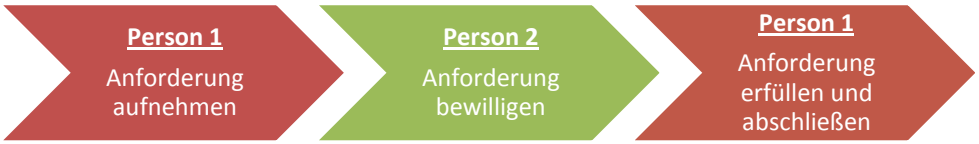



**Abbildung 42: Funktionsteilung in mehrere Aufgabenbereiche – Teilung in Durchführung und Kontrolle**

Die Anforderung wird von einer anderen Person geprüft, bevor sie weiter behandelt werden darf. Die Funktionstrennung ist durch die Teilung in Durchführung und Kontrolle gegeben.

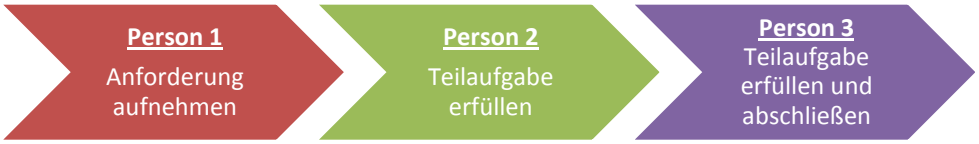



**Abbildung 43: Funktionsteilung in mehrere Aufgabenbereiche – Verteilung auf mehrere Personen**

Die einzelnen Arbeitsschritte sind auf mehrere Personen verteilt. Die Funktionstrennung ist durch die Aufteilung in mehrere Aufgabenbereiche gegeben.

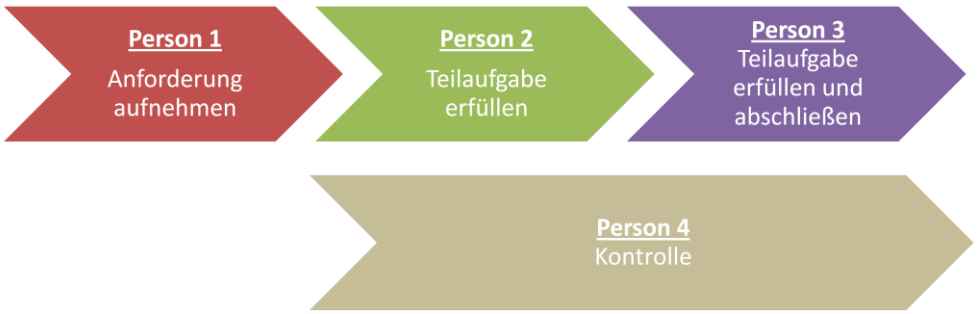



**Abbildung 44: Funktionstrennung mit IKS**

Die Anforderung wird von einem internen Kontrollprozess begleitet. Die Funktionstrennung ist durch die zur Durchführung parallel laufenden Kontrolle gegeben.

Eine Funktionsteilung in mehrere Aufgabenbereiche ist immer zielgerichtet auf die Aufgabenerfüllung. Jeder Schritt ist Teil der Anforderungsbehandlung bis zum Abschluss. Dies inkludiert auch Freigaben oder Prüfungen, die erfolgreich absolviert werden müssen, bis weitere Tätigkeiten gesetzt werden. Ein IKS ist ein paralleler Prozess, der nicht zwingend in zeitlicher Relation zu den Prozessschritten der Aufgabenerfüllung abläuft.

Durch eine funktionale Aufgliederung zur Erfüllung einer Aufgabe wird erreicht, dass eine klare Funktionstrennung zwischen unvereinbaren Rollen zur Minimierung des Risikos gegeben ist. Beispielsweise darf jener Mitarbeiter, der Kundenaufträge entgegennimmt, nicht Zahlungen initiieren, da er ansonsten Geldmittel unterschlagen könnte.

Berücksichtigt man den Aspekt der Funktionstrennung im Sinne einer gestaffelten Abwehr gegen Angriffe, so lässt sich der folgend dargestellte Prozess gestalten. In den vorigen Abschnitten wurde der Fokus auf die Behebung von Störungen gelegt. Nun wird ein Beispiel eines Service Requests herangezogen, der in Zuge des Request Fulfillments behandelt wird.

Betrachtet man die Freigabe einer Berechtigung auf ein Netzwerklaufwerk, so ergeben sich die folgenden grundsätzlichen Schritte. Die Anforderung zur Berechtigungsfreigabe muss zunächst aufgenommen werden. Basierend auf den erfassten Daten wird die Berechtigung erteilt und das Ticket abgeschlossen.

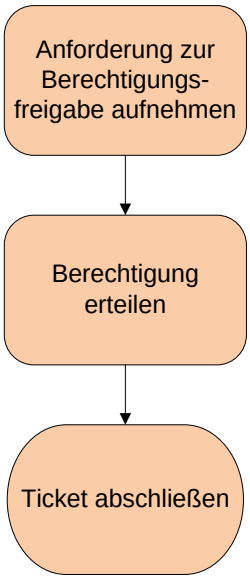



**Abbildung 45: Beispielprozess: Berechtigungsfreigabe – einfaches Szenario**

Der dargestellte Prozess ist zwar funktional, bietet aber vielerlei Angriffsmöglichkeiten für einen Social Engineer. Zum einen kommt es zu keiner Prüfung der Anforderung, zum anderen muss der Social Engineer nur eine Person erfolgreich zu einer unrechtmäßigen Handlung bewegen, um eine bestimmte Freigabe zu erhalten.

Um den Prozess aus Sicherheitssicht zu verbessern, müssen weitere Prozessschritte, wie in der folgenden Darstellung, eingeführt werden. Hierbei wird eine Anforderungsprüfung nach dem Erfassen durchgeführt. Die Anforderung wird anschließend an den Teamleiter weitergeleitet, welcher diese bewilligen muss. Erst danach wird die Berechtigung auf das Netzlaufwerk für den Anforderer eingerichtet. Entsprechend Vorgaben von ITIL wird die Konfigurationsänderung in der CMDB eingetragen, sodass die Informationen innerhalb der CMDB stets aktuell sind. Erst danach werden alle involvierten Personen darüber informiert, dass die Anfrage bearbeitet und abgeschlossen wurde.

Der Prozess ist linear gestaltet. Jegliche Störung des Prozessdurchlaufs, zum Beispiel wenn der Teamleiter keine Bewilligung erteilt, die Vorabprüfung eine Schwierigkeit aufzeigt oder wenn die Freigabe technisch nicht durchgeführt werden kann, führt zu einem Abbruch des Prozesses. In diesem Fall müssen entsprechende Eskalationsschritte durchgeführt werden, die nicht in Zuge dieses Beispiels angeführt sind.

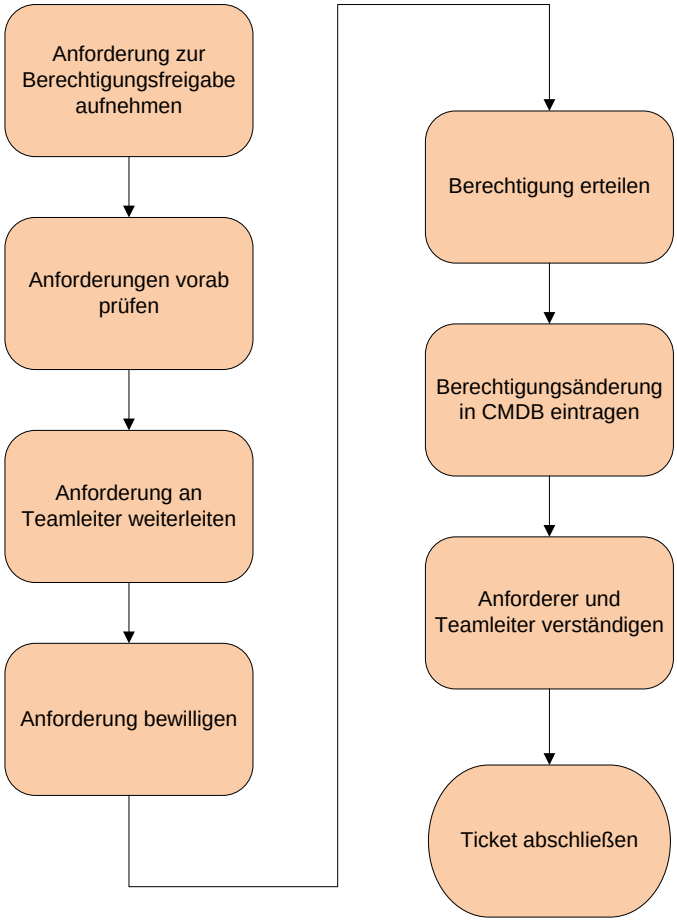



**Abbildung 46: Beispielprozess: Berechtigungsfreigabe – erweitertes Szenario**

Im Sinne einer gestaffelten Abwehr durch Funktionstrennung werden nun die einzelnen Prozessschritte handelnden Personen zugeordnet. Dies wird in der folgenden Abbildung verdeutlicht. Der 1st Level Mitarbeiter nimmt die Anforderung entgegen, indem er ein entsprechendes Ticket anlegt, und führt eine erste Vorabprüfung durch. Der Teamleiter des Anforderers erhält automatisiert über das Ticket Tool die Anforderung zur Bewilligung. Die Berechtigungsänderung wird anschließend durch das Tool durchgeführt und automatisiert in der CMDB aktualisiert. Die Verständigung der im Prozess

involvierten Personen wird ebenfalls automatisiert über einen Mailversandt realisiert. Zuletzt muss der 1st Level Mitarbeiter das Ticket manuell schließen.

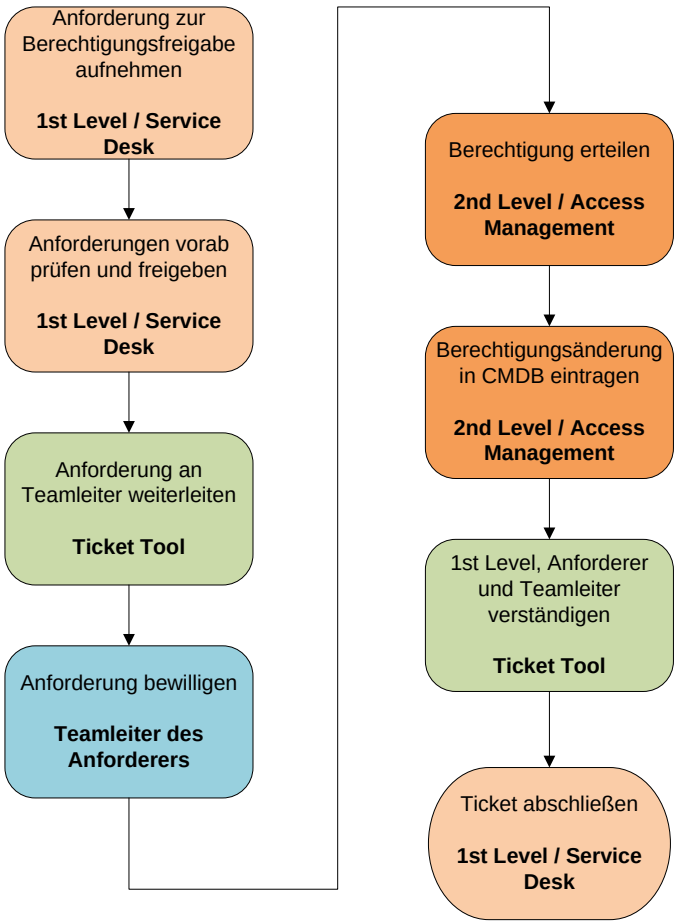



**Abbildung 47: Beispielprozess: Berechtigungsfreigabe – Szenario mit Funktionstrennung**

Innerhalb dieser Prozessschritte gibt es ganz wesentliche Sicherheitsmaßnahmen, welche es einem Social Engineer unmöglich machen, mit denselben Angriffsvarianten wie bei der Ausganglage dieses Beispiels erfolgreich zu sein.

In erster Linie führt die Aufteilung der Aufgaben auf mehrere Personen mitsamt einem expliziten Bewilligungsschritt dazu, dass ein Social Engineer mehrere handelnde Personen manipulieren müsste. Hierbei kommt erschwerend hinzu, dass die Personen unterschiedliche Sichtweisen und Zugänge zur Anforderung haben. Der 1st Level Mitarbeiter beurteilt die formale Korrektheit der Anforderung, während der Teamleiter des

Anforderers die fachliche Korrektheit der Anforderung bestätigen muss. In gewisser Weise hat er eine Kontrollfunktion in der Prozessdurchführung.

Die Vorabprüfung des 1st Level Mitarbeiters gilt in erster Linie formalen Aspekten, wie zum Beispiel jenen, ob alle notwendigen Informationen im Ticket erfasst wurden. Hierbei sollte dem Ticket Tools eine ganz entscheidende Rolle zukommen. Jegliche Prüfung, die durch das Ticket Tool durchgeführt werden kann, steht in der Regel außerhalb der Manipulationsmöglichkeiten eines Social Engineers. Die Prüfung durch das Ticket Tool sollte Folgendes umfassen, insbesondere wenn es im Zuge der in ITIL vorgeschlagenen Selbsthilfe (siehe [OGC07O]) durch den Kunden bedient wird, er selbst also die Anforderung anstelle eines 1st Level Mitarbeiters in das Ticket Tool eingibt.

- Sind alle Informationen enthalten? Im Ticket Tool sollen alle relevanten Informationen erfasst werden, wobei aber die primäre Informationsquelle das Tool und nicht der Anforderer sein sollte. Das Ticket Tool soll fehlende Informationen automatisch ergänzen oder bereitstellen, sodass der 1st Level Mitarbeiter nicht beim Anforderer nachfragen muss. Dies inkludiert beispielsweise die automatische Ermittlung der Kontaktdaten des Teamleiters des Anforderers über das elektronische Personenverzeichnis des Unternehmens. Abgesehen davon, dass damit menschliche Eingabefehler vermieden werden, nimmt dies auch einem Social Engineer weitere entscheidende Angriffsmöglichkeiten. Zusätzlich hat ein derartiges System den Vorteil, dass ergänzende Informationsquellen verbunden werden können, wie zum Beispiel, ob ein Teamleiter anwesend ist, in Urlaub oder krank gemeldet ist, wer seine Vertretung ist usw.
- Ist die Anforderung plausibel? Einfache oder komplexe Regeln können die Plausibilität der Anforderung automatisch prüfen und den 1st Level Mitarbeiter gegebenenfalls warnen. Genauere Details, wie ein derartiges Verfahren zur Plausibilitätsprüfung aussehen könnte, werden in den folgenden Abschnitten näher erläutert.
- Ist die eingetragene Information für den späteren Verarbeitungsschritt gefährlich? Beachtet werden muss, dass die Eingaben „bösartige“ Daten beinhalten können, die eine spätere automatisierte Verarbeitung korrumpieren könnten. Beispielsweise sei hier auf die Gefährdungsmöglichkeit von SQL Injections verwiesen:

Wird die Eingabe einer Mitarbeiternummer in der Variable $MNR gespeichert, worauf basierend später alle weiteren Daten aus der Mitarbeiterdatenbank gelesen werden, so wird $MNR in der folgenden Datenbankabfrage durch den Wert ersetzt.

*Select * from Mitarbeiter where MitarbeiterNummer='$MNR'*

Im Normalfall entsteht bei der Eingabe von *1234* als Mitarbeiternummer:

*Select * from Mitarbeiter where MitarbeiterNummer='1234'*

Ein Angreifer könnte allerdings *1' or MitarbeiterNummer > 0* eingeben, woraus

*Select * from Mitarbeiter where MitarbeiterNummer='1'or MitarbeiterNummer > 0*

entsteht und damit alle Mitarbeiterdaten ausliest.

Würde man bei diesem Beispiel als Eingabe nur eine Zahl erlauben, so wäre dieser Angriff nicht möglich.

Grundsätzlich gilt daher, dass allen Benutzereingaben prinzipiell misstraut werden muss (engl. „Do Not Trust User Input") und diese daher genauestens geprüft werden müssen. Für detailliertere und weiterführende Informationen siehe [Farn05] [BSI06] [Anle02] und [Lerd06].

Ein entscheidendes Sicherheitskriterium gegen Angriffe ist, dass die Informationsverarbeitung und -weitergabe innerhalb eines abgeschirmten Kanals stattfindet. Das heißt, jegliche Information zur Behandlung der Anfrage wird innerhalb des Ticket Tools verwaltet und über geeignete Kanäle den Mitarbeitern zur Verfügung gestellt. Das Ticket Tool ist somit die zentrale Informationsquelle. Ein Social Engineer kann daher nicht direkt, das heißt ohne über einen Anwender des Ticket Tools, mit nicht-technischen Mitteln Informationen einschleusen, löschen oder verändern. Das Ticket Tool sollte mit aktuellen technischen Sicherheitsmechanismen versehen sein.

Der Teamleiter des Anforderers muss die Anforderung freigeben. Der Vorgang der Freigabe sollte authentifiziert (siehe dazu beispielsweise [Steph07] als geeignetes Authentifikationssystem) innerhalb des Ticket Tools abgebildet sein. Durch diesen Prozessschritt wird die Anforderung fachlich geprüft. Dies ist etwas, was in der Regel nicht durch einen 1st Level Mitarbeiter durchgeführt werden kann. Im Sinne der gestaffelten Abwehr müsste der Social Engineer sowohl den 1st Level Mitarbeiter als auch den Teamleiter des angeblichen Anforderers zu einer unrechtmäßigen Handlung überreden.

In Abbildung 48 wird durch das in ITIL beschriebene Access Management die Zugriffsfreigabe erteilt. Die Durchführung der Zugriffsfreigabe auf das Netzlaufwerk kann aber auch automatisch durch das Ticket Tool (beziehungsweise durch ein davon initiiertes Programm) abgewickelt werden. Daraus ergeben sich eine schnelle Bearbeitungszeit, eine korrekte Durchführung ohne etwaige menschliche Fehler und eine einheitliche Vorgehensweise bei jedem Prozessdurchlauf.

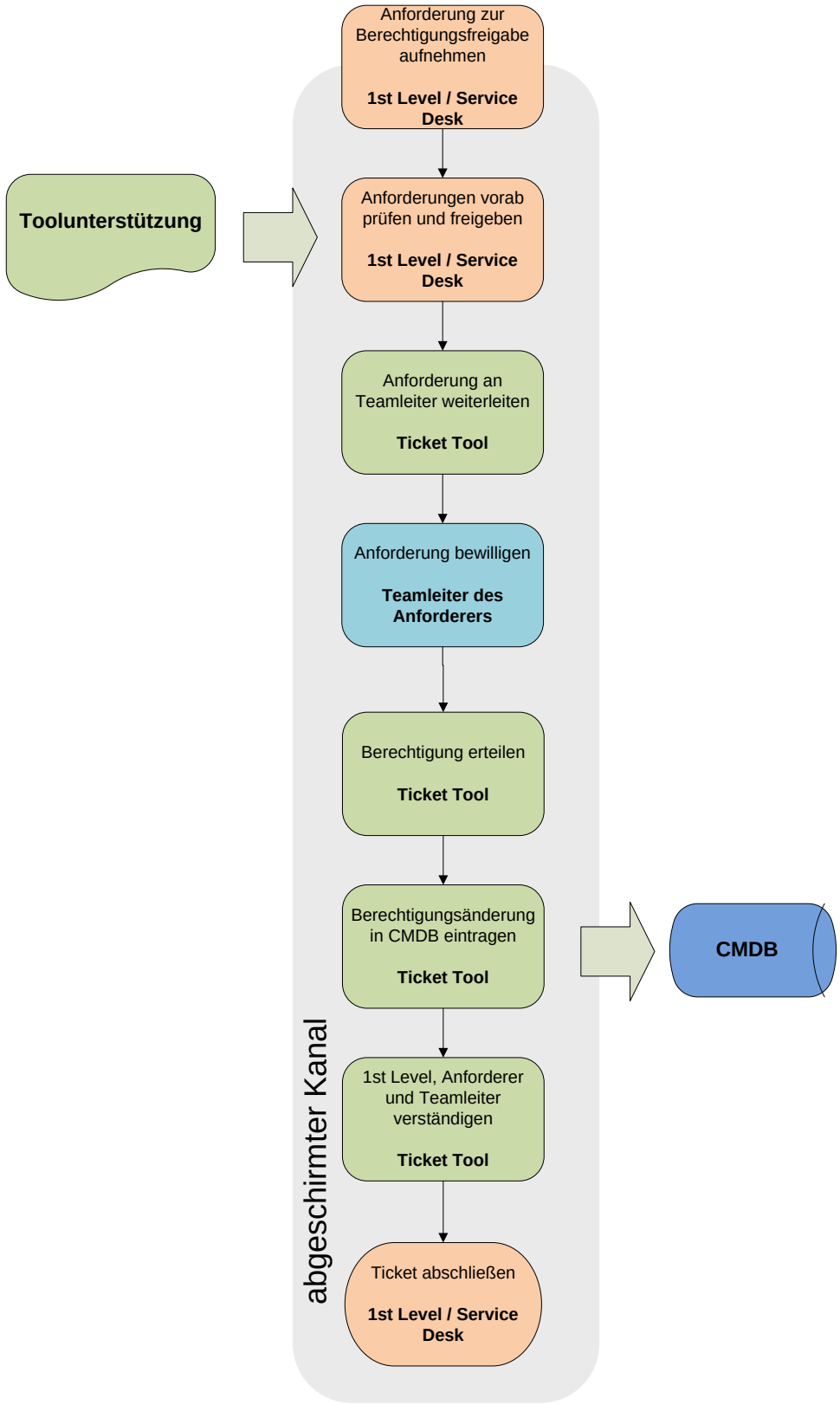



**Abbildung 48: Beispielprozess: Berechtigungsfreigabe – Sicherheitsmaßnahmen**

Des Weiteren wird durch die Teilautomatisierung von Prozessschritten die Notwendigkeit zur Verwendung des Ticket Tools und der darin hinterlegten ITIL konformen Prozesse für die Aufgabenerfüllung zwingend notwendig. So kann in diesem Beispiel ein 1st Level Mitarbeiter keine Netzwerklaufwerksfreigabe direkt durchführen. Aufgrund des Principle of Least Privilege verfügt er nicht über die dafür notwendigen administrativen Berechtigungen. Er muss somit das Ticket Tool verwenden. Damit kann die Einschränkung, dass der Sicherheitsgewinn durch die vorigen vorgestellten Maßnahmen und Grundprinzipen nur gegeben ist, wenn sich die Mitarbeiter an die Prozesse halten, in einen relativierten Kontext gesehen werden. Der folgende Abschnitt befasst sich unter anderem mit weiteren relativierenden Maßnahmen.

Das Prinzip der gestaffelten Abwehr findet man in ITIL aber nicht nur auf Prozessebene, sondern auch in der Trennung von Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement. Aus Sicherheitssicht gegen Social Engineering Attacken ist die Trennung zwischen den ausführenden Organen im Service Operations Bereich (Service Operators) und dem Information Security Management (näher beschrieben in Kapitel 5.8) im Bereich Service Design entscheidend. Das Information Security Management hat eine strategische Aufgabe, definiert Standards und Vorgaben und kontrolliert die Einhaltung. Die Zusammenlegung jener Rolle, welche Prozesse bestimmt und überwacht, mit der Rolle, welche Prozesse ausführt, würde ansonsten eine sicherheitstechnische Konfliktsituation ergeben.

## 5.6 Einfachheit

*Zur Authentifikation muss ein Benutzer einer Anwendung ein Passwort eingeben. Damit das Passwort sicher vor zufälligem Erraten ist, muss es aus mindestens acht Zeichen bestehen, sowohl Groß- als auch Kleinbuchstaben beinhalten und aus mindestens einer Zahl bestehen. Das Passwort muss regelmäßig geändert werden. Hierzu läuft die Gültigkeit monatlich ab und ein neues muss vom Benutzer gewählt werden. Dieses wird auf Ähnlichkeit mit vergangenen verglichen und nur wirklich neue Passwörter werden akzeptiert.*

*Das System gilt als sicher. Leider ist es für Mitarbeiter zu kompliziert, sich diese immer neuen Passwörter zu merken. Post-its mit dem aktuellen Passwort werden auf den Bildschirm des Arbeitsplatzes geklebt.*

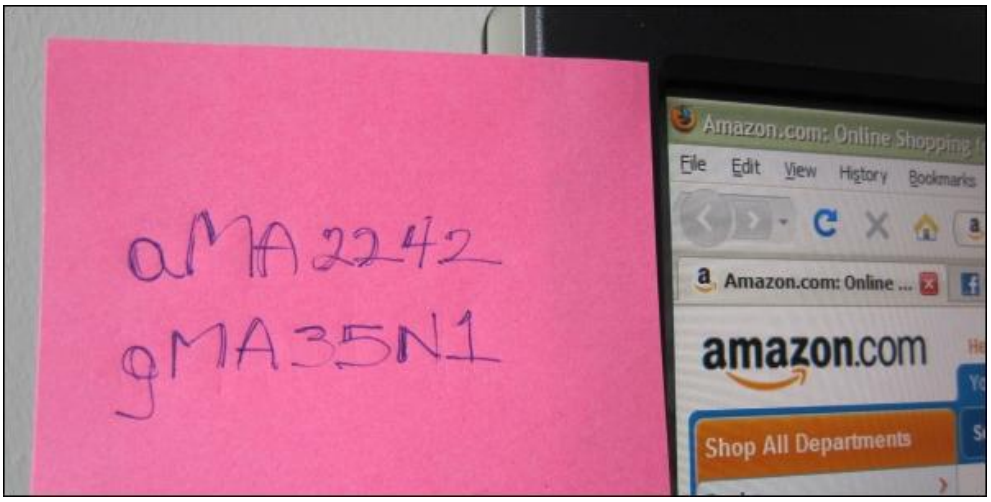



**Abbildung 49: Post-it mit Passwort für eine Webanwendung**

Dieses Beispiel soll demonstrieren, dass ein System zwar sicher sein kann, die Sicherheitsmaßnahmen allerdings durch die Mitarbeiter des Unternehmens ausgehebelt werden können.

Grundsätzlich gilt, dass je einfacher etwas gestaltet ist, umso robuster und sicherer ist es mit hoher Wahrscheinlichkeit. Dieser Sachverhalt wurde bereits mehrfach wissenschaftlich analysiert und verifiziert. So wurde zum Beispiel in der Softwareindustrie durch Moore [McCo04] ermittelt, dass 1000 Codezeilen typischer Anwendungen zwischen 15 und 50 Fehler beinhalten. Microsoft Anwendungen haben durchschnittlich zwischen 10 und 20 Fehlern nach der Entwicklung, einen halben pro 1000 Codezeilen nach allen Testzyklen vor dem finalen Release. Daraus ergibt sich, dass Anwendungen mit weniger Codezeilen statistisch eine geringere Anzahl von Fehlern beinhalten.

Das Sicherheitsprinzip der Einfachheit (engl. „Simplicity“) beinhaltet aber auch die Schnittstelle zum Menschen, also in dem Zusammenhang die einfache Bedienbarkeit. Passwörter können theoretisch sicher sein, wenn der Anwender sie sich allerdings nicht merken kann und sie auf Post-its schreibt und auf den Computerbildschirm klebt, sind sie in der Praxis ein enormes Sicherheitsloch.

Daraus ergibt sich, dass die Prozesse als auch die verwendeten Werkzeuge wie das Ticket Tool so gestaltet werden müssen, dass sie für die Mitarbeiter einfach und leicht anwendbar sind. Des Weiteren soll sich durch die Anwendung der Prozesse oder der Werkzeuge ein effektiver Mehrwert

ergeben. Dies fördert den Willen der Mitarbeiter, Verfahren und Werkzeuge zu verwenden und damit nicht indirekt die Sicherheitsmaßnahmen zu unterwandern.

Jakob Nielsen definiert in [Niel93] Usability als ein Qualitätsattribut, welches festlegt, wie einfach User Interfaces zu benutzen sind. Usability bezieht sich aber auch auf die Methoden, die während des Designprozesses eingesetzt werden, um eine gute Usability zu erreichen. Nielsen beschreibt in [GrBe09] fünf Qualitätskomponenten guter Usability: Erlernbarkeit, Effizienz, Einprägsamkeit, möglichst geringe Fehlerrate durch den Benutzer in seinen Handlungen und die Zufriedenheit des Benutzers.

In der Norm EN ISO 9241 [ISO06] wird die Ergonomie der Mensch-System-Interaktion behandelt. Hierbei werden die Forderungen nach der Effektivität zur Lösung einer Aufgabe, der Effizienz der Systemhandhabung sowie der Zufriedenheit der Nutzer einer Software als Bedingungen für die Gebrauchstauglichkeit definiert. Benutzerschnittstellen sollen den Prinzipien der Aufgabenangemessenheit, der Selbstbeschreibungsfähigkeit, der Lernförderlichkeit, der Steuerbarkeit, der Erwartungskonformität, der Individualisierbarkeit und der Fehlertoleranz folgen.

Die entscheidende Notwendigkeit einer sehr guten Usability ist insbesondere beim Design des Ticket Tools als zentrales Werkzeug alle ITIL Prozesse zu berücksichtigen. Des Weiteren soll die Verwendung des Ticket Tools einen entscheidenden Mehrwert für die Mitarbeiter bringen. Folgend wird der Sachverhalt beispielhaft erläutert.

Das Ticket Tool sollte Templates für die Erfassung von Tickets zur Verfügung stellen. Hierbei können bestimmte Eingaben einer Formularmaske unter einen Namen als Template abgespeichert werden. Dieses Template sollte man wahlweise weiteren Benutzern freigeben können. Wird das Template über eine möglichst effiziente Auswahlmöglichkeit später gewählt, wird das Formular entsprechend wieder befüllt.

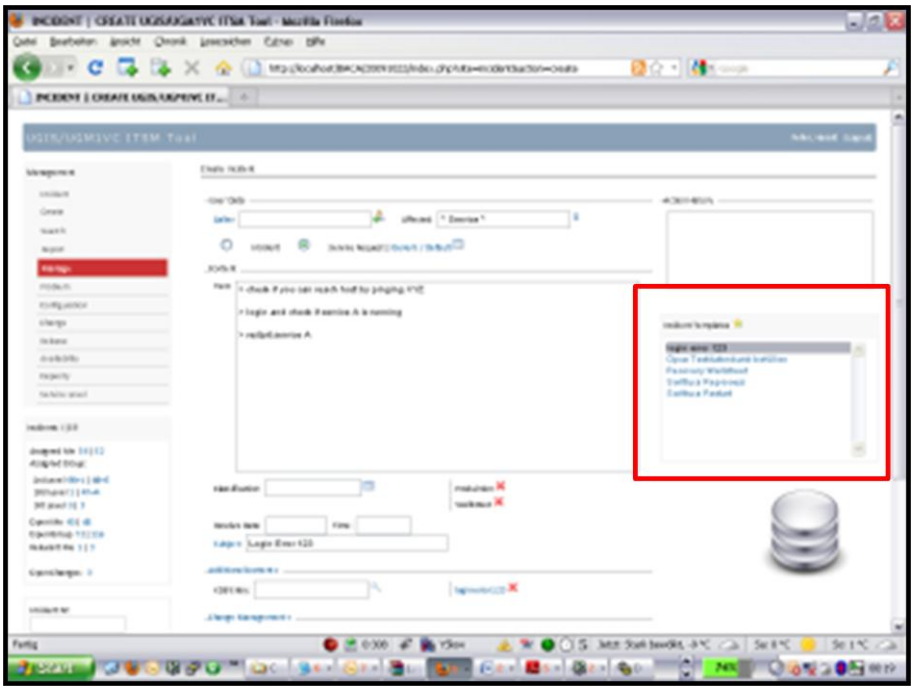


**Abbildung 50: Beispiel: Templates des Ticket Tools**

Beispielsweise könnte eine bestimmte Störung bei einem Druckertyp immer wieder auftreten. Ein Mitarbeiter füllt ein entsprechendes Störungsticket aus, indem er unter anderem die Schritte einer ausführlichen Störungsanalyse, Lösungswege und die Referenz zum SKMS erfasst. Dieses wird als Template allen Service Desk Mitarbeitern zur Verfügung gestellt. Tritt die Störung noch einmal auf, so kann sie effizient behandelt werden. Des Weiteren führt die einfache Handhabbarkeit durch das Ticket Tool dazu, dass alle Mitarbeiter ein einheitliches Vorgehen mit gleicher Qualität nutzen. In ITIL spricht man bei der Definition von Templates aufgrund vieler ähnlicher Störungen von vordefinierten Standard Incident Modellen. Incident Modelle bedingen eine spezielle Handhabung und müssen entsprechend bearbeitet werden. So werden beispielsweise Security Incidents toolunterstützt zu den Spezialisten Teams eskaliert.

Ein Incident Modell muss folgende Komponenten beinhalten:

- Jene Aktivitäten, die man zur Behandlung des Incidents durchführen muss
- Die Reihenfolge der Aktivitäten
- Zuständigkeiten, wer welche Aktivitäten durchführen muss

- Zeitliche Rahmenbeschränkungen, bis wann spätestens einzelne Aktivitäten durchzuführen sind und bis wann der Incident geschlossen sein muss
- Eskalationsverfahren
- Etwaige notwendige Beweissicherung, die vor allem für Security Incidents relevant ist

Ein weiterer Mehrwert entsteht, indem das Ticket Tool möglichst gut in anderen Werkzeugen und Informationsquellen integriert ist. Wenn beispielsweise eine Störung aufgenommen wird, sollte per Knopfdruck das SKMS nach bekannten, ähnlichen Störungsmustern durchsucht werden. Als Suchkriterien sollten die Eingaben des Incident Tickets herangezogen werden (Kurzbeschreibung, Kategorisierung, Klassifizierung usw.). Hilfreiche SKMS Einträge sollten als Referenz ebenfalls möglichst effizient zum Incident Ticket hinzugefügt werden.


**Abbildung 51: Beispiel: Verbindung zum SKMS (als Wiki realisiert) im Ticket Tool**

Analog zu den Vorteilen von Templates führen diese Maßnahmen zur Erhöhung der Transparenz und zur Vereinheitlichung der Vorgehensweise bei gleichbleibender Qualität.

In Zuge von Request Fulfillment sollte das Ticket Tool eine Auflistung gängiger Anforderungen effizient zur Auswahl anbieten.

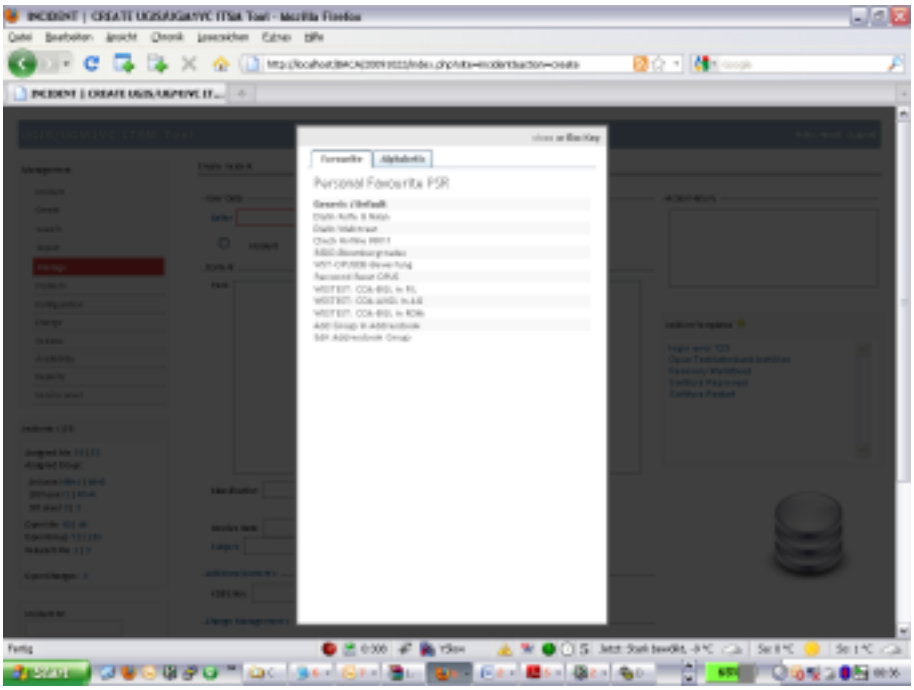


**Abbildung 52: Beispiel: Auswahl des Standard Changes im Ticket Tool**

Gängige Anforderungen werden in ITIL oftmals als Standard- Change behandelt. Hierbei handelt es sich um eine Kategorie von Request for Changes, welche vom Change Management bewilligt und aus Effizienzgründen entschieden wurde, gleichartige Anfragen nicht über das Change Management neuerlich zu bewerten, sondern direkt in Form von Standard- Changes im Request Fulfillment abzuarbeiten.

Wird ein Standard- Change ausgewählt, sollte der gesamte Workflow innerhalb des Ticket Tools abgebildet sein. Dies beinhaltet insbesondere die auszufüllenden Formulare, Freigabebewilligungen, hinzuzufügende Dateianhänge usw. pro Arbeitsschritt, als auch den Ablauf der einzelnen Arbeitsschritte, also in welcher Reihenfolge das Ticket von wem behandelt werden muss. Des Weiteren sollte es definierte maximale Bearbeitungszeiten pro Arbeitsschritt beinhalten, sodass automatisiert eine Eskalation angestoßen wird, wenn das Ticket aus irgendeinem Grund nicht weiter behandelt wird.

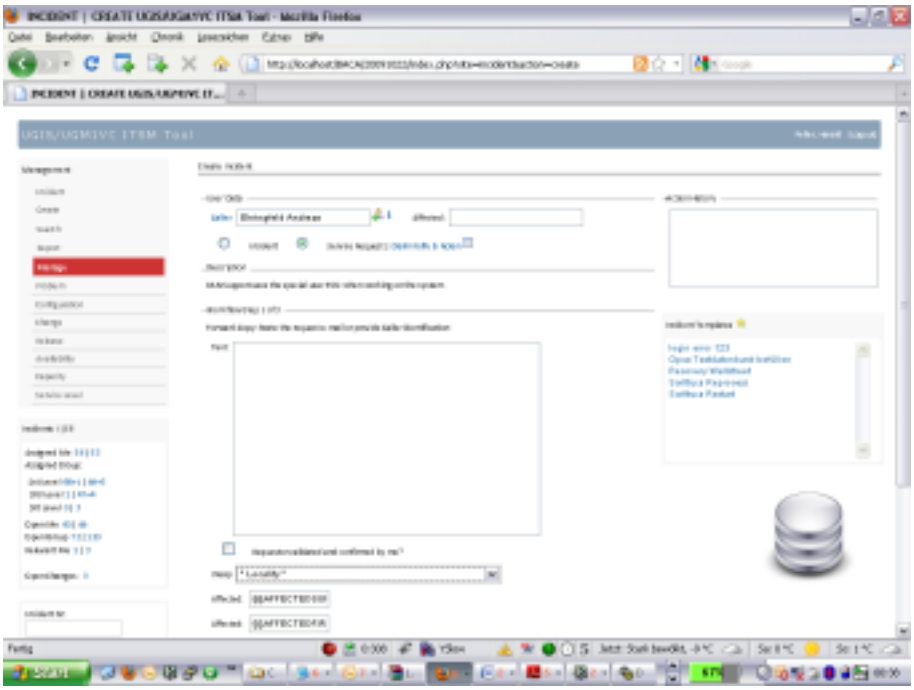


**Abbildung 53: Beispiel: Standard- Change Formular im Ticket Tool**

Durch die Automatisierung von Workflows werden nicht nur die Transparenz und die Vereinheitlichung der Vorgehensweise mit gleichbleibender Qualität einzelner Arbeitsschritte, sondern des gesamten Ablaufs sichergestellt. Ebenfalls kann es somit zu keinen Kommunikationsproblemen führen. Einzelne Arbeitsschritte können auch vollkommen automatisiert werden, wie zum Beispiel das Versenden von Bestätigungs- oder Informationsmails.

[itSMF02] definiert, dass es Aufgabe des jeweiligen Prozessmanagers (zum Beispiel verwaltet der Incident Manager den Incident Prozess) ist, die Effektivität und Effizienz des Prozesses zu überwachen. Auch obliegt es ihrer Verantwortung, Verbesserungsvorschläge aufzunehmen oder selbst zu erstellen, zu analysieren und gegebenenfalls umzusetzen. Durch die Berücksichtigung des Sicherheitsprinzips der Einfachheit wird sichergestellt, dass sich Mitarbeiter an die Vorgaben halten. Es stellt somit eine Basis für die Wirksamkeit anderer Sicherheitsprinzipien dar.

Einheitliches Vorgehen, vordefinierte Arbeitsabläufe, teilweise automatisierte Arbeitsschritte und eine definierte Kommunikation bei der Behandlung mehrerer Arbeitsschritte verringern die Erfolgschance von

Human- based Social Engineering Attacken oder verhindern sie gegebenenfalls gänzlich.

## 5.7 Das schwächste Glied sichern

*Ein Atomkraftwerk muss aufgrund seines Gefahrenpotentials höchsten Sicherheitsanforderungen unterliegen. Unfälle können Katastrophen globalen Ausmaßes annehmen. Die Nutzung der Kernenergie stellt durch die Gefährlichkeit von Radioaktivität der Spaltprodukte eine besondere Herausforderung dar, der durch den Einsatz vieler Sicherheitsmechanismen zu entgegnen versucht wird. Vielerlei Sicherheitsmechanismen werden eingesetzt, um den Betrieb eines Kernreaktors abzusichern.*

*Am 12. Dezember 1952 ereignete sich ein ernstzunehmender Reaktorunfall in Chalk River, Kanada. Während eines Tests des Forschungsreaktors wurde durch Fehlbedienungen, Missverständnisse zwischen Operator und Bedienungspersonal, falsche Statusanzeigen im Kontrollraum, Fehleinschätzungen und zögerliches Handeln des Operators der Reaktorkern bei einer partiellen Kernschmelze zerstört.*

*Am 28. März 1979 kam es in Zuge eines Unfalls im Kernkraftwerk Three Mile Island, USA, zu einer Kernschmelze, in der ein Drittel des Reaktorkerns fragmentiert wurde. Die Katastrophe konnte auch deswegen nicht verhindert werden, da 42 Stunden zuvor ein Test stattfand, bei dessen Ende vergessen wurde, Blockventile eines Notspeisesystems wieder zu öffnen. Damit reagierte zwar das Notsystem, als es zur Störung kam, war aber nicht funktional.*

*Am 26. April 1986 ereignete sich der wohl bekannteste und verheerendste Reaktorunfall, jener in Tschernobyl, Sowjetunion. Auch hier waren Teil der Ursache Fehlbedienungen sowie schwerwiegende Verstöße gegen geltende Sicherheitsvorschriften, welche in Kombination mit der Baueigenschaft des Reaktors zu der endgültigen Katastrophe führten.*

*Zu einer Umweltkatastrophe ganz anderer Art kam es am 24. März 1989, als der Öltanker Exxon Valdez auf ein Riff auflief. Der betrunkene Kapitän schlief gerade, als ein übermüdeter Offizier die Verantwortung auf der Brücke trug und eine abgestimmte Kurskorrektur verabsäumte.*

„Menschliche Fehler sind Symptome von tieferliegenden Fehlern im System. Um Versagen zu erklären, sollte man nicht nur danach suchen, wo

Menschen Fehler gemacht haben. Man muss auch danach suchen, warum die Einschätzungen und Handlungen von Menschen in der gegebenen Situation Sinn zu ergeben schienen.“ [Reas94]

Im Information Security Management gemäß ITIL als Teil des Service Design wird eine Security Strategie erarbeitet, damit Business Ziele entsprechend ihrer Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität erreicht werden. Das Information Security Management erarbeitet daraus eine Security Policy sowie ein davon abgeleitetes Information Security Management System (ISMS), welches die Standards und Management Verfahren zur Unterstützung der Security Policy beinhaltet.

In ITIL wird ISO/ IEC 27001 als formaler Standard zur Zertifizierung des ITSM durch eine unabhängige Organisation empfohlen. Hierbei sollte das Sicherheitsmodell bezüglich systematischen und konsistenten Designs, Umsetzung, Steuerung, Aufrechterhaltung und Sicherstellung der Informationssicherheitsprozesse und -kontrollen im Unternehmen geprüft werden (siehe [OGCO7]).

Das Information Security Modell nach ITIL unter Berücksichtigung gängiger Standards wie ISO/ IEC 27001 ergibt das folgende Framework.

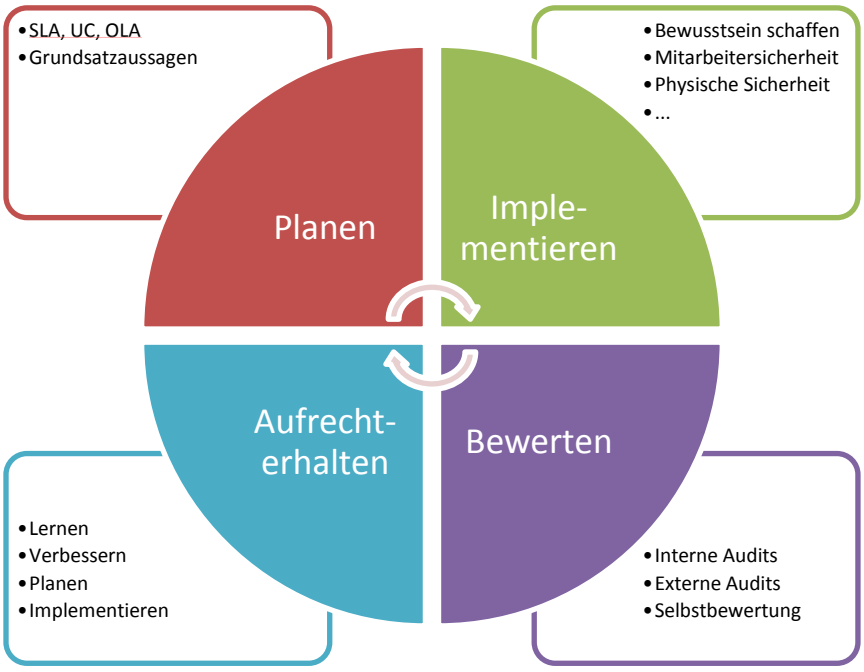



**Abbildung 54: Framework für Handhabung der Sicherheit [OGC07D]**

Durch die Steuerung der Phasen Planen, Implementieren, Bewerten und Aufrechterhalten wird ein Information Management System etabliert. Es dient weiterhin der Errichtung der Organisationsstruktur, welche die Informationspolitik vorbereitet, anerkennt und implementiert, und der Zuweisung von Verantwortung an die Mitarbeiter. [Breit09]

Im Information Security Management werden des Weiteren Schulungsstrategien, Kommunikationsstrategien und Grundsätze der Informationssicherheit erarbeitet. Überwachungsprozesse als Teil des Security Managements sollen die Einhaltung prüfen und gewährleisten. [Bon08D]

Obwohl sich ITIL als ganzheitliches Sicherheitskonzept versteht, das die Bereiche Personal, Prozesse, Produkte (inklusive der Technologie) sowie Partner (einschließlich Lieferanten) abdeckt [Bon08D] [Broe07], stellt eine Analyse in [Breit09] fest, dass ITIL sehr wohl identifiziert hat, dass Informationssicherheit eine Managementaktivität ist, nicht aber erläutert wird, wie das Management konkret dazu beitragen kann, dass das Thema Informationssicherheit einen adäquaten Stellenwert bei den Mitarbeitern des Unternehmens einnimmt. Des Weiteren wird ausgeführt, dass es im ITIL Best Practice Framework an Verfahren und Methoden fehlt, Mitarbeiter an das Thema Informationssicherheit heranzuführen. So wird in Abbildung 54 als Maßnahme die Schaffung von Bewusstsein in ITIL definiert, wie dies zu geschehen hat, wird allerdings nicht ausgeführt. Laut [Breit09] fehlt aber auch die explizite Schaffung der Motivation zu Informationssicherheit. Dies entspricht auch der Analyse menschlicher Fehler von [Reas94], in der die Frage, warum der Mensch eine bestimmte (fehlerhafte) Handlung oder Einschätzung gemacht hat, mit in den Vordergrund gerückt wird.

In [Zhan10] wird festgehalten, dass eine Zertifizierung entsprechend dem ISO-Standard zur Informationssicherheit nur auf der Basis von ISO 27001 stattfinden kann. Da dieser Standard auf den ISO 27002 Standard Bezug nimmt, muss ISO 27002 bei einer Zertifizierung unbedingt beachtet werden. Eine ausschließlich auf den ISO 27002 Standard ausgerichtete Zertifizierung, kann ohne Berücksichtigung des ISO 27001 Standards nicht realisiert werden.

Da ITIL zum Aufbau eines ISMS auf die Einhaltung des ISO/ IEC 27001 Standards verweist, werden die in ISO/ IEC 27002 angeführten Kontrollziele (engl. „Control Objectives“) für die folgende Analyse herangezogen. ISO/ IEC 27002 ist in elf Überwachungsbereiche mit insgesamt 39 Sicherheitskategorien gegliedert, zu jeder Sicherheitskategorie

ist ein Kontrollziel angegeben. Die Kontrollziele sind mit insgesamt 133 Sicherheitsmaßnahmen untersetzt, deren Anwendung die Erreichung unterstützt.

In ISO/ IEC 27001 wird in 5.1 festgehalten, dass das Management selbst seine eigene Verpflichtung für den gesamten ISMS Prozess nachweisen muss. Hierzu führt ISO/ IEC 27002 weiter in 6.1.1 die Verpflichtung des Managements aus, sich zur Informationssicherheit zu bekennen. Das Management soll aktiv Sicherheit innerhalb des Unternehmens durch klare Anweisungen, einem klaren Bekenntnis, explizite Verantwortlichkeiten und Anerkennung von Informationssicherheit fördern.

In ISO/ IEC 27002 wird der menschliche Faktor primär im Überwachungsbereich Human Ressource Security in Abschnitt 8 behandelt. Weiter strukturiert ist der Bereich in „Vor der Anstellung“, „Während der Anstellung“ und „Beendigung oder Veränderung der Anstellung“.

| # | Kontrollziel | Beschreibung |
|---|---|---|
| **8.1.** | **Vor der Anstellung** | |
| **8.1.1** | Rollen und Verantwortlichkeiten | Sicherheitsaufgaben und -verantwortung von Angestellten, Auftragnehmern und Externen müssen im Einklang mir den Informationssicherheitsgrundsätzen der Organisation definiert und dokumentiert werden. |
| **8.1.2** | Überprüfung | Überprüfungen der Vergangenheit aller Bewerber, Auftragnehmer und Externen müssen in Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen ausgeführt werden und den Geschäftsanforderungen, der Klassifikation der Informationen, die diese verwenden werden, und den erkannten Risiken angemessen sein. |
| **8.1.3** | Arbeitsvertragsklauseln | Als Teil ihrer vertraglichen Auflagen müssen Angestellte, Auftragnehmer und Externe den Vertragsklauseln ihres Anstellungsvertrags zustimmen und diesen unterzeichnen; diese Klauseln müssen ihre und die |

| | | |
|---|---|---|
| | | Verantwortlichkeiten der Organisation für Informationssicherheit festlegen. |
| **8.2.** | **Während der Anstellung** | |
| **8.2.1** | Verantwortung des Managements | Das Management muss verlangen, dass Angestellte, Auftragnehmer und Externe Sicherheit in Übereinstimmung mit den festgelegten Leitfaden und Verfahren der Organisation anwenden. |
| **8.2.2** | Sensibilisierung, Ausbildung und Schulung für Informationssicherheit | Alle Angestellten der Organisation, und, falls relevant, Auftragnehmer und Externe, müssen geeignete Sensibilisierungsmaßnahmen (engl. „Awareness“) in Sachen Informationssicherheit erhalten und regelmäßig über organisatorische Regelungen und Verfahren, die für ihre Arbeit von Bedeutung sind, informiert werden. |
| **8.2.3** | Disziplinarverfahren | Gegen Angestellte, die einen Sicherheitsverstoß begangen haben, muss ein formales Disziplinarverfahren eingeleitet werden. |
| **8.3** | **Beendigung oder Änderung der Anstellung** | |
| **8.3.1** | Verantwortlichkeiten bei der Beendigung | Die Verantwortlichkeiten für das Beenden oder Ändern eines Anstellungsverhältnisses müssen klar definiert und zugewiesen werden. |
| **8.3.2** | Rückgabe von organisationseigenen Werten | Alle Angestellten, Auftragnehmer und Externe müssen alle organisationseigenen Werte (engl. „Assets“) in ihrem Besitz bei Beendigung ihres Anstellungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben. |
| **8.3.3** | Zurücknahme von Zugangsrechten | Die Zugangsrechte aller Angestellten, Auftragnehmer und Externen zu Informationen und informationsverarbeitenden Einrichtungen müssen aufgehoben, wenn ihre Anstellung, ihr Vertrag oder ihre Vereinbarung endet, oder bei Veränderungen angepasst werden. |

**Tabelle 6: Human Ressource Security aus ISO/ IEC 27002**

Betrachtet man entsprechend [Rose02] die Bestimmungsgrößen für das Leistungsverhalten eines Mitarbeiters, so ist dies zunächst beeinflusst durch das persönliche Wollen und das individuelle Können. Diese beiden Faktoren sind die so genannten persönlichen Bestimmungsgrößen. Während das individuelle Können (Leistungspotential) geprägt wird durch Qualifikation, Training und Unterstützung, wird das persönliche Wollen (Leistungsbereitschaft) entscheidend durch die Motivation geprägt. Awareness ist ein Faktor, der sowohl dem persönlichen Wollen als auch dem individuellen Können zugeordnet werden kann.


**Abbildung 55: Bestimmungsgrößen des Verhaltens [Rose02]**

Das Verhalten von Menschen lässt sich aber nicht alleinig durch Motivation und Fähigkeit erklären, sondern, wie in [Rose02] festgestellt wird, durch die parallel dazu zu betrachtenden Situationsgrößen. Diese setzen sich aus sozialem Dürfen und situativer Ermöglichung zusammen.

Will man eine Absicherung des schwächsten Gliedes (engl. „Secure the Weakest Link“), also des Menschen, vor Social Engineering Attacken erreichen, so sollte man dies entsprechend ISO/ IEC 27001 und ISO/ IEC 27002 bereits beim Personalauswahlprozess und -verfahren berücksichtigen.

Bei neu einzustellenden Mitarbeitern ist es empfehlenswert, Können und Wollen in Bezug auf Sicherheit zu überprüfen. [Breit09] Unter der Begrifflichkeit der Eignungsdiagnostik versteht man verschiedene Verfahren und Methoden zur Messung der Kompetenz und von Verhaltensansätzen in Bezug auf Bildungswege und berufliche Tätigkeiten. Ziel der Eignungsdiagnostik ist, eine auf Wahrscheinlichkeit basierende Vorhersage zu treffen, ob ein Bewerber sowohl das Leistungspotential als auch die Leistungsbereitschaft für einen Bildungsweg oder eine berufliche Tätigkeit aufbringt.

Die Eignungsdiagnostik kennt laut [Schu05] drei klassische Ansätze, die sich in Methode und Validierungslogik unterscheiden. Die Eignung des Bewerbers kann über den Eigenschafts-, den Simulations- und den Biographieansatz gemessen werden. Beim Eigenschaftsansatz werden relativ stabile menschliche Merkmale mittels psychologischer Testverfahren ermittelt. Beim Simulationsansatz wird das Verhalten in und der Umgang mit bestimmten Situationen beobachtet, welche beispielsweise typische berufliche Tätigkeit nachstellen. Der Biographieansatz hingegen beurteilt auf Basis vergangener Erfahrungen und Merkmale. Hierzu werden Arbeitszeugnisse, Ausbildung, Spezialkurse, Projekterfahrung usw. analysiert.

Die DIN- Norm 33433 beschreibt die Anforderungen an Verfahren und deren Einsatz bei berufsbezogenen Eignungsbeurteilungen. Hierbei behandelt DIN 33433 sowohl die Planung der Eignungsbeurteilung, die Auswahl eines geeigneten Verfahrens zur Eignungsprüfung als auch die Interpretation der Auswahlverfahrensergebnisse. Ein ganz entscheidender Faktor, der auch in die Norm eingeflossen ist, ist die Bestimmung der Anforderungen an die Personen, die am Auswahlverfahren teilnehmen. Gerade hierbei können Fehler passieren, die zu einer Verfälschung der Ergebnisse führen (vergleiche hierfür die wissenschaftliche Untersuchung [Grec07] zu möglichen Einflussfaktoren bei der Verhaltensbeobachtung und -bewertung im Assessment Center).

Durch die Anwendung einer adäquaten Eignungsdiagnostik soll sichergestellt werden, dass auch im Bezug auf Sicherheit geeignete Mitarbeiter gefunden werden. Eine Vergangenheitsprüfung durch eine Strafregisterbescheinigung soll ebenfalls die Vertrauenswürdigkeit des Bewerbers sicherstellen. In besonderen Fällen ist auch eine Sicherheitsüberprüfung nach Sicherheitspolizeigesetz (SPG) §55 [Oest09] möglich.

Zusätzlich müssen Maßnahmen getätigt werden, sowohl das Wollen als auch das Können von Mitarbeitern zu steigern. Um das Können, also die Qualifikation, von Mitarbeitern zu steigern, müssen entsprechend ISO/ IEC 27001 und ISO/ IEC 27002 regelmäßig Schulungen durchgeführt werden. Die Qualifikation von Mitarbeitern umfasst nach [HoPr03] Maßnahmen zum Aufbau, Erhalt und Ausbau von Fähigkeiten und Fertigkeiten, die zur Bewältigung von tätigkeitsspezifischen Anforderungen notwendig sind. Diese wie in [Unbe01], [Kee08] beschriebenen Schulungsmaßnahmen zur Steigerung des Sicherheitsbewusstsein, stellen ein wertvolles Instrument gegen Social Engineering dar. Entscheidende Erfolgsfaktoren sind hierbei sowohl die Bereitstellung von allgemeinen Informationen, aber auch die Erläuterung sehr spezifischer Szenarien. Die Schulungsprogramme müssen auf die Bedürfnisse der Mitarbeiter angepasst werden. So ist es demotivierend, hochqualifizierte Mitarbeiter mit bekannten Sachverhalten zu langweilen. Dies gilt selbstverständlich nicht für die Auffrischung erlernten Wissens durch bewusste Wiederholung. Mitarbeiter in besonders sensiblen Bereichen benötigen jedenfalls eine intensivere Schulung bezüglich Sicherheit. Die im Schulungsinhalt enthaltenen Szenarien sollen der Arbeitssituation des Mitarbeiters entsprechen.

Neben Maßnahmen, das Können von Mitarbeitern zu verbessern, müssen auch Maßnahmen gesetzt werden, die das Wollen der Mitarbeiter steigern. In [HoPr03] wird ausgeführt, dass nur motivierte Mitarbeiter ihr gesamtes Leistungspotential einsetzen und sich um die Belange des Unternehmens kümmern und der Grad der Motivation entscheidenden Einfluss auf die Aufgabenbewältigung im Allgemeinen als auch auf eine gewissenhafte und sicherheitskonforme Bewältigung der Aufgaben hat.

Eine Studie von Hewitt im Jahr 2009 [Hewi09] hat ergeben, dass 31% der Unternehmen in Zentral- und Osteuropa der Meinung waren, dass die Leistungsbereitschaft der Mitarbeiter sinke. Im Vergleich dazu waren lediglich 15% im Vorjahr dieser Meinung. Als Grund für die gestiegene Unproduktivität der Mitarbeiter werden deren Zukunftsängste und Unsicherheiten aufgrund der schwachen wirtschaftlichen Lage identifiziert. In [LiHe07] werden mögliche Gründe für die Demotivation von Mitarbeitern als situative Bedingungen angesehen, die sich zeitnah ergeben. Die Einflussfaktoren werden auf die drei Ebenen – der Ebene der Organisation, des Teams und des Individuums – kategorisiert.

| Ebene | Beispiel |
|---|---|
| **Organisations-ebene** | • Mangelnde Transparenz der Unternehmensstrategie und -ziele<br>• Starre und unflexible Organisationsstrukturen<br>• Keine einheitliche Führungskultur<br>• Schlechtes Betriebsklima<br>• Unbefriedigende Arbeitsbedingungen |
| **Teamebene** | • Fehlende Anerkennung und Unterstützung<br>• Mangelnde Informationsweitergabe<br>• Einsame oder fehlende Entscheidungen<br>• Unzureichende Mitwirkung/Einbindung in Entscheidungsfindungsprozesse<br>• Ineffiziente Meetingkultur<br>• Delegationsfehler |
| **Individualebene** | • Unsicherheit, Ängstlichkeit, Depression<br>• Zu hohe Erwartungshaltung an die eigene Leistung<br>• Fehlende Work-Life-Balance<br>• Intrapersonelle Rollenkonflikte (Beruf – Familie)<br>• Erlebte Einschränkungen in Selbstverwirklichung und Autonomie<br>• Kompetenz stimmt nicht mit Anforderungsgrad der Aufgaben überein (Folge: Über- oder Unterforderung |

**Tabelle 7: Gründe für die Demotivation von Mitarbeitern [LiHe07]**

Es gibt eine Reihe von Arbeiten und wissenschaftlichen Analysen, welche Maßnahmen zur Motivationssteigerung von Mitarbeitern behandeln. Beispielsweise sei auf [Beck90], [HeKa05], [Nerd03], [Lauf04] und [CoRo09] verwiesen.

Neben den persönlichen Bestimmungsgrößen sind nach [Rose02] auch Situationsgrößen entscheidend für das Leistungsverhalten von Mitarbeitern. Hierbei handelt es sich um objektiv fördernde oder hindernde Bedingungen als auch um Gesetze, Normen und Betriebsvereinbarungen. Auch diese Faktoren müssen vom Management berücksichtigt werden, damit Mitarbeiter ihr volles Leistungspotential ausschöpfen können. Die Aspekte des sozialen Dürfens sind in der Organisationsebene von [LiHe07] abgedeckt. Aspekte der situativen Ermöglichung können nicht klar erfasst werden. Sie umfassen die Ergonomie des Arbeitsplatzes, Klimatisierung bis hin zu umfangreichem Büromaterial und dem Einsatz adäquater Kommunikationssysteme. Sie umfasst des Weiteren die Bereitstellung von

Verpflegung, wie Kaffee und Wasser, bis hin zur Lärmbelästigung am Arbeitsplatz.

Die Schulungen der Mitarbeiter, motivationssteigernde Maßnahmen als auch die Beeinflussung von Situationsgrößen müssen Bestandteil einer Strategie zur Etablierung von Bewusstsein vor der Gefahr von Social Engineering Attacken sein. In [Mann08] wird diese Strategie in vier Phasen gegliedert. Die erste Phase soll die immer gegenwärtige Gefahr vor Social Engineering Attacken in den Köpfen der Mitarbeiter festigen. Hierbei werden Maßnahmen wie die erläuterten Schulungen eingesetzt, aber auch Poster (siehe dazu die im Anhang angeführten Beispiele), Informationsmaterial in Intranetseiten uvm.

In Phase zwei muss eine Sicherheitskultur bei den Mitarbeitern des Unternehmens aufgebaut werden. Entscheidend hierfür ist deren Motivation.

Die dritte Phase der Sicherheitsstrategie vor Angriffen eines Social Engineers entsprechend [Mann08] ist das Etablieren von so genannten Alarmauslösern. Hierzu müssen Mitarbeiter trainiert werden, bestimmte Merkmale von Human- based Social Engineering als solche zu erkennen. Beispielsweise wenn ein Anrufer auffällig freundlich ist, seltsame oder ungewöhnliche Anfragen stellt, die Dringlichkeit übermäßig betont wird, besonders stark über Autorität Druck ausgeübt wird oder auffällig oft die Zugehörigkeit zum Unternehmen betont wird (vergleiche hierzu Kapitel 4.3), sollten Mitarbeiter vorsichtig, misstrauisch und vorgewarnt vor Engineering Attacken reagieren oder gegebenenfalls Alarm schlagen.

Neben der menschlichen Etablierung von Alarmauslösern wird in Zuge dieser Arbeit auch eine technische Möglichkeit präsentiert. Grundsätzliche Idee ist, dass bei der Erfassung von Incidents oder Service Request Tickets, eine Kategorisierung im Ticket Tool durchgeführt wird. Beispielsweise ruft ein Mitarbeiter X an und möchte für die Applikation XYZ eine Freigabe auf das Storage. Dieser Sachverhalt spiegelt sich in der CMDB wider, wenn die Kategorisierung „Mitarbeiter X“, „Applikation XYZ“, „Storage“ durchgeführt wird und die Kategorien die Stützpunkte eines Graphen aufbauen.

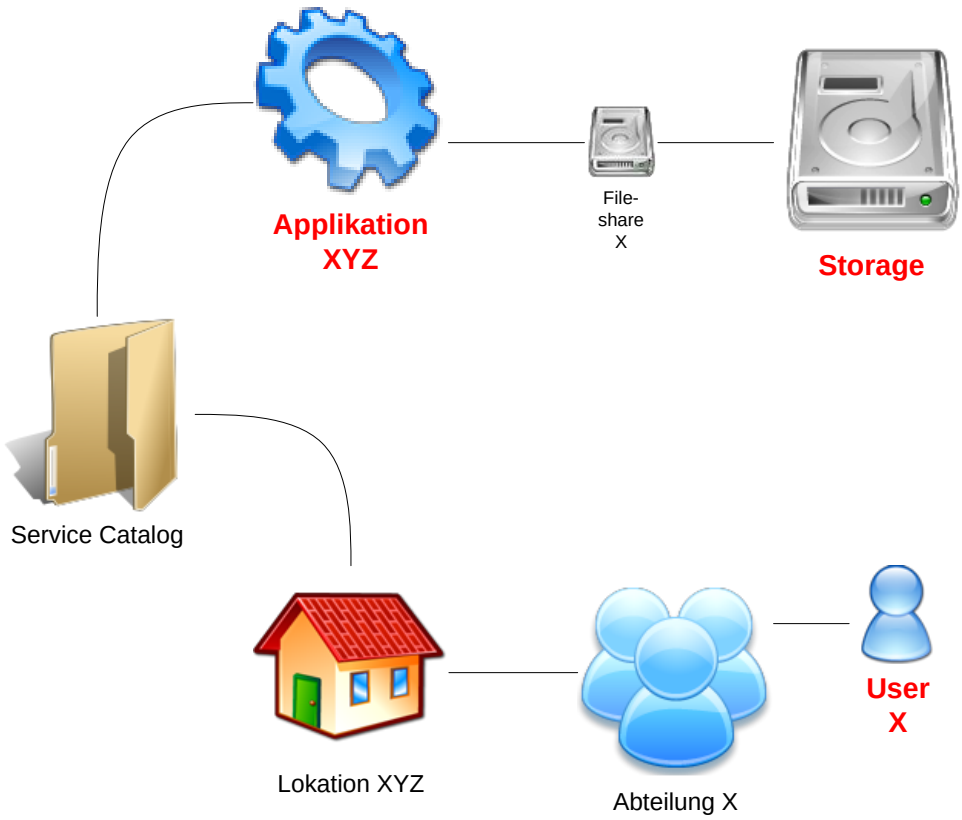



**Abbildung 56: Incident/ Service Request – CMDB – Spanngraph**

Baut man nun einen Spanngraph aus diesen Stützpunkten durch Ermittlung der kürzesten Pfade innerhalb der CMDB auf, so wird die Auswirkung des Service Requests ersichtlich. Wenn beispielsweise der Mitarbeiter X keine Rechte auf Applikation XYZ hat, ist dieser Graph nicht verbunden, besteht also aus zwei unverbundenen Graphen. In diesem Fall kann automatisch eine Warnung im Ticket Tool ausgegeben werden.

Grundsätzlich bietet dieses Verfahren eine effiziente Informationsbereitstellung für die Beurteilung und Behandlung des Incidents oder des Service Requests. Der Mitarbeiter wird in seiner Tätigkeit unterstützt. Zusätzliche Informationen, wie zum Beispiel aktuelle Incidents oder Wartungsarbeiten innerhalb des Graphen, können den Mehrwert weiter steigern. In der Praxis sieht ein derartiger Graph wie in der folgenden Darstellung aus. Hierbei ist auf einen Blick erkennbar, dass eine Vielzahl offener Incidents auf den Pfaden liegen.

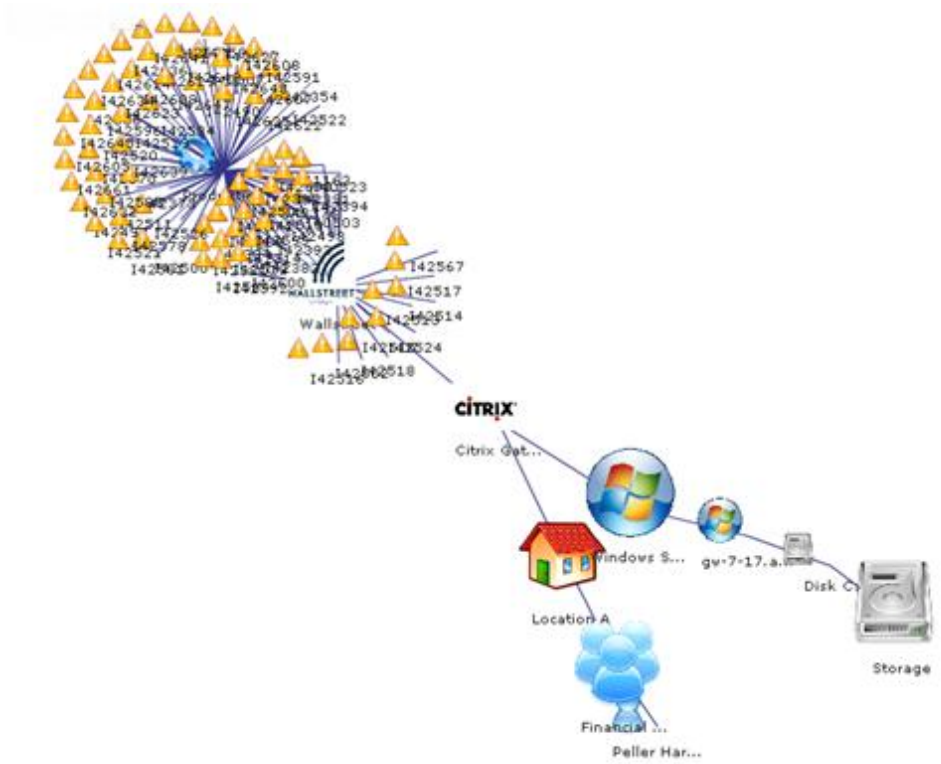



**Abbildung 57: Incident/Service Request – CMDB – Spanngraph mit eingezeichneten Incidents**

Eine andere Möglichkeit der automatisierten Alarmerkennung von Social Engineering Angriffen ist die Suche nach Anomalien in Tickets über Reports. Werden beispielsweise von einem Mitarbeiter ungewöhnlich viele Anfragen innerhalb einer bestimmten Zeit gestellt oder wird die Anfrage des Mitarbeiters einer für ihn ungewöhnlichen Kategorie zugewiesen, so würde dies automatisch erkannt und ein entsprechender Eskalationsprozess eingeleitet werden.


**Abbildung 58: Vier Phasen zur Etablierung einer Strategie für Bewusstsein von möglichen Social Engineering Angriffen [Mann08]**

Entsprechend [Mann08] sind Tests die vierte Phase einer Strategie zur Etablierung eines Gefahrenbewusstseins möglicher Human- based Social Engineering Attacken. Der Aspekt des Testens wird in Kapitel 5.9 näher erläutert. Grundsätzlich soll damit sowohl Erlerntes regelmäßig erprobt, als auch Geleistetes verifiziert werden.

## 5.8 Das Rad nicht immer neu erfinden

*Das Open Systems Interconnection (OSI) Referenzmodell ist ein Architekturmodell für offene Kommunikationssysteme. Offene Kommunikationssysteme besitzen die Fähigkeit, mit anderen Systemen zu kommunizieren und zu kooperieren. Kooperieren bedeutet dabei die Kommunikation zwischen Systemen zu dem Zweck, eine gemeinsame Aufgabe zu erledigen bzw. ein gemeinsames Anfangsverständnis durch Übertragung von Informationen fortzuschreiben.* [Sieg99] *Das Ziel des OSI-Referenzmodells ist es, eine herstellerunabhängige Kommunikation zwischen verschiedenen Teilnehmern zu ermöglichen. Dazu werden standardisierte Protokolle genutzt.* [Mank07]

*Das ursprüngliche Modell, welches von der International Organization for Standardization (ISO) entwickelt wurde, besteht aus sieben Schichten. Es ist eine Aufteilung der für eine Kommunikation notwendigen Funktionen. Jede*

*Schicht hat ihre eigenen Protokolle, die für einen geregelten Informationsaustausch zwischen Schichten der gleichen Ebene von verschiedenen Endterminals sorgt. Dabei baut eine Schicht auf der anderen auf, das heißt, eine Schicht N stellt ihre Kommunikationsmöglichkeiten als Dienst der übergeordneten Schicht N+1 zur Verfügung und nutzt selber die Dienste der Schicht N-1.* [Mank07]

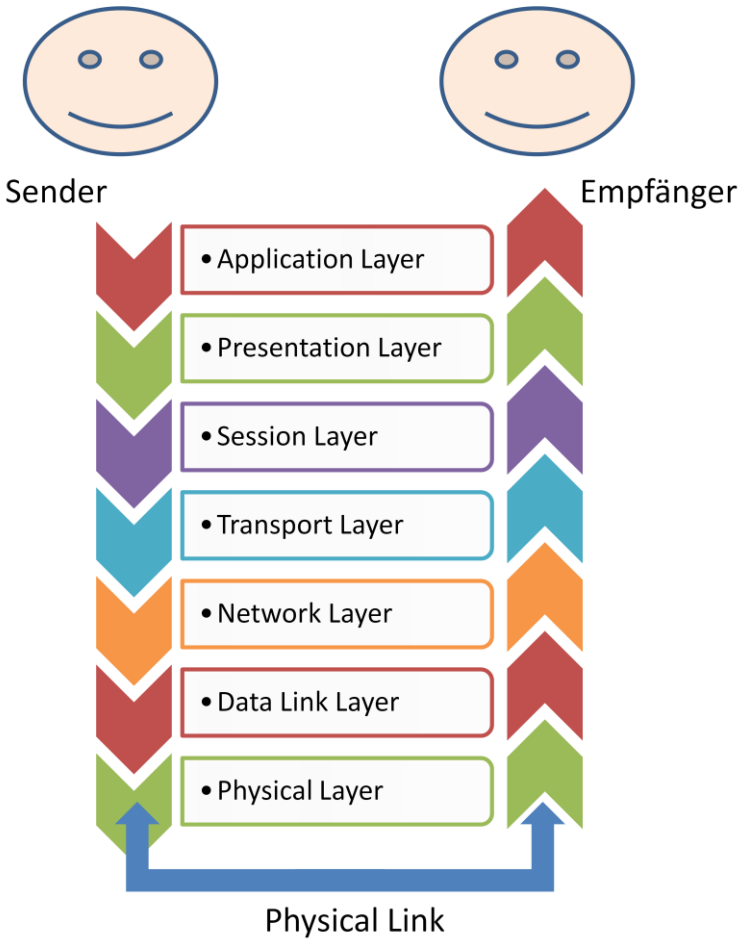



**Abbildung 59: OSI-Modell**

*Durch dieses Schichtenmodell müssen sich Applikationen nicht um Verbindungsaufbauten, Transport der Daten über die Leitung, Wiedersenden bei Datenverlust oder Verbindungsprobleme und vieles mehr kümmern. All diese Funktionen werden von der tieferliegenden Schichten erfüllt.*

*Aus Sicherheitssicht bedeutet das, dass eine Vielzahl an Anwendungen auf die darunter liegenden Schichten des OSI-Modells zugreift. Ein etwaiger*

*Fehler wirkt sich somit auf alle darüber liegenden Schichten und Anwendungen aus. Dem entgegen ist aber die Wartung im Schichtenmodell praktikabel. Der Fehler kann durch den Tausch einer Komponente behoben werden. Ansonsten müsste jede Anwendung neu installiert werden, was absolut unpraktikabel ist. Auch ist davon auszugehen, dass in der Regel Anwendungsentwickler keine Netzwerkspezialisten sind, weshalb sich im Sinne der Kompetenzaufteilung und der wesentlich schnelleren Entwicklung von Anwendungen das Modell durchgesetzt hat.*

Wie in Kapitel 5.7 dargestellt, verweist ITIL bei der Implementierung, Etablierung und Pflege eines ISMS auf den ISO/ IEC 27001 Standard. ITIL versucht somit das Rad nicht neu zu erfinden, sondern auf Bewährtes aufzubauen.

Betrachtet man die elf Überwachungsbereiche des ISO/ IEC 27001 Standards, so kann man sie in Management Aspekte, technische Aspekte und physische Aspekte gliedern. Zusätzlich haben die Bereiche eine unterschiedliche organisatorische und betriebliche Gewichtung, wie in der folgenden Abbildung dargestellt.

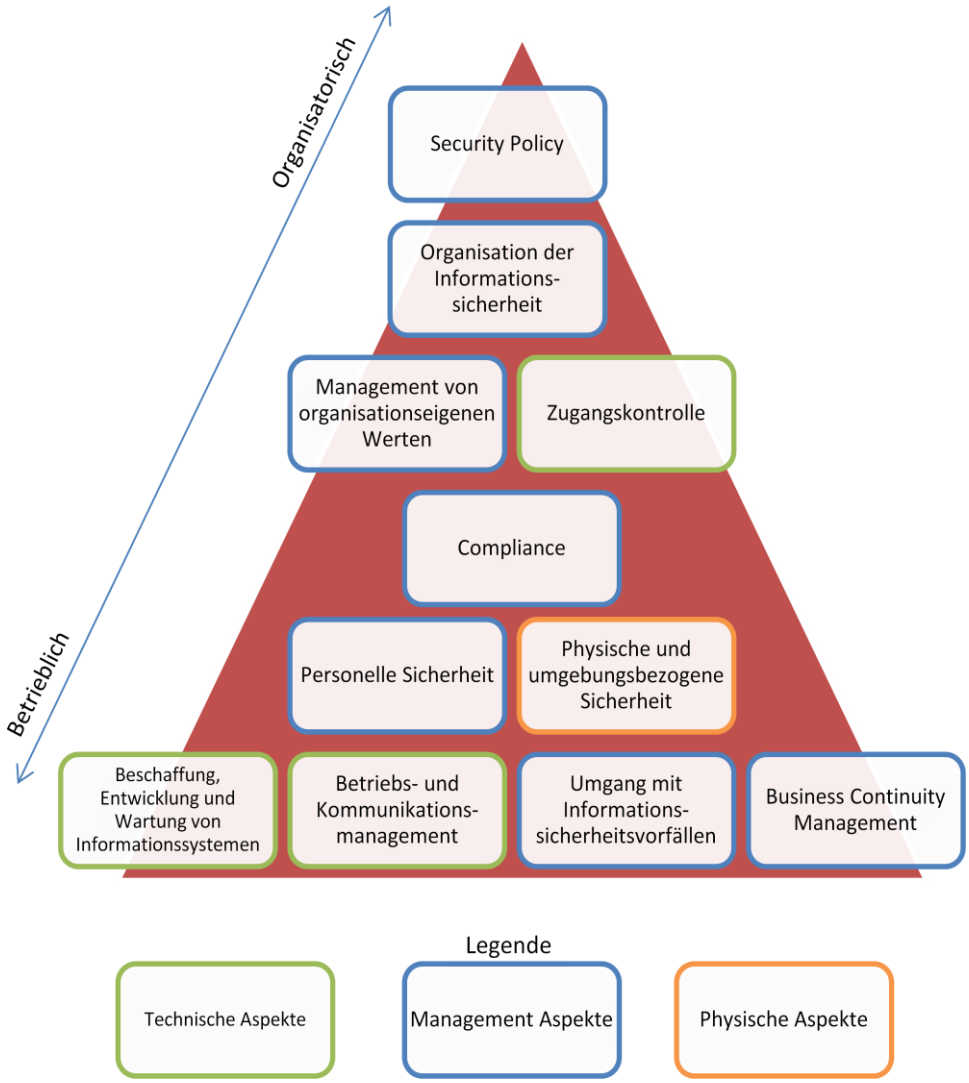



**Abbildung 60: Überwachungsbereiche des ISO/ IEC 27001 Standards**

ISO/ IEC 27001 deckt somit mehrere Bereiche ab, die nun vorgestellt werden. Für weiterführende Informationen wird auf [Zhan10] und [Kers09] verwiesen.

Die **Sicherheitsleitlinie** (engl. „Information Security Policy“) dient dazu, dem Management vor dem Hintergrund der Geschäftsanforderungen und der anzuwendenden Gesetze und Regelungen Orientierung und Unterstützung bei der Informationssicherheit zu geben. Man kann diesen Überwachungsbereich als das Rahmenwerk für alle Maßnahmen verstehen.

Im Überwachungsbereich der **Organisation der Informationssicherheit** (engl. „Organization of Information Security“) geht es um die Handhabung der Informationssicherheit innerhalb und außerhalb der Organisation. So werden neben der Organisation auch Kunden, Externe, spezielle Interessensgruppen und Behörden explizit berücksichtigt und eingebunden. Der Regelbereich umfasst das Engagement des Managements, Koordinations- und Steuerungsmaßnahmen sowie Verantwortlichkeiten und Kontrollmechanismen zu Informationssicherheit.

**Management von organisationseigenen Werten** (engl. „Asset Management“) behandelt Managementaspekte zur Erreichung und Erhaltung eines angemessenen Schutzes der organisationseigenen Informationswerte. Organisationseigene Informationswerte müssen inventarisiert und eine klare Eigentumszuordnung muss durchgeführt werden. Es ist notwendig, Informationen bezüglich ihres Wertes, ihrer gesetzlichen Anforderungen, ihrer Sensibilität und ihrer Kritikalität für die Organisation zu klassifizieren und geeignet zu kennzeichnen. Darauf basierend müssen Verfahren und Methoden zum geeigneten Umgang mit Information umgesetzt werden. Die Klassifizierung in unterschiedliche Vertraulichkeitsstufen bewirkt, dass Information entsprechenden Schutzzonen zugeordnet werden kann. Stellt man sich die Kategorisierung als Schutzschichten mit von innen nach außen gehenden Schalen „streng geheim“, „geheim“, „vertraulich“ und „öffentlich“ vor, so ist ersichtlich, warum man von Informationspolitik nach außen spricht. Dies entspricht dem Sicherheitsprinzip, einem Angreifer nur eine möglichst kleine Angriffsfläche zu bieten (engl. „Reduce Your Attack Surface”).

In der **Personellen Sicherheit** (engl. „Human Resources Security”) wird die Qualifikation und Zuverlässigkeit vom Personal behandelt. Dieser Überwachungsbereich wird in Kapitel 5.7 im Speziellen in der Risikobetrachtung von Human- based Social Engineering Attacken ausführlich behandelt.

Der Überwachungsbereich der **Physischen und Umgebungsbezogenen Sicherheit** (engl. „Physical and Environmental Security“) umfasst die Definition von Sicherheitszonen, Zutrittskontrollen, Sicherungen von Büros, Räumen und Einrichtungen. Es soll sichergestellt werden, dass Unberechtigte keinen physischen Zugriff auf Informationen haben. Hierzu sind klassische Sicherheitsmaßnahmen wie Wände, Sicherheitstüren, Alarmsicherungen usw. notwendig. Des Weiteren werden aber auch

Vorgaben zum Arbeiten in der Sicherheitszone beschrieben. Daraus ergibt sich zum Beispiel, dass Wartungstechniker nur nach Anmeldung, Genehmigung und unter Aufsicht etwaige Reparaturen in Schutzbereichen durchführen dürfen. Gegebenenfalls muss das Reinigungspersonal beaufsichtigt werden. Selbst im Brandfall muss das geordnete Verlassen der Sicherheitszonen sichergestellt werden. Die geeignete Platzierung und der Schutz von Betriebsmittel wie beispielsweise der Blickschutz bei Authentifizierungsgeräten ist ebenso zu berücksichtigen wie die Wartung und Entsorgung der Betriebsmittel. So müssen Speichermedien vor der Entsorgung nicht wiederherstellbar gelöscht werden. All diese Maßnahmen zielen direkt darauf ab, Attacken eines Social Engineers wie Dumpster Diving und Shoulder Surfing entgegenzuwirken.

Das **Betriebs- und Kommunikationsmanagement** (engl. „Communications and Operations Management“) soll den regelkonformen Ablauf aller Prozesse, ein systematisches Nachverfolgen aller Aktivitäten und eine Aufteilung von Verantwortlichkeiten auf definierte Rollen sicherstellen. Zusätzlich soll es eine Trennung von Entwicklung und Produktion und eine ausreichend tiefe Erzeugung von Nachweisen geben.

Die **Zugangskontrolle** (umfasst auch Zugriffskontrolle, engl. „Access Control“) befasst sich mit dem kontrollierten Zugang, Zutritt und Zugriff zu Informationsobjekten der Organisation. Von Benutzerverwaltung, Passwortverwendung, Benutzerrechen bis hin zu dem Grundsatz des aufgeräumten Schreibtisches und leeren Bildschirms umfasst der Überwachungsbereich sowohl technische als auch organisatorische Maßnahmen. Netzwerkbereiche müssen entsprechend den Schutzzonen segmentiert werden. Session Timeouts sollen inaktive Sitzungen sperren und einem Social Engineer keinen Zugriff auf das System erlauben. Auch dass der Arbeitsplatz aufgeräumt sein muss, soll sicherstellen, dass ein Angreifer, der zum Beispiel außerhalb der Arbeitszeiten Zutritt zu den Räumlichkeiten hat, keinen Zugriff auf Daten, Medien und Dokumente erlangen kann. Organisatorische Maßnahmen wie Betriebsanweisungen für Telearbeiter und Leitlinien zur sicheren Verwendung von Mobile Computing und Kommunikationseinrichtungen müssen festgelegt werden.

Die **Beschaffung, Entwicklung und Wartung von Informationssystemen** (engl. „Information Systems Acquisition, Development and Maintenance“) berücksichtigt Sicherheitsaspekte bei der Planung, Beschaffung Entwicklung, Integration und Wartung von Systemen.

Der Überwachungsbereich des **Umgangs mit Informationssicherheitsvorfällen** (engl. „Information Security Incident Management“) regelt von der Meldung von Sicherheitsvorfällen (engl. „Security Incident“) bis hin zum Sammeln von Beweisen und dem Lernen aus Vorfällen alle diesbezüglichen Schritte. Zusätzlich sollen proaktiv Schwachstellen identifiziert und geeignet behandelt werden.

Das **Sicherstellung des Geschäftsbetriebs** (engl. „Business Continuity Management“) soll den unterbrechungsfreien Betrieb bzw. das ordnungsgemäße Wiederanlaufen im Katastrophenfall sicherstellen. Prinzipiell verhindert der Einsatz geeigneter Maßnahmen und Verfahren die Unterbrechung von Geschäftsprozessen. Zusätzlich sollte die Auswirkung personeller und technischer Ausfälle oder von Elementarereignissen auf die Geschäftsprozesse begrenzt werden. Wenn es zu Ausfällen kommt, sollte so schnell wie möglich eine Fortführung der Geschäftsprozesse sichergestellt werden.

Die **Einhaltung von Vorgaben** (engl. „Compliance“) betrachtet alle Maßnahmen aus dem Blickwinkel der rechtlichen Einordnung. Anwendbare Gesetze, amtliche und vertragliche Forderungen und diverse Rechte müssen genau so berücksichtigt werden wie beispielsweise der Datenschutz, das geistige Eigentum oder die Vertraulichkeit personenbezogener Daten. Die Mitverantwortung des Managements, die Prüfung der Einhaltung der Maßnahmen als auch Revisionen werden in diesem Überwachungsbereich behandelt.

Innerhalb dieses Überwachungsbereichs kann die Notwendigkeit und Prüfung der Einhaltung von weiteren Sicherheitsregelungen und -standards, wie beispielsweise im Grundschutzkatalog, definiert werden.

## 5.9 In Frage stellen

*Der Aderlass ist eine der ältesten Behandlungsverfahren in der Medizin. Bereits in der Antike wurden Kranken nicht unerhebliche Mengen an Blut abgenommen. Es galt so zu sagen als generelles Heilmittel und Verfahren. Die Grundlage hierfür war zum einen der feste Glaube, dass sich Blut in den Gliedmaßen stauen und so verderben würde, zum anderen dass ein Gleichgewicht zwischen der Menge an Blut, gelber und schwarzer Galle und Schleim herrschen müsse. Selbst als im 17. Jahrhundert die Wirksamkeit des Aderlasses wissenschaftlich widerlegt wurde, kam er bis*

*zum frühen 19. Jahrhundert weiterhin zum Einsatz und die Wirksamkeit wurde nicht in Frage gestellt.*

Das Sicherheitsprinzip des Infragestellens hat mehrere Ausprägungen. Das grundsätzliche Wesen dieses Sicherheitsprinzips ist es, regelmäßig alles neuerlich zu analysieren und nichts als gegeben anzunehmen. Dies findet sich in mehreren Bereichen von ITIL wieder und wird zusammengefasst in diesem Abschnitt behandelt.

In Frage stellen bedeutet, nicht blind darauf zu vertrauen, dass die gelieferte Leistung den Anforderungen des Betriebs oder des Kunden entspricht.

In ITIL ist in der Qualitätssicherung der von Deming [Demi86] entwickelte PDCA-Zyklus fest verankert (siehe [itSMF02]). Der PDCA-Zyklus, oftmals auch als Demingkreis bezeichnet, besteht aus vier Schritten. Im Plan-Schritt wird die Umsetzung geplant, im Do-Schritt die Umsetzung vollzogen, im Check-Schritt die realisierte Umsetzung mit den Zielvorgaben der Planung verglichen und im Act-Schritt wird gegebenenfalls eine neuerliche Planung initiiert, um sich durch Änderungen den Zielvorgaben weiter anzunähern.

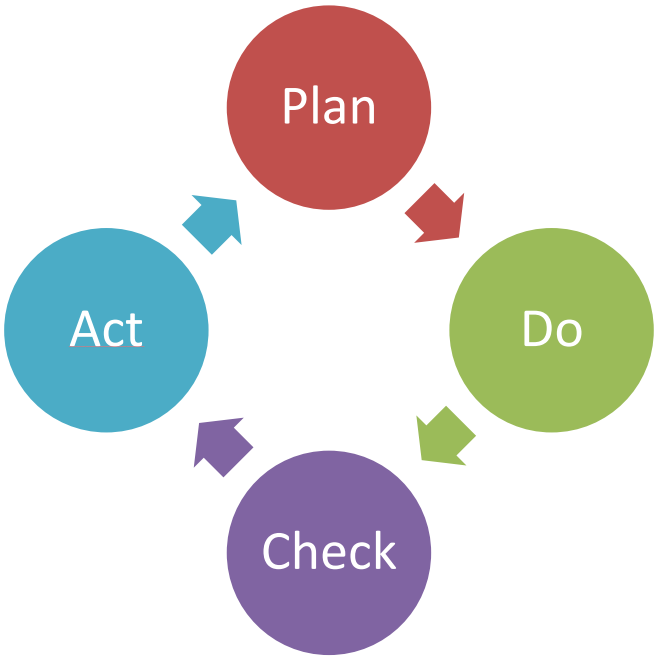



**Abbildung 61: PDCA-Zyklus [Demi86]**

Das Sicherheitsprinzip des Infragestellens ist direkter Bestandteil des PDCA-Zyklus. Erbrachten Leistungen wird in gewisser Weise misstraut und

so wird im Schritt Check die Qualität der Umsetzung geprüft. Diese Prüfung wird zumeist mit Messungen durchgeführt. Messen, Verifizieren und Analysieren der Umsetzung sind wesentliche Tätigkeiten des Prozessverantwortlichen (zum Beispiel ist der Incident Manager für den Incident Management Prozess verantwortlich), dessen Aufgabe die Steuerung und die kontinuierliche Verbesserung des jeweiligen Prozesses ist. Alle Service Operation Prozessumsetzungen sollten unter anderem die Robustheit vor Social Engineering als Zielvorgabe haben.

Eine besondere Art des Prüfens ist das so genannte Penetration Testing. Hierzu schlüpft ein Sicherheitsexperte in die Rolle eines Angreifers und versucht mit dessen Mitteln die Sicherheitsmechanismen zu umgehen oder auszutricksen. Das System soll so korrumpiert werden, dass der Angreifer nichtautorisierten Zugriff auf sensible Daten erhält. Die Gesamtsicherheit wird direkt gegen typische Angriffsmuster geprüft, man versucht somit Schwachstellen zu identifizieren. Auch im Bereich von Human- based Social Engineering gibt es Penetration Tests. In [DiPi09] werden zwei Methoden vorgestellt, wie auf Social Engineering Methoden basierende physische Penetration Tests durchgeführt werden können. Die beiden Methoden unterscheiden sich dadurch, ob das Opfer weiß, dass ein Penetration Test durchgeführt wird oder nicht.

Die Durchführung von Human- based Social Engineering Penetration Tests ist besonders heikel, da Angestellte durch die Penetration Tests verärgert werden können, die Privatsphäre verletzt oder das Vertrauen der Mitarbeiter in das Unternehmen und die Unternehmensführung beeinträchtigt werden kann. Rechtlichen Bestimmungen können durch diese Tests verletzt und die Produktivität des Unternehmens kann gefährdet werden. Gerade wenn sich beispielsweise herausstellt, dass ein bestimmter Mitarbeiter dem Angreifer fälschlicherweise sensible Informationen preisgegeben hat, stellt dies in weiterer Folge eine unglaubliche Stresssituation für den Mitarbeiter dar. In den Augen seiner Kollegen verliert er an Vertrauen und Respekt. Dieser Umstand macht die Durchführung von Social Engineering Penetration Tests besonders heikel. Auch ist deren Aussagekraft durch den Faktor Mensch anders zu bewerten als bei Penetration Tests einer technischen Infrastruktur. Der gleiche Mensch kann in scheinbar genau der gleichen Situation anders reagieren. Da die Einflussfaktoren wie gute Laune wegen eines bevorstehenden Urlaubs, Übermüdung und Kopfschmerzen aufgrund einer Party tags davor, schlechte Stimmung wegen eines Streits mit der Ehefrau, Wohlbefinden aufgrund eines guten Mittagessens und vieles mehr unbestimmbar sind, aber Auswirkungen auf den Testausgang haben, sind

Human- based Social Engineering Penetration Testergebnisse entsprechend zu bewerten.

Durch den in ITIL integrierten PDCA-Zyklus wird die Qualität kontinuierlich gesteigert, das heißt die Realisierung erfüllt immer besser die Zielvorgaben.

In Frage stellen bedeutet aber nicht nur, die Zielerfüllung einer abgeschlossenen Realisierung zu prüfen, sondern auch direkt die operativen Tätigkeiten zu kontrollieren. Der in Abbildung 38 dargestellte Incident Management Prozess wird von einen Kontrollprozess begleitet. Hierbei kontrolliert der Incident Manager alle oder zumindest alle signifikanten Tickets, ob sie entsprechend den Vorgaben behandelt werden. Ebenfalls identifiziert er all jene Tickets, die eine Service Level Agreement Verletzung verursachen könnten, hält Rücksprache mit dem Ticket Bearbeiter und leitet gegebenenfalls entsprechende Gegenmaßnahmen, wie zum Beispiel das Bereitstellen weiterer Ressourcen, ein. Der in ITIL bestimmte Aufgabenbereich der Prozessmanager stellt ein Vier-Augen-Prinzip für alle wesentlichen Tickets dar. Das Bewusstsein der Mitarbeiter, dass Tickets durch die Prozessmanager kontrolliert werden, stärkt direkt den Schutz vor Social Engineering. Die Schwelle, den Mitarbeiter zu einer ihm als unrechtmäßig bewussten Handlung zu überreden, erhöht sich. Zusätzlich erhöht sich die Wahrscheinlichkeit, dass der Angriff eines Social Engineers erkannt wird, da der Prozessmanager zusätzlich den Sachverhalt und die Tätigkeiten prüft.

Grundsätzlich zeigt sich somit, dass die Sicherheitsprinzipien der Transparenz, Funktionstrennung (engl. „Functional Separation“) und minimalen Ausübungsrechte (engl. „Least Privilages“) fest im ITIL Framework verankert sind.

Eine noch tiefgreifendere Ausprägung des Sicherheitsprinzips des Infragestellens ist die Notwendigkeit eines etablierten internen Kontrollsystems (IKS). Das IKS umfasst alle in der Unternehmensorganisation vorgesehenen Maßnahmen, die dazu bestimmt sind, das vorhandene Vermögen zu sichern, die betriebliche Leistungsfähigkeit zu steigern und die Einhaltung der Geschäftspolitik sowie der Richtlinien und Vollständigkeit der Aufzeichnungen zu gewährleisten. [KlRi06] Es beinhaltet alle Formen von prozess- und organisationsimmanenten Überwachungsmaßnahmen, die in die zu überwachenden Geschäftsvorfälle integriert sind. [BeBe04] Zusätzlich soll

durch ein IKS die Zuverlässigkeit von betrieblichen Informationen als auch die Funktionsfähigkeit sichergestellt werden.

Die Bedeutung des internen Kontrollsystems wächst mit der Größe des Unternehmens [KlRi06] sowie mit der Zunahme an rechtlichen Vorgaben, die ein Unternehmen erfüllen muss (vergleiche hierzu beispielsweise den Sarbanes Oxley Act 2002 [Sar02] als ein US Bundesgesetz, welches die Einhaltung von entsprechenden Sicherheitsmaßnahmen vorschreibt und die Verlässlichkeit der Berichterstattung von Unternehmen verbessern soll). Ziel eines IKS ist die betriebliche Steuerung und Überwachung, sodass die gesetzlichen Anforderungen erfüllt werden können (engl. „Compliance"), die Ausrichtung der IT-Zielsetzungen den Geschäftszielen entsprechen (engl. „Effectiveness") und die Wirksamkeit und Wirtschaftlichkeit der Prozesslandschaft verbessert wird (engl. „Effectiveness und Efficiency"). Dem Management sollen angemessene Information zur Verfügung gestellt werden (engl. „Reliability"), um das Unternehmen zu leiten und seine Treue- und Governance-Pflichten ausüben zu können. Integraler Bestandteil des IKS ist ein adäquates ISMS wie Vertraulichkeit, Integrität und Verfügbarkeit.

Betrachtet man nun ITIL im Kontext eines Kontrollsystems, so kann man zunächst Control Objectives for Information and related Technology (COBIT) heranziehen. Wie in Kapitel 3.3 erläutert, ist COBIT eine Sammlung an Best Practices, welche als Rahmenwerk für IT-Management verstanden wird. Es wurde 1992 erstmals von Information Systems Audit and Control Association (ISACA) und IT Governance Institute (ITGI) publiziert. Die aktuelle Version 4.2 ist unter [ITGI07] erhältlich. Entsprechend [Lach07] ist COBIT das international anerkannteste Rahmenwerk für IT-Governance und Kontrollen. Die Kompatibilität zwischen ITIL und COBIT kann sowohl in mehreren Publikationen von ISACA (siehe [ISACA10]) detailliert nachgelesen, als auch in der wissenschaftlichen Betrachtung durch [SaSh08] nachgewiesen werden. So wird festgestellt, wenn man ITIL mit COBIT bewertet (ein „benchmarking" durchführt) korrespondieren die beiden Standards sehr gut miteinander, vor allem wenn die Prozesse von COBIT auf ITIL basieren, wie das in der aktuellen Version von COBIT der Fall ist. Die Autoren verbinden die beiden Standards gemäß der folgenden Tabelle.

| ITIL | COBIT |
|---|---|
| Konzepte und Prozesse | Kritische Erfolgsfaktoren (CSF) |
| Aktivitäten | Metriken (CSF,KPI) |
| Kosten/ Nutzen | Benchmarking (CMM) |
| Planung für Implementierung | - |
| - | Audit |

**Tabelle 8: Verbindung zwischen ITIL und COBIT [SaSh08]**

ITIL kann man als die operative Basis verstehen, auf die COBIT als zusätzliche kontrollierende und steuernde Ebene aufgesetzt werden kann. Die Vorzüge von COBIT liegen in der Darlegung eines konkreten Vorgehensmodells für Audits, indem zu messende Metriken definiert werden.

Audits identifizieren somit Sicherheitsschwächen, denen man entsprechend entgegenwirken muss. Als proaktive Sicherheitsmaßnahme führt das Wissen um regelmäßige oder Ad-hoc-Audits dazu, dass Mitarbeiter definierte Prozesse und Kompetenzen einhalten.

# 6 Analyse der Sicherheitsgrundsätzen in Service Operation Prozessen

Die im vorigen Abschnitt im ITIL Rahmenwerk identifizierten allgemeinen Sicherheitsprinzipien gegen Angriffe eines Social Engineers werden im folgenden Abschnitt strukturiert und kategorisiert. Als Rahmen für die Strukturierung wird der Verlauf eines Security Incidents gemäß [CaOv99] herangezogen. Ein Angreifer nützt eine Gefahr für einen Angriff aus, wobei die Gefahr dem Servicebetreiber bekannt oder unbekannt sein kann. Der Incident ist der eigentliche Angriff, welcher Schaden verursacht, der vom Servicebetreiber abschließend behoben wird. Daraus ergibt sich der Ablauf: Gefahr – Incident (Angriff) – Schaden – Recovery (Wiederherstellung).

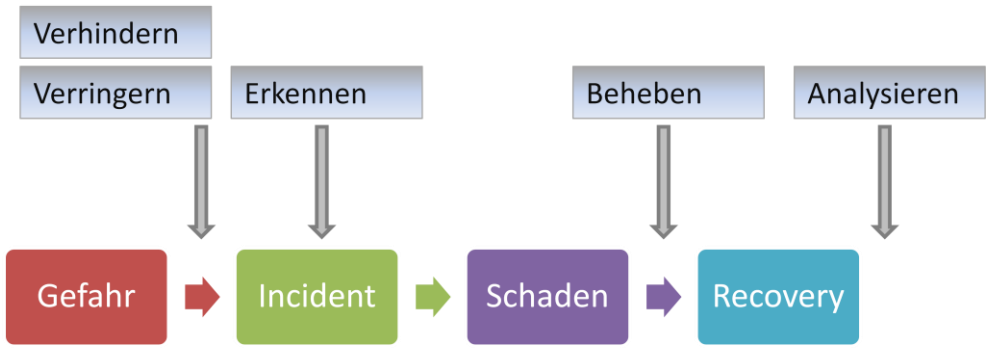



**Abbildung 62: Ablauf von Security Incidents [CaOv99]**

Risiken können entsprechend der beiden Normen ISO/ IEC 27001 und ISO/ IEC 27002 auf folgende Arten behandelt werden: Risikovermeidung (engl. „Avoid Risk“), Risikominimierung und Risikobegrenzung (engl. „Reduce Risk“), Risikoüberwälzung (engl. „Transfer Risk“) und Risikoakzeptanz (engl. „Accept Risk“). Risikovermeidung beinhaltet Maßnahmen und Vorgehen, wodurch Risiken vollständig vermieden werden, indem beispielsweise risikobehaftete Services nicht weiter angeboten werden. Zusätzliche Sicherheitsmaßnahmen, ausfallssichere Architekturen sowie regelmäßige Datensicherungen können unter anderem zur

Risikominimierung und -abgrenzung führen. Das Gefahrenszenario tritt somit mit einer geringeren Wahrscheinlichkeit und verminderten Schadenpotential auf. Unter Risikoüberwälzung versteht man zum Beispiel die vollständige Auslagerung von risikobehafteten Services an Dritte unter entsprechenden vertraglichen Bedingungen, wodurch das Risiko weitergegeben wird. Selbst bei der Risikominimierung kann man das so genannte Restrisiko nie ausschließen. Risikoakzeptanz behandelt verbliebenes Restrisiko, also jenes Risiko, das man entweder nicht verhindern kann oder will.

In Abbildung 62 spiegelt sich das Risikomanagement durch Verhinderung und Verminderung von Gefahren (Risikovermeidung und Risikoverminderung) wider sowie durch Angriffserkennung und Schadensbehebung (Risikobegrenzung). Im Sinne eines kontinuierlichen Verbesserungsprozesses wird die Behandlung von Security Incidents stets analysiert, um weitere Verbesserungsmaßnahmen zu identifizieren.

Um die identifizierten Sicherheitsprinzipien im ITIL Rahmenwerk gegen Social Engineering Attacken zu strukturieren, werden sie in Maßnahmen welche „Human- based Social Engineering Angriffe erschweren“, „Human-based Social Engineering Angriffe erkennen“, „Human- based Social Engineering Angriffe beheben“ und „Human- based Social Engineering Angriffe analysieren“ eingeordnet.

In Zuge der Strukturierung der auf ITIL basierenden Sicherheitsmaßnahmen gegen Angriffe eines Social Engineers werden diese in Anlehnung am „Social Engineering Model of Protection“ von [Mann08] kategorisiert. Die folgende Abbildung stellt das Sicherheitsmodell dar.

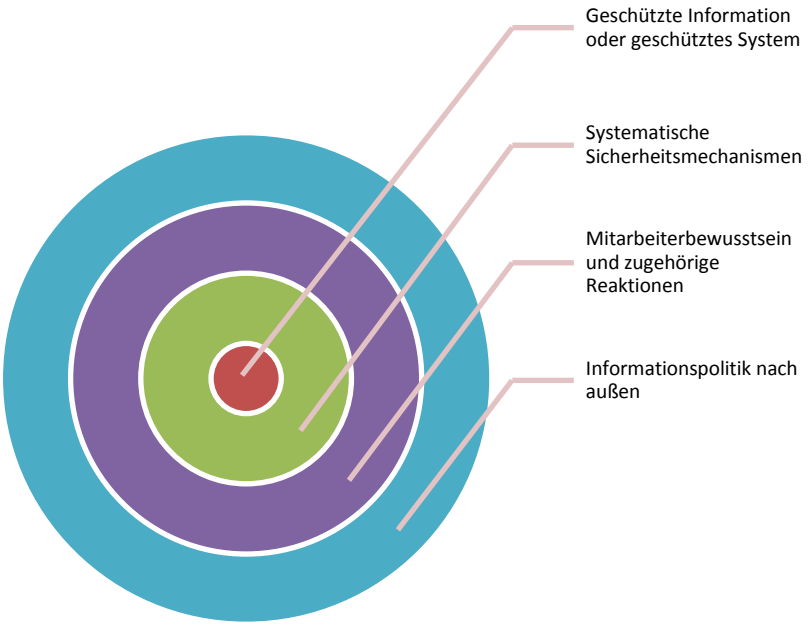



**Abbildung 63: Social Engineering Model of Protection [Mann08]**

Das Social Engineering Model of Protection besteht aus drei „Verteidigungsringen“ um die schützenswerte Information, welche das Ziel des Social Engineers darstellt. Ein Angreifer muss sämtliche Schichten überwinden, um Zugang zu den Informationen zu erlangen. Die äußerste Verteidigungsschicht spiegelt die Informationspolitik nach außen wider. Vergleicht man das in Kapitel 4.5 dargestellte Social Engineering Vertrauens- und Angriffsmodell, so soll die Informationspolitik nach außen die Recherchetätigkeit eines Social Engineers unmöglich machen oder zumindest wesentlich erschweren. Dadurch können Angriffe generell verhindert oder aufgrund einer schlechteren Vorbereitungsbasis leichter entdeckt werden.

Wie beispielsweise in [Unbe01] und [Kee08] sind bewusstseinsbildende Maßnahmen der Mitarbeiter gegen Human- based Social Engineering eine gängige Sicherheitsmaßnahme. Sie entspricht einer innenliegenden Schicht im Social Engineering Model of Protection. Schulungsprogramme für Mitarbeiter sollen die Gefahren vor Attacken eines Social Engineers aufzeigen und ein Bewusstsein zur Einhaltung von Sicherheitsrichtlinien schaffen.

[Mann08] versteht unter die von ihm genannten systematischen Sicherheitsmaßnahmen einerseits physische Maßnahmen als auch rein auf Technik basierende Maßnahmen gegen Social Engineering Attacken.

Beispielsweise würde ein Spamfilter darunter fallen, der den Empfang von verdächtigen Mails blockiert. In dieser Arbeit wird das Modell von [Mann08] verfeinert. Hierzu wird in das Modell das in späterer Folge vorgestellte Modell von [KiBe06] (siehe Kapitel 7.1) integriert, wodurch sich das in Abbildung 64 dargestellte erweiterte Social Engineering Sicherheitsmodell ergibt.

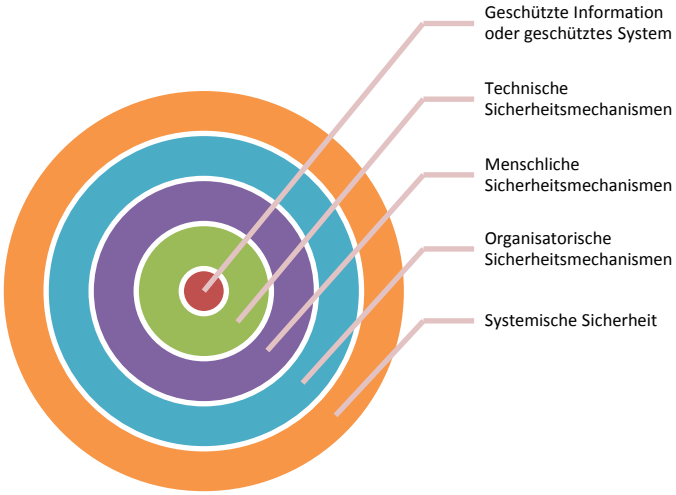



**Abbildung 64: Erweitertes Social Engineering Sicherheitsmodell von [Mann08]**

Hierbei entspricht die systematische Sicherheitsschicht von [Mann08] der Schicht der technischen Sicherheitsmaßnahmen. Physische und technische Sicherheitsmaßnahmen werden in technische Sicherheitsmaßnahmen subsummiert. Maßnahmen zur Etablierung eines Mitarbeiterbewusstseins werden menschlichen Sicherheitsmaßnahmen zugeordnet. Informationspolitik nach außen ist Bestandteil organisatorischer Sicherheitsmaßnahmen. Systemische Sicherheitsmaßnahmen werden aber analog zu [KiBe06] als Kombination von Mensch, Technologie und Organisation in einem prozessorientierten Umfeld verstanden, welche als System betrachtet werden. Charakteristisch für systemische Sicherheit ist auch ihre Einflussnahme auf die Umwelt des Unternehmens, wie etwa auf Lieferanten, Kunden oder andere Unternehmen. Unter "systematisch" wird in der Arbeit die Sichtweise auf ein bestimmtes (technisches) System oder eine nach einem System folgende Vorgehensweise verstanden. Eine "systemische" Betrachtungsweise zeichnet sich hingegen durch ihr übergreifendes Zusammenwirken einzelner Komponenten im größeren

Kontext aus. Beispielsweise liegen die Ursachen für Probleme hierbei nicht bei den Teilen, sondern im Zustand des Systems.

Im erweiterten Social Engineering Sicherheitsmodell sind in dem Verteidigungsring der menschlichen Maßnahmen nur jene enthalten, die als isoliert von den anderen Schichten zu betrachten sind. Dies gilt analog für die technische und für die organisatorische Schicht. Eine Maßnahme hingegen, die in Wechselwirkung zu mindestens einer aus einem anderen Verteidigungsring steht, wird entsprechend der systemischen Sichtweise in der Ebene der systemischen Maßnahmen eingeordnet.

Die visuelle Darstellung der systemischen Sicherheit kann man wie in Abbildung 65 als eine zusätzliche, neue Schicht verstehen, oder aber wie in der folgenden Abbildung als eine Verstärkung der bestehenden Verteidigungsringen – menschliche, technische und organisatorische Sicherheitsmaßnahmen.

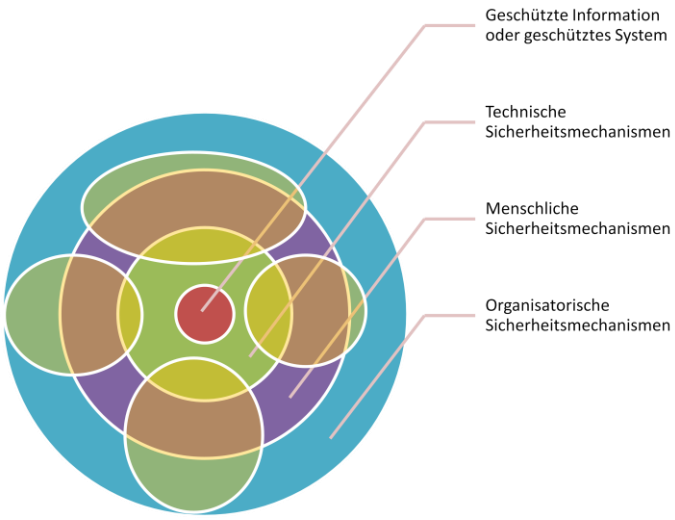



**Abbildung 65: Erweitertes Social Engineering Sicherheitsmodell von [Mann08] (Systemische Sicherheit als Stärkung bestehender Sicherheitsmaßnahmen)**

## 6.1 Social Engineering Angriffe erschweren

Social Engineering Attacken eines Hackers können erschwert werden, indem einer oder mehrere Durchführungsschritte des Angriffs (vergleiche hierzu Kapitel 4.4 und Kapitel 4.5) durch entsprechende Gegenmaßnahmen

gestört werden. Dies führt entweder dazu, dass der Social Engineer signifikant mehr Aufwand investieren muss, weitaus mehr Vermögen einbringen muss oder dass bestimmte Angriffstechniken gänzlich unmöglich werden.

Wenn gemäß dem ITIL Best Practice Rahmenwerk beispielsweise eine Zuständigkeitsmatrix (Maßnahme M20, Kapitel 6.5) definiert wird, deren Einhaltung fest in der Prozesslandschaft verankert ist, erschwert dies einem Social Engineer, einen Mitarbeiter zu unbefugten Tätigkeiten zu überreden. Klare Vorgaben zur Abarbeitung von mehreren Tickets (Maßnahme M08, Kapitel 6.5) verringern die Erfolgschance durch die Ausnutzung des menschlichen Faktors der Knappheit, wie in Kapitel 4.3.6 dargestellt, einen Mitarbeiter unter Druck zu setzen.

Die im ITIL Best Practice Rahmenwerk enthaltenen Sicherheitsmaßnahmen zum Erschweren von Human- based Social Engineering Angriffen werden in der Maßnahmenmatrix in Kapitel 6.5 zusammengefasst.

## 6.2 Social Engineering Angriffe erkennen

Maßnahmen, welche die Chance erhöhen, dass Social Engineering Angriffe als solche erkannt werden, führen dazu, dass das Eintreten von Schaden verhindert wird – insofern der Angriff rechtzeitig entdeckt wurde – und erhöhen das Risiko signifikant, das der Angreifer eingeht.

Beispiele hierfür findet man im ITIL Best Practice Rahmenwerk etwa in der Etablierung eines Service Desks als Single Point of Contact (Maßnahme M01, Kapitel 6.5). Durch diese Maßnahme kann das Personal gezielt, effizient und effektiv geschult werden, Social Engineering Angriffe zu erkennen. Das Bereitstellen von relevanten CMDB Informationen im Ticket Tool (Maßnahme M17, Kapitel 6.5) gibt dem Benutzer eine zusätzliche Hilfestellung, fehlerhafte Angaben des Social Engineers zu entlarven. Für die gesamte Liste an ITIL basierten Maßnahmen zur Human- based Social Engineering Angriffserkennung wird auf Kapitel 6.5 verwiesen.

## 6.3 Security Engineering Angriffe beheben

Wurde ein Angriff eines Social Engineers als solcher erkannt, muss auch geeignet darauf reagiert werden. In ITIL wird entweder ein bestehendes Incident Ticket als Security Incident markiert, oder ein neues Security Incident Ticket im Ticket Tool erfasst.

Eine strukturierte prozessorientierte Behandlung von Security Incidents (Maßnahme M11, Kapitel 6.5) soll sicherstellen, dass Angriffen schnell und effektiv entgegengewirkt wird. Priorität liegt in der weiteren Schadensvermeidung. Die eigentliche Ursachenanalyse ist ein nachgelagerter Prozess im Problem Management. Für die gesamte Liste an ITIL basierten Maßnahmen zur Human- based Social Engineering Angriffsbehebung wird auf Kapitel 6.5 verwiesen.

## 6.4 Social Engineering Angriffe analysieren

Die Möglichkeit, einen Angriff eines Social Engineers im Nachhinein analysieren zu können, ist aus mehreren Gesichtspunkten relevant. Zum einen stellt es eine wichtige Voraussetzung für das Qualitätsmanagement dar. Aus Fehlern will man lernen, aber dazu muss man Fehler genau analysieren können. Zum anderen ist es aus sicherheitstechnischer Sicht ausgesprochen wichtig, die Schäden eines Angriffs genau eingrenzen zu können. Welche Informationen hat der Social Engineer unrechtmäßig erworben, welche Systeme sind korrumpiert worden und welche gefälschten Identitäten hat er angenommen? Auch ist zu beachten, dass die Möglichkeit, Human- based Social Engineering Angriffe analysieren zu können, für die Beweispflicht innerhalb eines etwaigen gerichtlichen Verfahrens essentiell ist.

Das im ITIL Best Practice Rahmenwerk verpflichtende Erfassen von allen Incidents, Service Requests und Requests for Change und das Dokumentieren der gesetzten Aktivitäten im Ticket Tool (Maßnahmen M04 und M05, Kapitel 6.5) führen dazu, dass zu jedem späteren Zeitpunkt die Aktivitäten der Akteure nachvollzogen werden können. In Kapitel 6.5. werden alle ITIL basierten Maßnahmen zur Analyse von Human- based Social Engineering Attacken zusammengefasst.

## 6.5 ITIL basierte Maßnahmenmatrix gegen Social Engineering Attacken

In der folgenden Tabelle werden die ITIL basierten Maßnahmenempfehlungen gegen Human- based Social Engineering Attacken, wie sie in Kapitel 5 erläutert wurden, zusammengefasst. Die Maßnahmen werden eindeutig gekennzeichnet durch „M“ und einer fortlaufenden Nummer. Jeder Empfehlung wird nach ihrer primären

Wirkungsweise strukturiert und entsprechend den Schichten des erweiterten Social Engineering Sicherheitsmodells nach Wirkungsbereichen kategorisiert.

| # | Maßnahme | Erschweren | Erkennen | Beheben | Analysieren | Technisch | Menschlich | Organisatorisch | Systemisch |
|---|---|---|---|---|---|---|---|---|---|
| **M01** | Service Desk als Choke Point | X | X | | | | | | X |
| **M02** | Caller geeignet authentifizieren | X | | | | | | | X |
| **M03** | Toolunterstützung bei der Authentifikation von Caller und Bereitstellen von zusätzlichen Caller Informationen | | X | | | | | | X |
| **M04** | Alle Incidents, Service Requests und Requests for Change umgehend als Ticket erfassen | | X | | X | | | | X |
| **M05** | Alle Maßnahmen im Ticket erfassen | | X | | X | | | | X |
| **M06** | Tickets geeignet klassifizieren und priorisieren | | X | | | | | | X |
| **M07** | Strukturierte prozessorientierte Behandlung von Tickets | X | | | | | | | X |
| **M08** | Strukturierte Abarbeitung von mehreren Tickets | X | | | | | | | X |
| **M09** | Strukturierte prozessorientierte Behandlung von Major Incidents | X | | | | | | | X |
| **M10** | Kennzeichnung von Security Incidents | | | | X | | | | X |
| **M11** | Strukturierte prozessorientierte Behandlung von Security Incidents | | | X | | | | | X |
| **M12** | Ursachenanalyse von Security Incidents im Problem Management zur Aktualisierung der SKMS und | | | | X | | | | X |

| | | | | | |
|---|---|---|---|---|---|
| | RfC zur Ursachenbehebung | | | | |
| **M13** | Überwachung des Prozesses durch Prozessverantwortliche (z.B.: durch den Incident Manager) | | X | | X |
| **M14** | Strukturierte Übergabe von Tickets zwischen Akteuren (Schnittstellen) | X | | | X |
| **M15** | SKMS als zentraler Wissensdatenpool | X | | | X |
| **M16** | CMDB als zentraler Informationsdatenpool (insbesondere Dokumentation der SLAs, Services, Prozesse und Verantwortlichkeiten, Rollen, Mitarbeiterverzeichnisse) | | X | | X |
| **M17** | Integration von CMDB in das Ticket Tool zur Unterstützung des Benutzers | | X | | X |
| **M18** | Integration von SKMS in das Ticket Tool zur Unterstützung des Benutzers | X | | | X |
| **M19** | Das Ticket Tool als zentrale Informationsquelle, Verwaltung und Verteilung von Information durch das Tool | X | X | X | X |
| **M20** | Zuständigkeitsmatrix zur Bearbeitung von Tickets | X | | | X |
| **M21** | Principle of least Privilege zwischen den verschiedenen Support Levels und Funktionseinheiten des Unternehmens | X | | | X |
| **M22** | Funktionstrennung im Sinne einer gestaffelten Abwehr (auch bei Major Incidents) auf Prozessebene | X | X | | X |
| **M23** | Funktionstrennung im Sinne der gestaffelten Abwehr (auch bei Major Incidents) auf Organisationsebene (z.B.: Service Operations zu Service Design) | X | X | | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **M24** | Definition von Standard-Changes und toolunterstützte Behandlung | X | | | | | | X |
| **M25** | Toolunterstützung soll Arbeit erleichtern und vereinfachen | X | X | X | | | | X |
| **M26** | Toolunterstützung soll für Benutzer Mehrwert haben | X | X | X | | | | X |
| **M27** | Definition und Toolunterstützung von Incident Modellen, insbesondere von Security Incidents | X | X | X | | | | X |
| **M28** | Transparenz durch prozessorientierte Behandlung von Tickets (insbesondere bei Standard- Changes) | X | | X | | | | X |
| **M29** | Automatisierung von Teilschritten innerhalb der Prozesskette durch das Ticket Tool (zum Beispiel: automatischer Mailversand an Caller zur Bestätigung, Selbsthilfe) | X | | | | | | X |
| **M30** | Information Security Policy nach ISO/ IEC 27001 | X | X | | | | | X |
| **M31** | Organisation der Informationssicherheit nach ISO/ IEC 27001 | X | X | | | | | X |
| **M32** | Management von organisationseigenen Werten nach ISO/ IEC 27001 eingebettet in ITIL Prozesslandschaft | X | X | | | | X | X |
| **M33** | Personelle Sicherheit nach ISO/ IEC 27001 | X | X | | | X | | |
| **M34** | Physische und umgebungsbezogene Sicherheit nach ISO/ IEC 27001 | X | | | X | | | |
| **M35** | Betriebs- und Kommunikationsmanagement nach ISO/ IEC 27001 eingebettet in ITIL Prozesslandschaft | X | X | | | | | X |
| **M36** | Zugangskontrolle nach ISO/ IEC 27001 | X | | | X | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **M37** | Beschaffung, Entwicklung und Wartung von Informationssystemen nach ISO/ IEC 27001 | X | | | X | |
| **M38** | Umgang mit Informations-sicherheitsvorfällen nach ISO/ IEC 27001 eingebettet in ITIL Prozesslandschaft | | X | | | X |
| **M39** | Business Continuity Management nach ISO/ IEC 27001 eingebettet in ITIL Prozesslandschaft | X | | | | X |
| **M40** | Compliance nach ISO/ IEC 27001 | X | X | X | | X |
| **M41** | Etablierung von Überwachungsprozessen zur Einhaltung der Sicherheitsgrundsätze | X | X | X | | X |
| **M42** | Etablierung eines kontinuierlichen Verbesserungsprozesses | | | X | | X |
| **M43** | Kontinuierliches Prüfen und Kontrolle der Anforderungserfüllung (IKS) | | | X | | X |
| **M44** | (externe) Kontrolle durch Audits | | | X | | X |

**Tabelle 9: Maßnahmenkatalog gegen Social Engineering**

### *6.5.1 Wirkungsweise*

Einige Maßnahmen haben mehr als eine primäre Wirkungsweise. Sowohl dass alle Incidents, Service Requests und Requests for Change umgehend als Ticket erfasst werden müssen (Maßnahme M04), als auch dass alle Aktivitäten im Ticket erfasst werden müssen (Maßnahme M05), dienen gleichermaßen der Analyse von Attacken eines Social Engineers sowie der Schaffung der Möglichkeit, einen laufenden Angriff zu erkennen.

Die Ticket Toolunterstützung (Maßnahme M19), das Sicherstellen der Nutzung des Ticket Tools (Maßnahme M26, M27 und M28) und die Etablierung von Überwachungsprozessen zur Einhaltung der Sicherheitsgrundsätze (Maßnahme M41) bilden das Fundament für alle Wirkungszwecke. Die Maßnahme Compliance von ISO/ IEC 27001

(Maßnahme M40) kann die Notwendigkeit und Prüfung der Einhaltung von weiteren Sicherheitsregelungen und -standards definieren, weshalb der Wirkungszweck nicht nur auf Analysieren, sondern auch auf Erschweren und Erkennen erweitert wird.

Funktionstrennung im Sinne einer gestaffelten Abwehr (Maßnahme M22 und M23), Information Security Policy (Maßnahme M30), Organisation der Informationssicherheit (Maßnahme M31), Management von organisationseigenen Werten (Maßnahme M32), Personelle Sicherheit (Maßnahme M33) und Betriebs- und Kommunikationsmanagement (Maßnahme M35) sind primär Maßnahmen zum Erschweren und Entdecken von Angriffen.

### *6.5.2 Wirkungsbereich*

Betrachtet man die Kategorisierung der Maßnahmen entsprechend der Schichten des Social Engineering Sicherheitsmodells so ist auffallend, dass alle Maßnahmen primär im systemischen Wirkungsbereich einzuordnen sind. Dies resultiert schlichtweg aus der systemischen Sicht des ITIL Best Practice Rahmenwerks selbst. Inhärenter Bestandteil von ITIL ist die prozessorientierte Kombination und Wechselwirkung zwischen Mensch – Technologie – Organisation, um ein IT Service Management aufzubauen, aufrechtzuerhalten und kontinuierlich zu verbessern. Technische Sicherheitsmechanismen sind nicht direkter Bestandteil des ITIL Best Practice Rahmenwerks, werden aber in ISO/ IEC 27001 in Zugangskontrolle (Maßnahme M36) und Beschaffung, Entwicklung und Wartung von Informationssystemen (Maßnahme M37) adressiert. Physische und umgebungsbezogene Sicherheit (Maßnahme M34) wird entsprechend der Definition des Modells ebenfalls als technische Maßnahme eingeordnet.

Personelle Sicherheit entsprechend ISO /IEC 27001 (Maßnahme M33) liegt als einzige Maßnahme primär in der Schicht der menschlichen Sicherheitsmechanismen.

Im organisatorischen Bereich ist als einzige Maßnahme das Management von organisationseigenen Werten (Maßnahme M32) zugeordnet.


**Abbildung 66: Überblick der Kategorisierung der auf ITIL basierten Sicherheitsmaßnahmen gegen Human- based Social Engineering Attacken**

Die Abbildung 66 verdeutlicht die Kategorisierung der Wirkungsbereiche der auf ITIL basierenden Sicherheitsmaßnahmen gegen Human- based Social Engineering Attacken basierend auf dem erweiterten Sicherheitsmodell.

### *6.5.3 Wirkungsvektor*

Will man die Sicherheit verschiedener Services vereinfacht visualisieren, so kann man die folgende Darstellung in Abbildung 67 wählen. Hierbei werden die drei Services – Service A, Service B, Service C – unter dem Aspekt menschliche, technischer und organisatorische Sicherheit bewertet. Service A hat sowohl eine schwache technische, menschliche als auch organisatorische Sicherheit. Service B hat eine mittelmäßige menschliche Sicherheit, aber sowohl eine hohe technische als auch eine hohe organisatorische Sicherheit. Service C verfügt über hohe Sicherheit in allen drei Bereichen.

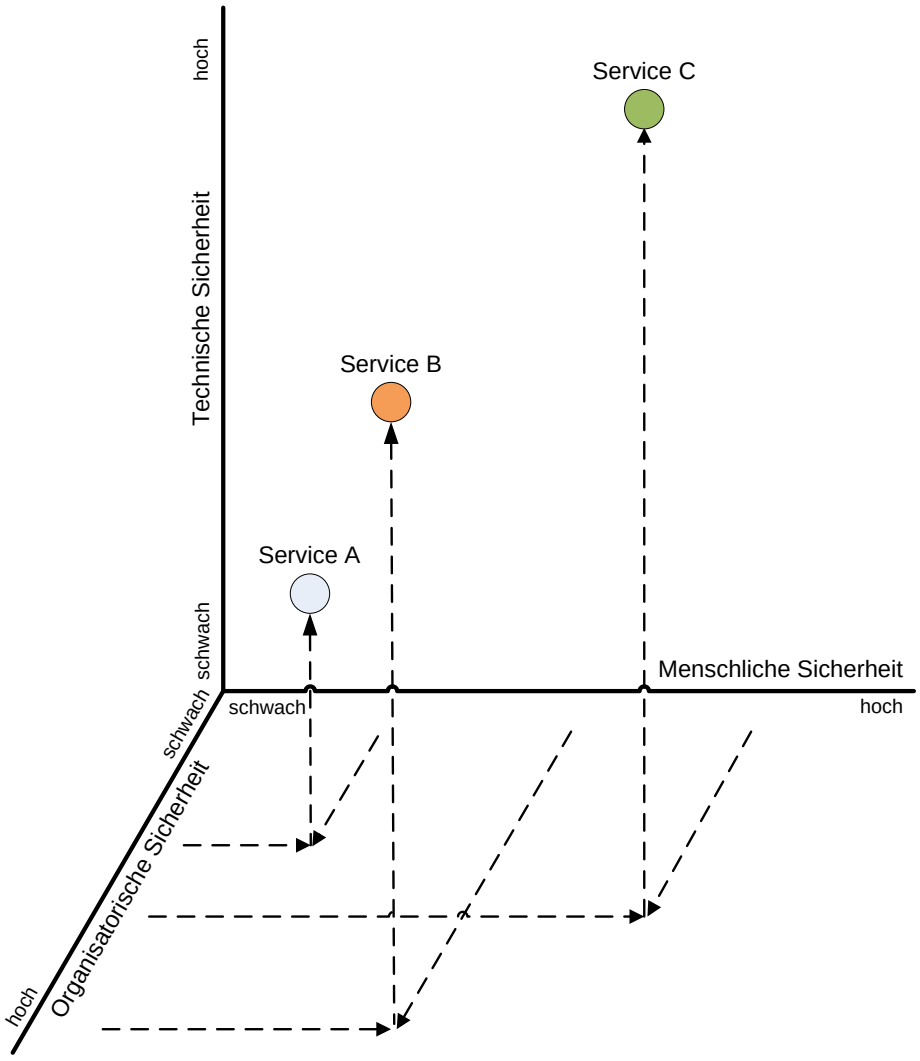



**Abbildung 67: Sicherheit von Services (vereinfachte Darstellung)**

Durch den bewussten Einsatz von ITIL als Sicherheitskonzept in Service Operation Prozessen gegen Human- based Social Engineering Attacken wird eine Verschiebung zu mehr Sicherheit in allen drei Achsen erreicht.

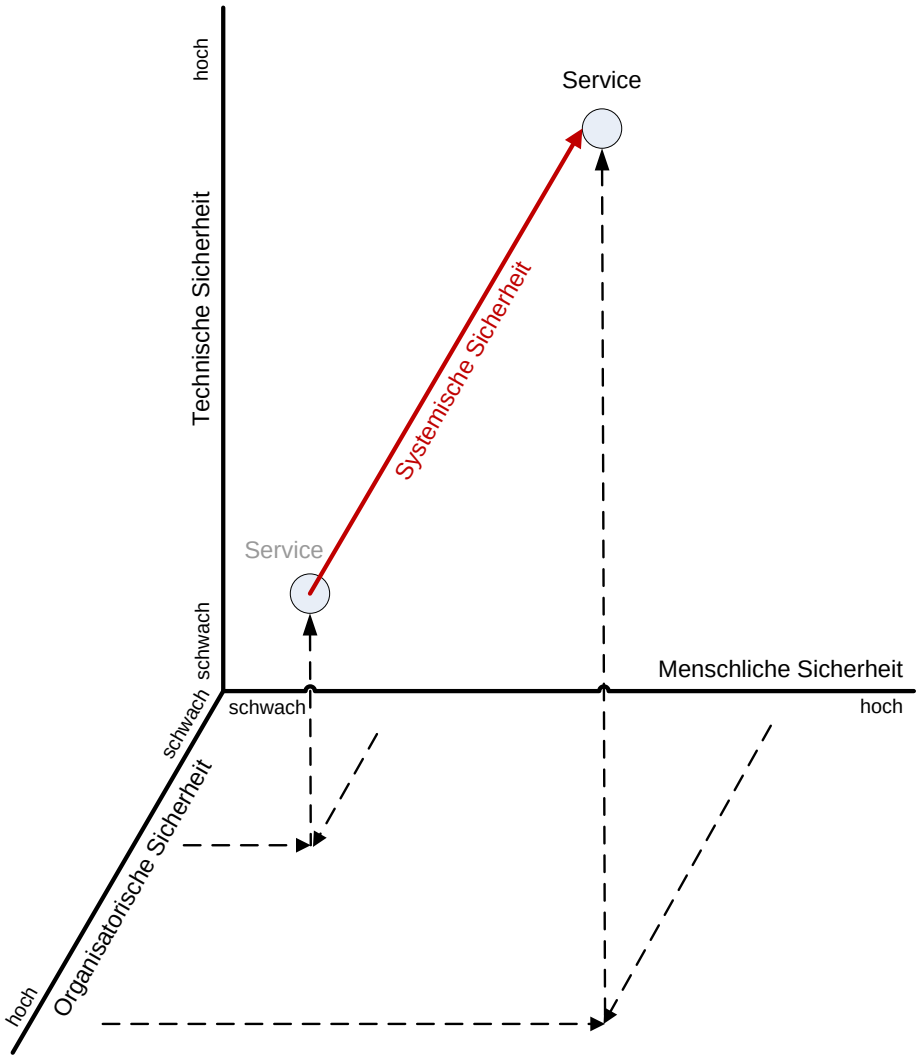



**Abbildung 68: Einfluss von ITIL auf die Sicherheit von Services**

Die systemische Sicherheit ergibt sich aus der prozessorientierten Kombination aus technischer, menschlicher und organisatorischer Sicherheit. Die Länge der Verschiebung zu mehr Sicherheit ist nicht fest vorgegeben, sondern hängt von variablen Faktoren wie beispielsweise dem Service selbst ab. Ein Service, welches operativ nur geringfügige menschliche Eingriffe benötigt, mag eine geringere Verschiebungslänge aufweisen als ein Service mit einer operativ stetigen menschlichen Interaktion. Natürlich ist die Länge der Verschiebung abhängig vom aktuellen Sicherheitsstand des Services. Es wurde daher bewusst die Begrifflichkeit des Wirkungsvektors gewählt, welcher die Verschiebung beschreibt, die Länge aber nicht festlegt.

### 6.5.4 Wirkungssteuerung und -kontrolle

Nachdem die Wirkungsweise, der Wirkungsbereich und der Wirkungsvektor von auf ITIL basierenden Sicherheitsmaßnahmen gegen Social Engineering analysiert wurden, muss die Frage behandelt werden, wie die Wirkung gesteuert und kontrolliert wird. Essentiell hierfür ist die Fragestellung, ob ein Unternehmen, das den Betrieb unter Berücksichtigung des ITIL Rahmenwerks organisiert hat, vielleicht sogar dementsprechend zertifiziert ist, automatisch vor Social Engineering Attacken geschützt ist. Die Frage kann klar verneint werden. Bezugnehmend auf Abbildung 66 ist ersichtlich, dass in ITIL die steuernde Kraft Service Level Agreements sind. Die Serviceerbringung wird also nach den Anforderungen und Wünschen des Kunden ausgerichtet, welche mit ihm abgestimmt und überwacht wurden.

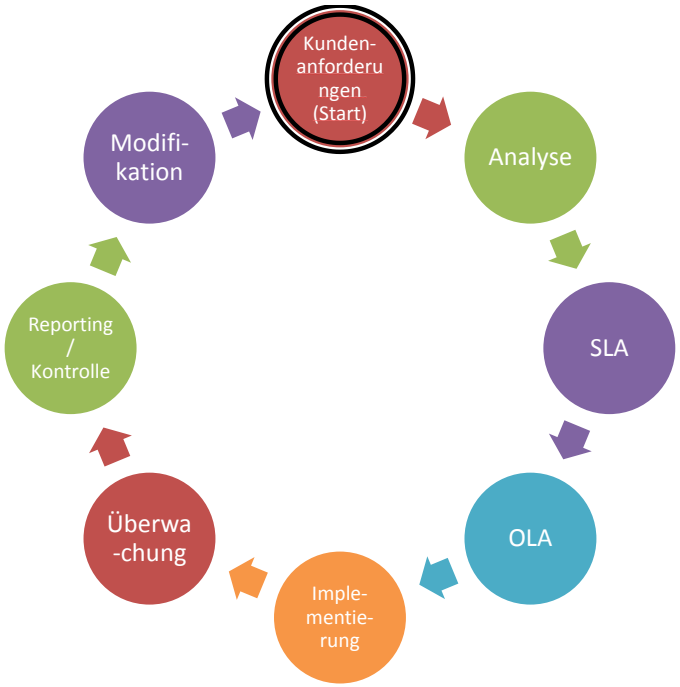



**Abbildung 69: Information Security Prozess, basierend auf [OGC07D]**

Betrachtet man den Information Security Prozess in einer etwas anderen Darstellung als Abbildung 69, so leiten sich die folgenden Schritte zur Steuerung und Kontrolle ab:

Eine Risikoanalyse und das Identifizieren der Kundenanforderungen stellen den Prozessbeginn dar. Darauf basierend bewertet die Organisation die

Umsetzbarkeit der Anforderungen auch unter Berücksichtigung firmeninterner Richtlinien für Informationssicherheit.

Zwischen den Kunden und dem Dienstleister wird ein Service Level Agreement geschlossen, welche die Sicherheitsanforderungen der Informationen spezifizieren, sowie die Messbarkeit und Nachweisbarkeit der Einhaltung definieren.

Operational Level Agreements (OLAs) können als unternehmensinterne SLAs verstanden werden. So werden beispielsweise Verfügbarkeitsanforderungen von Services zwischen den einzelnen Organisationseinheiten klar festgelegt.

Nach der Implementierung wird die Einhaltung der SLAs und OLAs überwacht und in Form von Reports ausgewertet und kontrolliert.

Die Messung über die Effektivität und den Status des Services bezüglich Information Security kann eine Anpassung sowohl der SLAs und OLAs als auch der Maßnahmen bedingen, wodurch der Kreislauf im Sinne eines kontinuierlichen Verbesserungsprozesses geschlossen ist. Auch können veränderte oder neue Kundenanforderungen einen neuerlichen Zyklusdurchlauf bedingen.

Wenn somit der Schutz vor Attacken eines Social Engineers kein definiertes Qualitätsziel ist, so wird beispielsweise der Incident Manager seine Prozesse nicht dementsprechend gestalten, Mitarbeiter werden nicht entsprechend geschult, die CMDB wird nicht entsprechend in das Ticket Tool integriert uvm. Der Betrieb widerspricht damit nicht automatisch den Vorgaben und Empfehlungen von ITIL. Auch das Information Security Management könnte die Gefahr vor Social Engineering Attacken als kundenseitig akzeptiertes Risiko einstufen. Selbstverständlich können unternehmensinterne Richtlinien zur Informationssicherheit die kundenseitigen übersteigen, wodurch trotz gegenteiliger Kundenanforderung der Schutz vor Social Engineering ein definiertes Ziel ist.

Dies zeigt, dass ITIL als Methode zu verstehen ist, in gewisser Weise ein Werkzeug, das gegen Social Engineering Attacken eingesetzt werden kann, insofern man das Werkzeug auch dementsprechend gebrauchen möchte. Die Steuerung und Kontrolle entsprechend dem in ITIL fest verankerten Deming PDCA Zyklus setzt auf Service Level Agreements auf. Mit dem Kunden sind innerhalb des SLAs klar zu definierende Ziele sowie eine Überprüfbarkeit und Nachweisbarkeit der Einhaltung festzulegen. Hierzu

bietet sich beispielsweise der Erfüllungsgrad der vorgestellten Maßnahmen gegen Human- based Social Engineering an. Zusätzlich sollten Messungen berücksichtigt werden wie der Prozentanteil der vom Incident Manager kontrollierten Tickets, das Verhältnis zwischen Standard- Changes und wiederholenden Service Requests, der Prozentanteil an Tickets die nach einem SKMS Eintrag behoben wurden, die Anzahl der Anrufe und Mails, die den Service Desk als Single Point of Contact umgingen uvm. Ebenfalls sollte in SLAs die Modalität von Reports und Audits definiert werden.

Die folgende Tabelle zeigt beispielhafte Kontrollen und Steuerungen (engl. „Key Performance Indicators“ – KPIs) auf. Diese sollten im Service Level Agreement zwischen Kunden und Dienstleister eindeutig definiert werden.

| # | Maßnahme | Beispielhafte Kontrolle und Steuerung |
|---|---|---|
| **M01** | Service Desk als Choke Point | Anzahl der Anrufe und Mails, die den Service Desk als Single Point of Contact umgangen haben |
| **M02** | Caller geeignet authentifizieren | Anzahl nicht authentifizierter Caller<br><br>Prozentanteil der Caller nach unterschiedlichen Authentifikationsmethoden |
| **M03** | Toolunterstützung bei der Authentifikation von Caller und Bereitstellen von zusätzlichen Caller Informationen | Auswertung der Nützlichkeit der bereitgestellten zusätzlichen Caller Information durch direkte Mitarbeiterbewertung |
| **M04** | Alle Incidents, Service Requests und Requests for Change umgehend als Ticket erfassen | Anzahl nicht erfasster Tickets, zum Beispiel kontrolliert über Auswertung der Telefonanlage oder Mailboxen |
| **M05** | Alle Maßnahmen im Ticket erfassen | Anzahl der Tickets ohne Maßnahmenbeschreibung<br><br>Beurteilung der Nachvollziehbarkeit |
| **M06** | Tickets geeignet klassifizieren und priorisieren | Anzahl der Tickets ohne Klassifizierung / Priorität<br><br>Anzahl der Tickets mit falscher Kategorisierung / Priorität |
| **M07** | Strukturierte, prozessorientierte Behandlung von Tickets | Anzahl (kundenseitig und intern) eskalierter Tickets aufgrund von |

| | | |
|---|---|---|
| | | Lösungszeitüberschreitung, Ressourcenproblemen, Kompetenzdefiziten etc. |
| **M08** | Strukturierte Abarbeitung von mehreren Tickets | Anzahl (kundenseitig und intern) eskalierter Tickets aufgrund von Lösungszeitüberschreitung, Ressourcenproblemen, Kompetenzdefiziten etc. in besonderen Betrachtungsintervallen (z.B.: während Kernarbeitszeit, nach Releaseeinsätzen) |
| **M09** | Strukturierte prozessorientierte Behandlung von Major Incidents | Anzahl (kundenseitig und intern) eskalierter Major Incidents aufgrund von Lösungszeitüberschreitung, Ressourcenproblemen, Kompetenzdefiziten etc. |
| **M10** | Kennzeichnung von Security Incidents | Anzahl fehlerhaft gekennzeichneter Incidents |
| **M11** | Strukturierte, prozessorientierte Behandlung von Security Incidents | Anzahl von Security Incidents<br><br>Anzahl (kundenseitig und intern) eskalierter Security Incidents aufgrund von Lösungszeitüberschreitung, Ressourcenproblemen, Kompetenzdefiziten, … |
| **M12** | Ursachenanalyse von Security Incidents im Problem Management zur Aktualisierung der SKMS. Analyse der zugehörigen Maßnahmen zur Behebung (RfCs) | Anzahl nicht gefundener Ursachen und Lösungsvorschläge von Security Incidents<br><br>Ausreichender Detailgrad und Nachvollziehbarkeit der Ursachen- und Lösungsbeschreibung. Hierbei kann sollte auch der Kunde mit einbezogen werden. |
| **M13** | Überwachung des Prozesses durch den Prozessverantwortlichen (z.B.: durch den Incident Manager) | Anzahl an SLA Verletzungen aufgrund mangelnder Prozesse |
| **M14** | Strukturierte Übergabe von Tickets zwischen Akteuren (Schnittstellen) | Durchschnittliche und maximale Zeit bei Ticketübernahme von einer Person zur anderen<br><br>Anzahl falscher Zuweisungen von Tickets |

| | | |
|---|---|---|
| | | Anzahl der Tickets mit eskalierter Lösungszeitüberschreitung aufgrund nicht weiter behandelter Tickets |
| **M15** | SKMS als zentraler Wissensdatenpool | Anzahl an zusätzlichen Informationsquellen, die nicht in SKMS integriert sind<br><br>Anzahl an Service Requests aufgrund fehlender / nicht aktueller / falscher Informationen in SKMS<br><br>Lösungsrate im 1st Level / 2nd Level Support |
| **M16** | CMDB als zentraler Informationsdatenpool (insbesondere Dokumentation der SLAs, Services, Prozesse und Verantwortlichkeiten, Rollen, Mitarbeiterverzeichnisse) | Anzahl an zusätzlichen Informationsquellen, die nicht in CMDB integriert sind<br><br>Anzahl an Service Requests aufgrund fehlender / nicht aktueller / falscher Informationen in CMDB |
| **M17** | Integration von CMDB in das Ticket Tool zur Unterstützung des Benutzers | Direkte Bewertung des Nutzens durch Mitarbeiter |
| **M18** | Integration von SKMS in das Ticket Tool zur Unterstützung des Benutzers | Anteil Tickets mit Relation zu SKMS Eintrag<br><br>Direkte Bewertung des Nutzens durch Mitarbeiter<br><br>Anzahl gleichartiger Tickets mit unterschiedlichen (individuellen) Lösungswegen |
| **M19** | Das Ticket Tool als zentrale Informationsquelle, Verwaltung und Verteilung von Information durch das Tool | Anzahl an Anfragen, wo der Service Desk nicht den aktuellen Status geben konnte |
| **M20** | Zuständigkeitsmatrix zur Bearbeitung von Tickets | Anzahl falsch zugeordneter Tickets<br><br>Anzahl an Eskalationen zum Prozessmanager aufgrund unklarer Zuständigkeit |
| **M21** | Principle of least Privilege zwischen den verschiedenen Support Levels und | Anzahl der Verletzungen des Sicherheitsprinzips ermittelt durch (externes) Audit |

| | | |
|---|---|---|
| | Funktionseinheiten des Unternehmens | |
| **M22** | Funktionstrennung im Sinne einer gestaffelten Abwehr (auch bei Major Incidents) auf Prozessebene | Anzahl der Verletzungen des Sicherheitsprinzips ermittelt durch (externes) Audit |
| **M23** | Funktionstrennung im Sinne der gestaffelten Abwehr (auch bei Major Incidents) auf Organisationsebene (z.B.: Service Operations zu Service Design) | Anzahl der Verletzungen des Sicherheitsprinzips ermittelt durch (externes) Audit |
| **M24** | Definition von Standard-Changes und toolunterstützte Behandlung | Anzahl an gleichartigen Service Requests, die nicht als Standard-Change hinterlegt sind |
| **M25** | Toolunterstützung soll Arbeit erleichtern und vereinfachen | Messbare Effizienzsteigerung durch Weiterentwicklung des Ticket Tools (z.B.: Anzahl bearbeiteter Tickets pro Mitarbeiter) |
| **M26** | Toolunterstützung soll für Benutzer Mehrwert haben | Direkte Zufriedenheitsbewertung durch Mitarbeiter |
| **M27** | Definition und Toolunterstützung von Incident Modellen, insbesondere von Security Incidents | Anzahl an Security Incidents, die nicht toolunterstützt als Incident Modell hinterlegt sind |
| **M28** | Transparenz durch prozessorientierte Behandlung von Tickets (insbesondere bei Standard- Changes) | Anzahl an gleichartigen Service Requests, die nicht als Standard-Change hinterlegt sind |
| **M29** | Automatisierung von Teilschritten innerhalb der Prozesskette durch das Ticket Tool (zum Beispiel: automatischer Mailversand an Caller zur Bestätigung, Selbsthilfe) | Anteil automatisierter Teilschritte<br><br>Bearbeitungszeit von Standard-Changes |
| **M30 bis M40** | Maßnahmen nach ISO / IEC 27001 | Kontrollen nach ISO / IEC 27002 |
| **M41** | Etablierung von Überwachungsprozessen zur Einhaltung der Sicherheitsgrundsätze | Anzahl an Verletzungen der Sicherheitsgrundsätze |
| **M42** | Etablierung eines kontinuierlichen | Verbesserungsgrad im Vergleich zur letzten Messung |

| | | |
|---|---|---|
| | Verbesserungsprozesses | |
| **M43** | Kontinuierliches Prüfen und Kontrolle der Anforderungserfüllung (IKS) | Anzahl an Anforderungsverletzungen |
| **M44** | (externe) Kontrolle durch Audits | Ergebnis der Audit Berichte<br><br>Anzahl und Grad identifizierter Maßnahmenempfehlungen |

**Tabelle 10: Beispielhafte Kontrollen und Steuerungen der Umsetzung des Maßnahmenkatalogs gegen Social Engineering**

# 7 Umfassendes Sicherheitskonzept gegen Social Engineering Attacken

*Am 11. Dezember 1998 startete die NASA Sonde Mars Climate Orbiter Richtung Mars. Nach fast einem Jahr erreichte die Sonde den Mars, wo sie in einen elliptischen Orbit eintrat. Als sie aus dem Funkschatten des Mars wieder austreten sollte, konnte allerdings kein Kontakt mehr hergestellt werden. Aufgrund eines Navigationsfehlers war die Sonde nicht wie geplant 150 km vom Mars entfernt, sondern näherte sich dem Planeten bis zu 57 km, wodurch Reibungskräfte und die Hitze die Sonde zerstörten.*

*Wie sich herausstellte, war die Ursache, dass die NASA Impulse im international gebräuchlichen SI-System mit der Einheit Newton mal Sekunde berechnete, die Navigationssoftware des Satelliten war hingegen vom Hersteller Lockheed Martin für das imperiale System der Impulseinheit Pound-force mal Sekunde ausgelegt.*

Dieses Beispiel verdeutlicht die Notwendigkeit einer stimmigen Gesamtlösung.

Die in Kapitel 5 identifizierten, auf ITIL basierten Sicherheitsmaßnahmen gegen Attacken eines Social Engineers wurden im vorigen Kapitel entsprechend Wirkungsweise und Wirkungsbereich kategorisiert. Anschließend wurden der Wirkungsvektor, die Wirkungssteuerung und -kontrolle beleuchtet.

In diesem Kapitel werden die auf ITIL basierten Sicherheitsmaßnahmen gegen Human- based Social Engineering Attacken in ein umfassendes Sicherheitskonzept eingebettet. Es wird gezeigt, dass diese Einbettung in moderne Informationssicherheitsmanagements harmonisch durchgeführt werden kann. Um die Praktikabilität zu verdeutlichen, werden Fallbeispiele aus der praktischen Umsetzung im Finanzbereich und bei rechtlich geregelten Wahlen erläutert. Abgeschlossen wird die Analyse durch eine Restrisikobestimmung, wobei Angriffsmöglichkeiten identifiziert werden, die durch ITIL nicht abgesichert sind. Zusätzlich wird die Möglichkeit analysiert, ob durch die Einführung von ITIL Prozessen in Unternehmen neue Social Engineering Angriffsvektoren entstehen.

## 7.1 ITIL als Teil eines Sicherheitskonzepts

Der klassische Ansatz des Informations-Sicherheitsmanagements besteht darin, Informationen in Sicherheitsstufen zu kategorisieren. Für jede Sicherheitsstufe werden minimale Standards und Maßnahmen definiert, die jede Person und jedes Objekt (Technologien, Prozesse), welche auf die Informationen zugreifen oder verarbeiten, erfüllen müssen. [CoE01]

Entwickelt haben sich die so genannten Multi- Level- Sicherheitssysteme in den 1970er-Jahren vorwiegend im militärischen Bereich. Typische Sicherheitsstufen hierbei waren „streng geheim“, „geheim“, „vertraulich“ und „öffentlich“. Sicherheitsmodelle, wie zum Beispiel das Bell LaPadula, Bipa oder Low Watermark Mandatory Access Control (LoMac), regelten die Einhaltung der Vertraulichkeit oder der Integrität. Beispielsweise erlaubt das Bell LaPadula Modells nicht, eine Informationen einer höheren Sicherheitsstufe zu lesen, gleichzeitig darf auch keine Informationen in eine niedrigere Sicherheitsstufe umgestuft werden.

In den 1990er-Jahren entwickelten sich mit dem Verbund- Modell und dem Chinese Wall- Modell so genannte Multiliterale Sicherheitsmodelle. Diese basieren auf Multi- Level- Sicherheitsmodellen, besitzen aber neben der horizontalen Einstufung in Sicherheitsstufen auch eine vertikale Einstufung, beispielsweise in Sachgebieten oder Suborganisationseinheiten. Um Zugriff auf eine bestimmte Information zu erlangen, muss man nicht nur Rechte in der entsprechenden Sicherheitsstufe, sondern auch Rechte auf das Sachgebiet haben.

In [Klai10] wird festgestellt, dass die Anforderungen, die beim traditionellen Ansatz von Informationssicherheit aufgestellt werden, einen statischen Charakter haben. Sie werden im Vorfeld relativ unabhängig vom eigentlichen Unternehmen erstellt und basieren vorwiegend auf den Sicherheitsstufen. Eine Information Security Policy wird bestimmt durch Erfahrung und Best Practices, wodurch Spezifika des Geschäftsumfeldes vernachlässigt werden. Aktuelle Entwicklungen der Informationssicherheit zeichnen sich durch ein multidimensionales Konzept aus, indem die einzelnen Domänen in Wechselwirkung zueinander stehen. Im Gegensatz zu traditionellen Sicherheitskonzepten werden weitere zusätzliche Faktoren berücksichtigt, wie beispielsweise die Unternehmenskultur. Als weiterer Trend in modernen Sicherheitskonzepten wird in [Klai10] die Behandlung der Subjektivität im Risikomanagement identifiziert.

Corporate Governance ist "*the ethic corporate behavior by directors or others charged with governance in the creation and presentation of wealth of all stakeholders*". [NaRo08] Information Technology Governance, IS Governance oder ICT Governance (Information and Communications Technology), sind Teilbereiche von Corporate Governance, welche sich auf IT Systeme, deren Performance und Risikomanagement fokussiert. [NaRo08] Eine Charakteristik von IT Governance ist, dass das Leistungsvermögen der IT nicht länger intransparent ist.

Governance ist eine Ansammlung von Verantwortlichkeiten und Verfahren, vom Management ausgeführt und gelebt mit dem Ziel, eine strategische Ausrichtung zum Erreichen von Unternehmenszielen zu etablieren, einen adäquaten Umgang mit Risiken zu schaffen und die Ressourcen des Unternehmens entsprechend einzusetzen. Dies wird in Abbildung 70 basierend auf [Klai10] dargestellt.

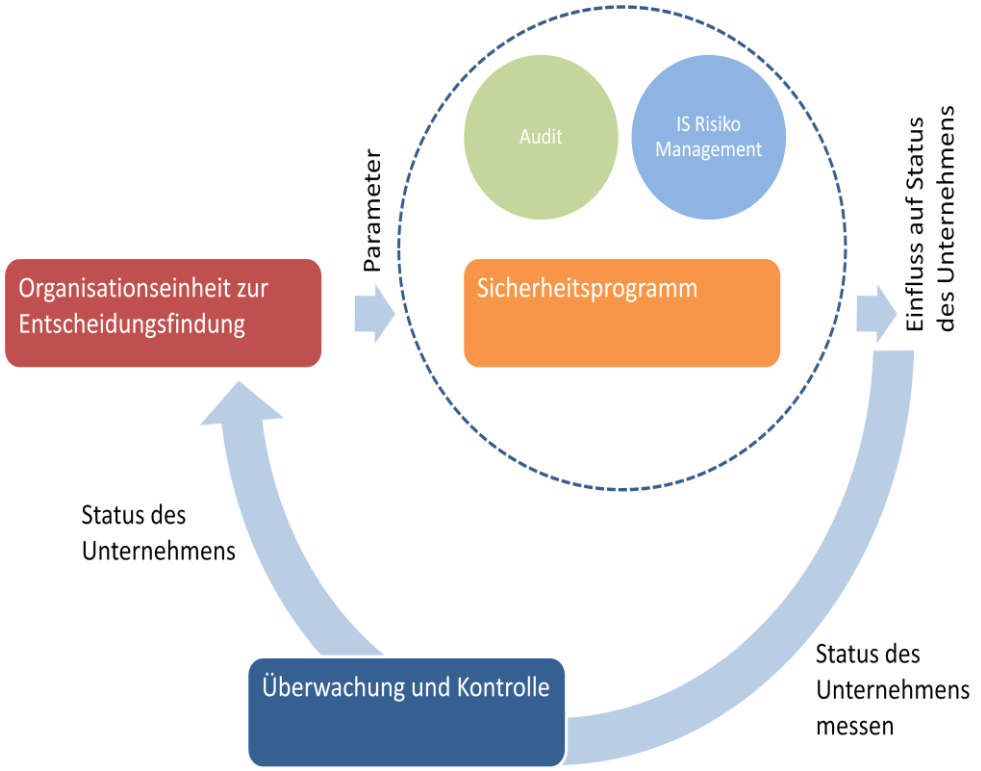



**Abbildung 70: Information Security Governance [Klai10]**

IS Governance richtet somit das Information Sicherheitsmanagement entsprechend der Unternehmensziele und -strategie aus. Im Gegensatz zu traditionellen Ansätzen von Sicherheitsmodellen ist die Informationssicherheit inhärenter Bestandteil der Unternehmensziele und -strategie, welcher durch das Management festgelegt und gesteuert wird.

Betrachtet man vorerst das Cobit Modell, welches das international anerkannteste Rahmenwerk für Governance und Kontrollen ist. [Lach07] Cobit wird in Organisationen und Unternehmen in mehr als hundert Ländern eingesetzt, um die Informationsressourcen effektiv zu nutzen, Information in Relation zu Risiken effektiv zu verwalten und das Management im Entscheidungsprozess zur IT Governance zu unterstützen. [JiYu06]

Das COBIT Modell gliedert die IT Aktivitäten in die vier Domänen: „plane und organisiere“ (engl. „plan and organise“), „beschaffe und implementiere (engl. „acquire and implement“), „erbringe und unterstütze“ (engl. „deliver and support“) und „überwache und beurteile“ (engl. „monitor and evaluate“). Analog zum ITIL Framework ist der PDCA Zyklus in den Domänen fest verankert.

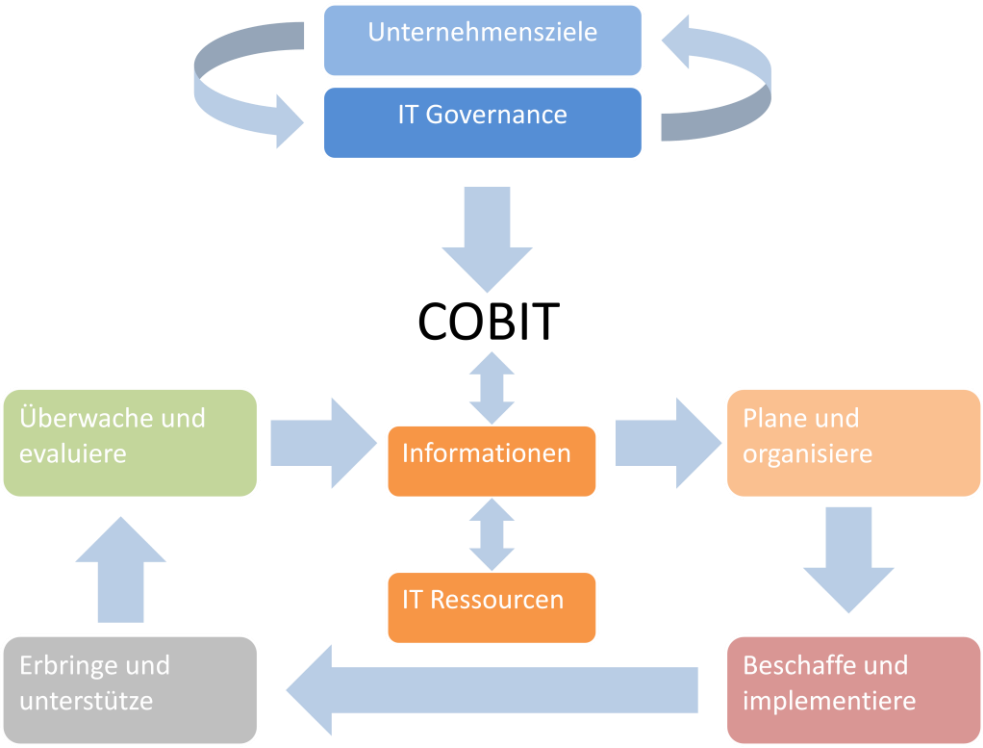



**Abbildung 71: IT Governance Modell von COBIT [ITGI07]**

Durch COBIT wird eine Kommunikationsbrücke zwischen Unternehmenszielen und IT Governance Zielen geschaffen. Zusätzlich werden parallel dazu ein effektives Management und Kontrollen für strategische Ausrichtung und effektive Nutzung von IT Ressourcen etabliert. COBIT identifiziert in [ITGI07] die folgenden vier IT Ressourcen:

- Anwendungen sind automatisierte Anwendungen und manuelle Verfahren, die Informationen verarbeiten.
- Informationen sind die Daten in all ihren Formen: Durch Informationssysteme eingelesen, verarbeitet oder ausgegeben, in jeder im Unternehmen verwendeten Form.
- Infrastruktur sind die Technologien und Anlagen (Hardware, Betriebssysteme, Datenbankmanagementsysteme, Netzwerke, Multimedia usw. und die Einrichtungen, die diese beherbergen und unterstützen).
- Personal sind jene Personen, die für Planung, Organisation, Beschaffung, Implementierung, Betrieb, Unterstützung, Monitoring und Evaluierung der Informationssysteme und Services benötigt werden. Sie können – je nach Bedarf – intern, outgesourct oder vertraglich gebunden sein.

In mehreren Publikationen von ISACA (siehe [ISACA10]) kann die Kompatibilität zwischen ITIL und COBIT nachgelesen werden. Wissenschaftlich analysiert und nachgewiesen wurde die Kompatibilität in [SaSh08]. Daraus leitet sich ab, dass ITIL mit modernem Informations-Sicherheitsmanagement harmonisiert und darin integrierbar ist.

In [NaSa08] geht man sogar einen Schritt weiter und stellt die Hypothese auf, dass die Service Strategie, wie in ITIL Version 3 definiert, bereits alle Charakteristika eines IT Governance Frameworks erfüllt. Basierend auf [CrCe05] werden die folgenden vier Erfüllungsmerkmale identifiziert: IT Wert / Nutzen und Ausrichtung zwischen Geschäftsbereich und IT, Risiko Management der IT Risiken und Geschäftsrisiken, wobei diese zumeist ineinandergreifen, Haftung / Verantwortlichkeit des Managements (siehe dazu Sarbanes- Oxley Act [Sar02]) und Performance Messung in den Bereichen: IT Wert / Nutzen, Benutzer, Qualität des Betriebs und Zukunftsorientierung / -sicherheit. Ebenfalls referenzierend auf [CrCe05] wird festgestellt, dass für ein gutes IT Governance ein Rahmenwerk basierend auf den folgenden drei Kernelementen implementiert sein muss: Struktur, Prozesse und Kommunikation. Die Struktur bestimmt die Entscheidungsträger, die Organisationsstruktur, die Zuständigkeiten und Verantwortlichkeiten. Prozesse legen fest, wie Entscheidungen getroffen werden. Des Weiteren bestimmen sie den konkreten Ablauf. Die Kommunikation definiert, wie die Ergebnisse von Prozessen (Output) und Entscheidungen überwacht, gemessen und kommuniziert werden. In [NaSa08] wird die Konformität der Service Strategie gemäß ITIL Version 3 zu einem IT Governance Framework diskutiert und prinzipiell festgestellt. Die einzelnen ITIL Prozesse müssten allerdings noch analog zu [SaSh08]

und [ISACA10] dem IT Governance Modell zugeordnet werden, um den Beweisschritt zu vervollständigen.

Nach dem durch die Kompatibilität mit COBIT erbrachten Nachweis, dass die auf ITIL basierten Sicherheitsmaßnahmen gegen Angriffe eines Social Engineers in ein umfassendes Sicherheitskonzept eingebettet werden können und mit diesem harmonisieren, wird abschließend auf ein anderes modernes systematisches Sicherheitsmodell eingegangen. 2005 wurde in University of Southern California's Institute for Critical Information Infrastructure Protection (ICIIP) ein Rahmenwerk für Enterprise Security entwickelt. Das in [KiBe06] vorgestellte Systemic Security Management Model beinhaltet die drei Eckpfeiler traditioneller Modelle – „Menschen" (Personal), „Prozesse" und „Technologie". Zusätzlich wird der vierte Eckpfeiler, jener der „Organisation Design und Strategie", hinzugefügt, wodurch ein dreidimensionales Modell in Form einer Pyramide (wie in Abbildung 72 dargestellt) aufgespannt wird.

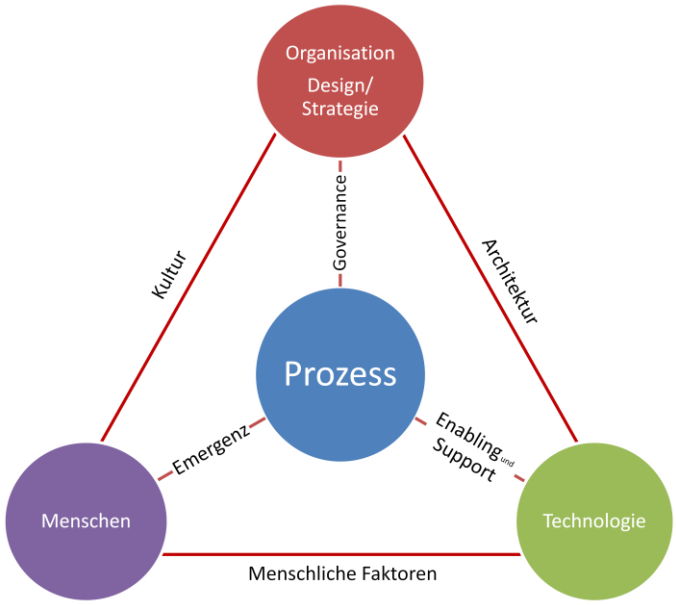



**Abbildung 72: Systemic Security Management Model [KiBe06]**

Die Beziehungen zwischen den Eckpunkten der Pyramide sind sechs dynamische Abhängigkeiten, welche im Modell als Spannungen (engl. „Tensions") bezeichnet werden, um die dynamische Komponente und die sich oftmals ergebenden Konfliktsituationen zwischen den Rollen hervorzuheben. Die sechs Spannungen sind: „Governance", „Kultur",

„Architektur“, „Emergenz“, „Menschliche Faktoren“ und „Enabling and Support“. Das Modell wird in [ISACA09] detailliert erläutert.

In [Klai10] wird festgestellt, dass die signifikanteste Neuerung in diesem Modell die Sichtweise ist und dass sich Sicherheit aus dynamischen Interaktionen multidimensionaler Eckpunkte ergibt.

Der systemische Ansatz findet sich auch in den Sicherheitsmaßnahmen gegen Human- based Social Engineering Attacken basierend auf dem ITIL Rahmenwerk wieder. Die Kombination und Wechselwirkung zwischen Mensch – Technologie – Organisation im prozessorientierten Umfeld, um ein IT Service Management aufzubauen, aufrecht zu erhalten und kontinuierlich zu verbessern, ist inhärenter Bestandteil von ITIL. Ebenfalls wird damit die Anforderung gemäß [KiBe06] erfüllt, dass systemische Sicherheit über das Unternehmen hinaus gehen sollte. Unternehmen, die eine ITIL konforme Prozesslandschaft aufgebaut haben, beeinflussen direkt den Kunden und die Lieferanten. Lieferanten unterliegen den ITIL Supplier Management Prozessen, Kunden kommunizieren mit dem Service Desk, um Fehler und Anfragen zu melden. Der Service Level Manager dient als weitere in ITIL festgelegte Ansprechperson für den Kunden. Des Weiteren führt die Etablierung einheitlicher Begrifflichkeiten, einheitlicher Standards und Zertifizierungsmethoden zu Vergleichbarkeiten zwischen Unternehmen, was einen direkten Einfluss auf die einzelnen Unternehmen hat (siehe dazu beispielsweise den Sarbanes- Oxley Act [Sar02]).

## 7.2 Fallbeispiele

Die folgenden Beispiele sollen die praktische Anwendbarkeit des ITIL Rahmenwerks als Bestandteil eines Sicherheitskonzepts für Service Operation gegen Angriffe eines Social Engineers darstellen. Hierbei wurden bewusst ein Beispiel aus dem öffentlichen Bereich und eines von einem privaten Dienstleister gewählt.

Beide Fallbeispiele zeigen auch, dass eine Einzelimplementierung der Maßnahmen auch ohne ITIL möglich wäre. Durch ITIL entsteht ein organisationsweites Rahmenwerk, welches nicht auf ein einzelnes Service und einzelne Organisationseinheiten ausgerichtet ist, sondern auf eine unternehmensweite Implementierung und den Betrieb von allen IT Services abzielt. Daraus ergibt sich eine einheitliche und harmonische Strategie und Umsetzung, die insgesamt kosteneffektiv, effizient und weiterentwickelbar sind. Die Kosteneffizienz ist durch die gemeinsame Nutzung von Ressourcen gegeben. Effizienz ist inhärenter Bestandteil von ITIL durch das

Qualitätsmanagement im PDCA Zyklus. Die Weiterentwickelbarkeit ist duch das strategische Vorgehensmodell sowie dessen Umsetzungskontrollen und Messverfahren zur Leistungserbringung gegeben.

Als Negativbeispiel könnte die Etablierung eines Incident Management Prozesses herangezogen werden. Wird für ein Service in einem Unternehmen ein Incident Management Prozess gelebt, so kann dieser durchaus effizient in einer auf dieses Service bezogenen isolierten Betrachtungsweise sein. Wird ITIL nicht als unternehmensweites Rahmenwerk herangezogen, so können sich für unterschiedliche Services verschiedene Ausprägungen von Incident Management Prozessen entwickeln und etablieren, die trotz möglicher Synergien unterschiedliche Ressourcen nutzen und bei unternehmensweiter Betrachtung komplex, nicht nachvollziehbar und kaum steuerbar sind.

### *7.2.1 ITIL bei Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft*

Der Einsatz der elektronischen Stimmabgabe (E-Voting) bei den Hochschülerinnen- und Hochschülerschaftswahlen war eines der anspruchsvollsten E-Government-Projekte des Jahres 2009 in Österreich. Dabei galt es, den papierbasierten Wahlprozess um einen elektronischen Wahlkanal zu ergänzen und so neue Möglichkeiten zur Stimmabgabe zu schaffen. [BMWF10]

Nach der Bekanntgabe durch Bundesminister Dr. Hahn im Mai 2007, dass er, entsprechend der Empfehlung der im Jahr 2004 im Bundesministerium für Inneres eingesetzten Arbeitsgruppe „E-Voting“ [Krim07], die Umsetzung von E-Voting bei den Wahlen zur Hochschülerinnen- und Hochschülerschaft 2009 beabsichtige, wurden die Möglichkeiten des E-Voting im Rahmen einer Machbarkeitsstudie im Sommer 2007 evaluiert und als positiv beurteilt.

Grundsätzlich sollte die elektronische Stimmabgabe so in den Wahlprozess integriert werden, dass sie eine zusätzliche Beteiligungsmöglichkeit darstellte und die Wahl im Papierweg in der bisherigen Form weiter bestehen würde. Daher wurde für das E-Voting die Sonderform der vorgezogenen Stimmabgabe eingeführt, die in der Woche vor dem ersten Wahltag der herkömmlichen Papierwahl von Montag 8.00 Uhr bis Freitag 18.00 durchgehend ermöglicht wurde. Während dieser Zeit sollten alle Studierenden an den österreichischen Universitäten durchgehend die Möglichkeit haben, die Stimmabgabe über das Internet durchzuführen. Nach

Ende des E-Voting-Zeitraumes sollten die elektronischen Stimmen bis zum Ende der herkömmlichen Wahl verschlüsselt aufbewahrt werden. Studierende, die von der Möglichkeit der elektronischen Stimmabgabe Gebrauch gemacht hatten, wurden in der Wählerevidenz mit dem Vermerk E-Voting markiert, womit eine Mehrfachstimmabgabe verhindert wurde.

Die rechtliche Grundlage für E-Voting ist in zwei Rechtstexten geregelt – dem Hochschülerinnen- und Hochschülerschaftsgesetz 1998 (HSG) [Oest98] und der zugehörigen Verordnung Hochschülerinnen- und Hochschülerschaftswahlordnung 2005 (HSWO) [BMWF05].

Vier Monate nach der Bekanntgabe durch den Bundesminister, E-Voting einzuführen, wurde von der Hochschülerinnen- und Hochschülerschaft ein Beschluss veröffentlicht [OeH07], welcher grundsätzliche Bedenken gegen E-Voting, der damit verbundenen Technologie und der angeführten nicht Vereinbarkeit mit den Grundsätzen der freien und geheimen Wahl beinhaltete. Wie in [BMWF10] festgestellt wird, wurde die Einführung von E-Voting als zusätzlichen Wahlkanal zu einem sehr kontroversiellen – oftmals ausgesprochen emotionalen – Thema, welches der dominierende Wahlkampfinhalt wurde. So kam es während der elektronischen Stimmabgabe bei den Wahlen der Österreichischen Hochschülerinnen- und Hochschülerschaft 2009 zu einer Vielzahl von Angriffen auf das E-Voting System und den Wahlkanal, welche exemplarisch in [EhNa10] analysiert werden. Unter anderem kam es zur weltweit ersten distributed Denial of Service Attacke gegen einen elektronischen Wahlkanal bei einer rechtsverbindlichen Wahl. Ebenfalls fand eine Reihe von Social Engineering Angriffen statt. Details zu den Angriffen und zur E-Voting Implementierung sind unter [EhNa10], [BMWF10] und [KrEh10] zu finden.

Um gegen die schon im Vorfeld erwarteten Angriffe gewappnet zu sein, wurden vom Betreiber des E-Voting Systems entsprechende Gegenmaßnahmen getroffen. Um Social Engineering entgegenzuwirken, war ITIL inhärenter Bestandteil des Sicherheitskonzepts, wie in den vorigen Kapiteln beschrieben. Folgend wird ein Fallbeispiel einer Anwendung analysiert, welche durch Human- based Social Engineering gefährdet war.

Grundsätzlich handelt es sich bei den Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft um mehr als dreihundert Wahlen, die zeitgleich an allen einundzwanzig Österreichischen Universitäten stattfinden. Gewählt werden Universitätsvertretungen, Studienvertretungen und eventuelle Urabstimmungen. Lokale Wahlkommissionen an den Universitäten leiten die Wahlen auf der

jeweiligen Universitätsebene. Eine österreichweite Bundeswahlkommission in Wien übernimmt die Gesamtkoordination.

Mit der Einführung von E-Voting musste das Aufgabenfeld der Wahlkommission erweitert und an die Anforderungen von E-Voting angepasst werden. Mit der Novelle obliegt der Wahlkommission an der jeweiligen Universität von nun an auch das Starten, Unterbrechen, Wiederaufnehmen und Beenden des E-Votingvorgangs (§ 14 Abs. 1 Z 17 HSWO 2005). [BMWF10]

Die Anforderung des Startens der Wahlen wurde durch eine formale Freigabe der Wahlkommissionen der Universitäten realisiert, sodass die elektronische Stimmabgabemöglichkeit automatisch exakt mit Beginn der Stimmabgabefrist vom E-Voting System aktiviert wurde. Analog wurde das automatische Beenden am Ende der Stimmabgabefrist realisiert. Das Unterbrechen und vorzeitigen Beenden einer oder aller Wahlen konnte über eine administrative Oberfläche vom Betreiber des E-Voting Systems durchgeführt werden. Eine Wahlkommission einer Universität ruft beim Betreiber an und verlangt, dass die Wahl unterbrochen werden muss, woraufhin der Mitarbeiter des Betreibers die entsprechende Wahl über die administrative Oberfläche stoppt.

Hierbei gibt es natürlich eine Reihe von Angriffsvektoren für einen Social Engineer. Es wäre für ihn ein Leichtes, sich für eine Wahlkommission einer Universität auszugeben und eine oder alle Wahlen zu stoppen, was einer Denial of Service Attacke gleichkommen würde. Zu beachten ist, dass die Wahlkommissionen an den Universitäten fast hundert Personen in Österreich sind und sich die Besetzung der Wahlkommission kurzfristig jederzeit ändern kann. Die Ausgabe von Losungsworten zur Authentifikation von Anrufern wäre somit ebenfalls wenig handhabbar und würde große Sicherheitslücken aufreißen.

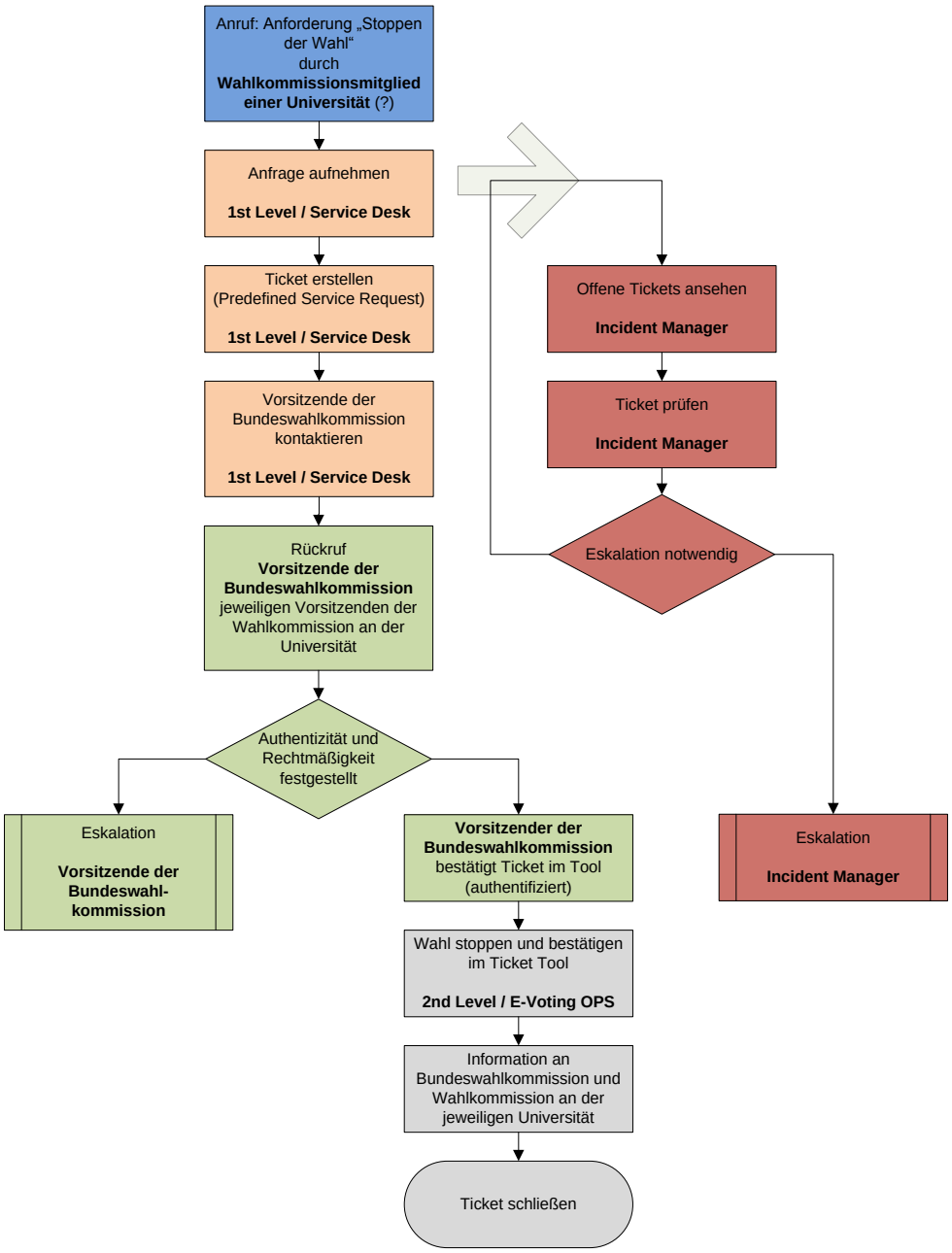



**Abbildung 73: Prozessbeschreibung zum Anhalten einer Wahl**

Betrachtet man nun den auf ITIL basierenden Prozess zur Behandlung der Anforderung, eine Wahl anzuhalten, so wird dieser wieder durch den Telefonanruf eines vermeintlichen Wahlkommissionsmitglieds einer Universität initiiert. Dem Sicherheitsprinzip, Choke Points zu verwenden, folgend, stellt der Service Desk einen Single Point of Contact dar (siehe Kapitel 5.1). Nur im Service Desk darf die Anfrage angenommen werden. Jegliche Anfragen werden im Ticket Tool erfasst, womit gleichzeitig eine wohl definierte Prozesskette Schritt für Schritt abgearbeitet wird, was dem

Prinzip, gut zu planen und sich daran zu halten, entspricht (siehe Kapitel 5.3). Der Prozessablauf ist im Ticket Tool für den Standard- Change „Anhalten einer Wahl“ definiert. Es weist den Service Desk Mitarbeiter an, den Vorsitzenden der Bundeswahlkommission zu kontaktieren. Dessen Kontaktdaten werden im Ticket Tool angezeigt und idealerweise erfolgt der Wählvorgang auch gleich durch eine Integration des Tickets Tools in die Telefonanlage. Dadurch stellt die Toolunterstützung einen großen Mehrwert für den Mitarbeiter dar, indem sich die toolunterstützte Prozessdurchführung sehr einfach gestaltet (siehe Kapitel 5.6). Der Vorsitzende der Bundeswahlkommission prüft die Authentizität des Wahlkommissionsmitgliedes sowie die Rechtmäßigkeit der Beschlussfassung innerhalb der Universitäts-Wahlkommission. Nur ihm müssen aufgrund der Wahlordnung alle Vorsitzenden der Universitäts-Wahlkommissionen bekannt sein. Nachdem er die Authentizität des Anrufers und die Rechtmäßigkeit der Anfrage bestätigt hat, kann der nächste Prozessschritt folgen. Die Authentizität des Vorsitzenden der Bundeswahlkommission muss ebenso sichergestellt werden. Hierzu stehen dem Vorsitzenden zwei Möglichkeiten zur Verfügung. Er kann über Nennung eines korrekten (Einmal-)Losungsworts, welches vom Service Desk Mitarbeiter im Ticket Tool eingetragen und vom Tool verifiziert und bestätigt wird, den nächsten Bearbeitungsschritt auslösen. Die andere Variante ist, dass der Vorsitzenden einen authentifizierten Direktzugriff auf das Ticket Tool nutzt (siehe Kapitel 5.2). Das Ticket wird automatisch einem 2nd Level Mitarbeiter der Betriebsmannschaft zugewiesen, der im Sinne der Sicherheitsprinzipien der gestaffelten Abwehr (siehe Kapitel 5.5). und des Infragestellens (siehe Kapitel 5.9) zuerst den korrekten bisherigen Prozessablauf prüft. Nur er verfügt über die notwendigen administrativen Rechte, eine Wahl zu stoppen (siehe Kapitel 5.5), was er entsprechend der Prozessdefinition auch tut. Mit dem Schließen des Tickets werden automatisiert durch das Tool Informationen zur Anfrage und Prozessdurchführung an die Wahlkommission der jeweiligen Universität und an die Bundeswahlkommission per E-Mail geschickt.

In Frage stellen bedeutet auch, die Einhaltung der Prozesskette und die Prozessqualität kontinuierlich zu prüfen. Diese Aufgabe wird vom Incident Manager wahrgenommen, der alle Tickets schon ab Erstellung immer wieder sichtet und gegebenenfalls entsprechende Eskalationsschritte einleitet (siehe Kapitel 5.9).

Der 2nd Level Mitarbeiter des Betriebsteams, welcher als einziger über die administrativen Rechte zum Stoppen der Wahl verfügt, ist sich wiederum der Transparenz seiner Handlungen vor allem gegenüber dem Incident

Manager bewusst. Zusätzlich hat er entsprechend der Prozessdefinition keinen Kontakt zum Anrufer, dem vermeintlichen Wahlkommissionsmitglied. Ein Social Engineer kann somit nicht die menschlichen Faktoren von Social Engineering wie Knappheit, Autorität, Sympathie, soziale Bewährtheit, Konsistenz oder Reziprozität (siehe Kapitel 4.3) ausnutzen. Insgesamt wird somit die korrekte Prozessbehandlung durch den 2nd Level Mitarbeiter ausreichend sichergestellt.

Zusätzlich wurden die Prozessabläufe, auch jener der Standard- Changes, im Vorfeld zu den Wahlen ausgiebig besprochen und trainiert. Die Gefahr von Human- based Social Engineering Attacken bei der Österreichischen Hochschülerinnen- und Hochschülerschaftswahlen wurde durch Schulungen dem gesamten Betriebsteam vermittelt, wodurch das schwächste Glied – der Mensch – zusätzlich gestärkt wurde (siehe Kapitel 5.7).

Indem man ITIL als Methode gegen Social Engineering Attacken im Sicherheitskonzept angewendet hat, konnte ein ausreichender Schutz aufgebaut werden, sodass es zu keiner erfolgreichen Attacke bei den Österreichischen Hochschülerinnen- und Hochschülerschaftswahlen kam. Das Fallbeispiel soll primär die praktische Anwendbarkeit verdeutlichen, die somit klar gegeben ist.

### *7.2.2 ITIL als Basis eines Kontrollsystems einer österreichischen Bank*

Als zweites Beispiel der praktischen Anwendbarkeit von ITIL als Sicherheitskonzept für Service Operation gegen Human- based Social Engineering Attacken wird eine österreichische Bank herangezogen. Diese zählt zu den kapitalstärksten Banken Österreichs und ist Teil einer internationalen Bankengruppe. Neben dem regionalen Netzwerk an Geschäftsstellen ist die Bank innerhalb der Bankengruppe für Zentral- und Osteuropa verantwortlich, womit es sich um ein großes internationales Finanzinstitut mit Wurzeln in mehr als zwanzig Ländern handelt.

Seit 2006 wird in der Bank im Betriebsbereich von Handelssystemen IT Service Management basierend auf ITIL aufgebaut, um die Qualität zusätzlich zu steigern und der publizierten Geschäftsstrategie von Qualität, Fairness und Transparenz noch besser zu entsprechen. Des Weiteren sollte damit eine Vergleichbarkeit und bessere Leistungsabgrenzung innerhalb des Bankennetzwerkes geschaffen werden. Hierzu wurden die etablierten Betriebsprozesse analysiert sowie entsprechend den Empfehlungen von ITIL angepasst und weiter optimiert. Zusätzlich wurde ein Ticket Tool

implementiert und schrittweise eingeführt. Das Ticket Tool entspricht den individuellen Anforderungen und unterstützt die prozessorientierte Bearbeitung insbesondere von Anfragen (Service Requests) und Störungsmeldungen (Incidents).

Als Fallbeispiel wird die Durchführung einer Passwort Zurücksetzung herangezogen. Laut Szenario kann ein Händler nicht mehr in sein Handelssystem einsteigen und benötigt dringend ein neu gesetztes Passwort. Da die Produktivität während der Prozessdurchführung nicht gegeben ist, liegt die Priorität in der schnellen Behandlung der Anfrage. Parallele Prozesse, die somit die Behandlungsdauer der Anfrage nicht beeinflussen, sollen die notwendige Sicherheit vor Human- based Social Engineering Attacken gewährleisten.


**Abbildung 74: Prozessbeschreibung des Zurücksetzen eines Passworts**

Die Behandlung der telefonischen Anfrage, das Passwort zurückzusetzen, ist aufgrund der Rahmenbedingungen bewusst sehr linear und somit effizient gestaltet. Die Anfrage wird vom Service Desk aufgenommen und in einem Ticket Tool augenblicklich erfasst. Da Passwortzurücksetzungen sehr oft vorkommen, ist hierfür ein Standard- Change hinterlegt, wodurch das Ticket Tool automatisch nach Anlegen des Tickets eine Mail an den Händler schickt. Da das Ticket Tool eine Schnittstelle zur Telefonanlage hat, werden sämtliche wichtigen Anruferdaten sofort im Ticket Tool dargestellt. Diese Informationen unterstützen den Service Desk Mitarbeiter schon im Vorfeld, Social Engineering Angriffe zu erkennen. Beispielsweise stellen der vollständige Name, die Abteilungszugehörigkeit und etwaige

andere aktuell offene Tickets des Anrufers eine wertvolle Unterstützung und Informationsbasis für den Mitarbeiter dar, wodurch widersprüchliche oder unplausible Angaben des Angreifers erkannt werden können (siehe dazu Kapitel 5.7). Zusätzlich unterstützen die Daten aus der Telefonanlage das schnelle Ausfüllen und Erstellen des Tickets (siehe Kapitel 5.6).

Basierend auf der Rufnummer wird an die automatisch vom elektronischen Firmentelefonbuch ausgelesene E-Mail Adresse des Anrufers eine Bestätigungsmail geschickt. Die E-Mail beinhaltet ein Einmal-Passwort in Form eines Links. Wenn der Empfänger den Link öffnet, wird die Anfrage zum Zurücksetzen des Passworts bestätigt. Alternativ kann der betroffene Benutzer das Ticket nach erfolgreicher Authentifikation im Ticket Tool bestätigen.

Vorerst nicht dem Sicherheitsprinzip der gestaffelten Abwehr folgend, wird das Ticket durch denselben Service Desk Mitarbeiter im 1st Level weiter behandelt. Grund hierfür liegt in den Rahmenbedingungen, wonach man eine möglichst schnelle Bearbeitung priorisiert. In den meisten Fällen ist davon auszugehen, dass der Anrufer noch in der Telefonleitung des 1st Level Mitarbeiters ist. Da der Händler dringend das Passwort zurückgesetzt braucht, bevor er weiter produktiv arbeiten kann, erfolgt die elektronische Bestätigung durch ihn umgehend. Die weitere Behandlung des Tickets durch denselben Service Desk Mitarbeiter ist damit ausgesprochen effizient. Das Ticket Tool generiert ein zufälliges Initialpasswort, auf welches er die Benutzerdaten des Händlers umstellt. Mit der Bestätigung der Durchführung wird eine E-Mail an den Händler geschickt. Die E-Mail beinhaltet das neue initiale Passwort, welches durch den Händler bei der ersten Anmeldung in die Handelsplattform neu zu vergeben ist.

Der parallel ablaufende Prozess des Incident Managers gestalten sich analog zum vorigen Fallbeispiel. Der Prozess ist auch als Kontrolle der Einhaltung der Prozesskette zu verstehen (siehe Kapitel 5.9).

Die Sicherheitsprinzipien der gestaffelten Abwehr und des Infragestellens sind transferiert und finden sich im ebenfalls parallel ablaufenden zusätzlichen Überwachungsprozess wieder. Angestoßen wird der Prozess durch eine technische Sicherheitsmaßnahme. Ändert sich der Dateiinhalt, so wird dies augenblicklich durch ein Monitoring System, auf das der Service Desk Mitarbeiter keinen Zugriff hat, erkannt und Informationen werden zur Veränderung über einen entsprechenden Kanal an einen Auditor geschickt. Der Auditor prüft die korrekte Prozessdurchführung, insbesondere ob eine entsprechende Bestätigung zur Passwort Rücksetzung vorhanden ist (siehe Kapitel 5.5 und Kapitel 5.9). Damit sich der Service Desk Mitarbeiter über

diese Kontrolle durch einen Auditor bewusst wird, kontaktiert ihm der Auditor zumindest für eine kurze Rücksprache. Dies stellt eine bewusste Stresssituation für den Service Desk Mitarbeiter dar, welche ebenfalls einem etwaigen Angriff eines Social Engineers entgegenwirkt (siehe Kapitel 5.7).

Das Fallbeispiel verdeutlicht nicht nur die Umsetzbarkeit der auf ITIL basierten Service Management Prozesse als Sicherheitskonzept gegen Human- based Social Engineering Attacken, sondern zeigt auch dass Sicherheitsmaßnahmen nicht zwangsläufig die Prozessdurchführungsdauer verlängern müssen. Das Passwort wird schnellstmöglich zurückgesetzt, sodass der Händler weiter seinen geschäftlichen Tätigkeiten nachgehen kann. Parallele Kontrollprozesse, welche technisch automatisiert angestoßen werden, sind die Grundstruktur eines effektiven Kontrollsystems.

## 7.3 Restrisikobestimmung

*An der Universität Bamberg wurde 1999 die Studie [Scha10] durchgeführt, die menschliches Versagen analysierte. Hierbei wurden Arbeitsunfälle in zwei Bergwerken miteinander verglichen. Während das erste Bergwerk über gut asphaltiert und ausgeleuchtet Stollen verfügte, waren die Wege im anderen deutlich schlechter. Man nimmt nun an, dass die Anzahl der Stolperunfälle im vermeintlich sichereren Bergwerk geringer wären. Die Studie zeigte aber, dass dies nicht der Fall war. Befragungen der Arbeiter ergaben, dass sie in den gut asphaltierten und ausgeleuchteten Stollen kein Risiko sahen. Die Bergarbeiter im anderen Bergwerk waren sich hingegen über den schlechten Ausbau des Stollens als Gefahrenquelle bewusst und verhielten sich dementsprechend vorsichtiger. Die Forscher kamen somit zum Schluss: „Wenn der Mensch kein Risiko sieht, wird er unvorsichtig und macht mehr Fehler.“*

Zweck dieses Kapitels ist es, Fehleinschätzungen und Überschätzungen vorzubeugen. In den vorigen Kapiteln wurde ITIL als Methode gegen Human- based Social Engineering Attacken für Service Operations vorgestellt. Die Wirkungsweise, der Wirkungsbereich, der Wirkungsvektor, die Wirkungssteuerung und -kontrolle wurden dargestellt und die praktische Anwendbarkeit über Fallbeispiele verdeutlicht. Dies könnte nun zum trügerischen Schluss führen, dass ein Angriff eines Social Engineers keine Gefahr mehr darstellt, sobald man ITIL basierte Betriebsprozesse eingeführt hat.

Klar ist, dass es keine absolute Sicherheit gibt.

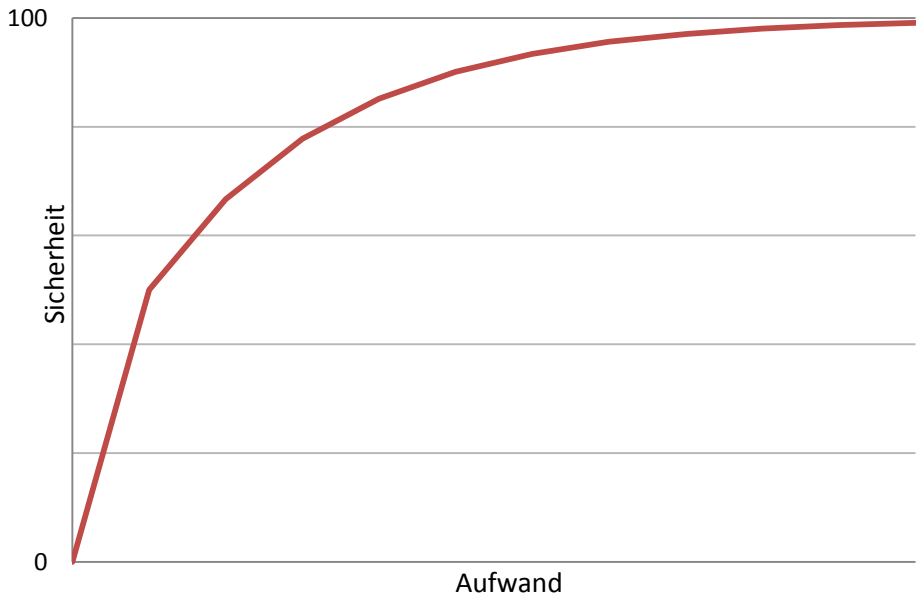



**Abbildung 75: Sicherheit in Relation zum Aufwand für Sicherheitsmaßnahmen [Raep01]**

Die Abbildung 75 stellt diesen Umstand visuell dar. Der Aufwand für mehr Sicherheit steigt stetig an, was in der Darstellung durch eine exponentielle Funktion veranschaulicht wird. Der Sachverhalt hierfür ist trivial. Es ist ein erheblicher Unterschied, ob man die Verfügbarkeit eines Services von 70% auf 71% erhöhen möchte oder von 99% auf 99,999%. Bei einer Verfügbarkeitsanforderung um die 70% kann das Service in etwa zwei Tage pro Woche nicht zur Verfügung stehen. Manuelle Wiederherstellungsprozeduren sind im Fehlerfall durchaus praktikabel. Ein Prozent mehr oder weniger macht hierbei kaum einen relevanten Unterschied. Bei einer Verfügbarkeitsanforderung von 99% darf es zu einer maximalen Ausfallszeit von knapp über einer Stunde pro Woche kommen. Fehler müssen dabei bereits automatisch frühzeitig erkannt werden, komplexe manuelle Wiederherstellungsprozeduren sind innerhalb der zeitlichen Anforderungen nicht umsetzbar. Bei einer Verfügbarkeitsanforderung von 99,99% darf es zu einer maximalen Ausfallszeit von einer Minute pro Woche kommen. Dieser Anforderung können nur redundant ausgelegte, spezielle Hochverfügbarkeitslösungen entsprechen.

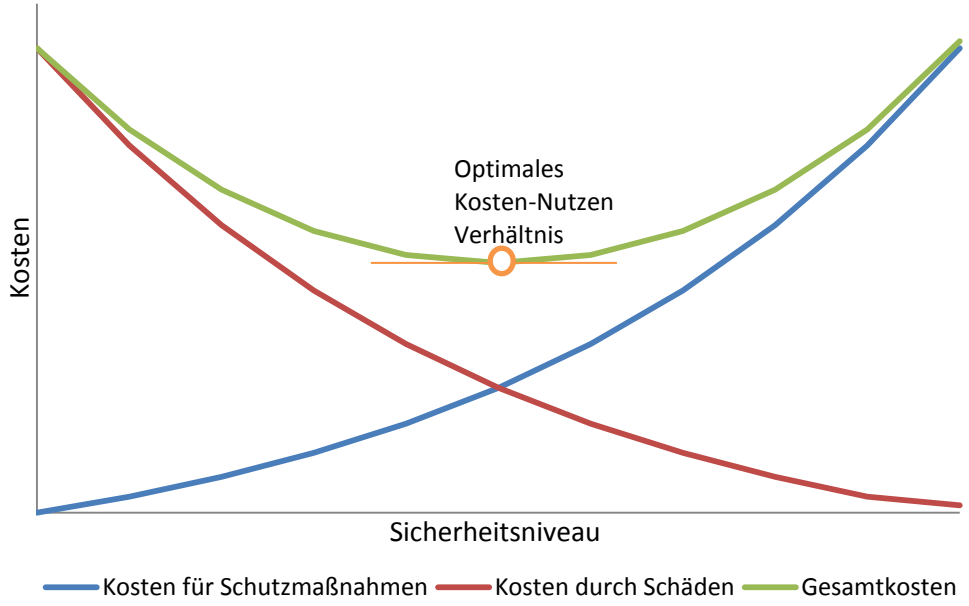



**Abbildung 76: Das optimale betriebliche Kosten-Nutzen-Verhältnis in Abhängigkeit von Sicherheitskosten und potentiellen finanziellen Schäden [Raep01]**

In [Raep01] wird das optimale betriebliche Kosten-Nutzen-Verhältnis in Abhängigkeit von Sicherheitskosten und potentiellen finanziellen Schäden beschrieben. Je mehr Investitionen in Sicherheit getätigt werden, umso geringere Schadenskosten ergeben sich. Summiert man die beiden Graphen auf, so entsteht eine Kurve, welche im Scheitelpunkt das optimale Kosten-Nutzen-Verhältnis wiedergibt.

Betrachtet man nun ITIL als Bestandteil eines Sicherheitskonzepts gegen Human- based Social Engineering für Service Operations, so ist ebenfalls notwendig festzustellen, dass keine absolute Sicherheit erreicht werden kann. Nachdem ITIL bereits in vielen Unternehmen zur Betriebsoptimierung eingeführt wurde, stellt es aber eine – wie in dieser Arbeit gezeigt – effiziente, effektive und praktikable Möglichkeit dar, mehr Sicherheit gegen Social Engineering durch einen inhärenten systematischen Ansatz zu etablieren. Hierbei ist entscheidend, dass der Grad der Sicherheit durch das Management steuerbar wird, da das Leistungsvermögen der IT nicht länger intransparent ist, Investitionen und Ressourcen strategisch eingesetzt und Risiken adäquat verwaltet werden können. [NaRo08] [Klai10]

Gliedert man die Restrisikobestimmung nach den Eckpfeilern des systemischen Ansatzes von ITIL, so spannt sich ein Betrachtungsraum bestimmt durch Mensch, Technologie und Organisation auf. Betrachtet man

zuerst den Faktor Mensch, so muss festgestellt werden, dass den in Kapitel 4.3 dargestellten menschlichen Faktoren von Social Engineering durch die im ITIL Rahmenwerk beschriebene Kombination aus Technologie, Organisation und Menschen entgegengewirkt wird, natürlich aber in der isolierten Betrachtungsweise eines Menschen immer seine Gültigkeit und Wirksamkeit auf ihn haben. Ein einzelner Mensch wird stets durch Autorität, Knappheit, Sympathie usw. potentiell beeinflusst werden können. ITIL kann aber die Wahrscheinlichkeit der erfolgreichen Manipulation verringern, die Auswirkung mindern sowie Human- based Social Engineering Angriffe erkennen und analysieren.

Wie in der Einleitung zu diesem Kapitel festgehalten, kann aber ein Sicherheitsgefühl trügerisch sein und so leicht von einem Social Engineer ausgenutzt werden. Die Studie [OFT09] der Universität Exeter zeigt, dass Personen, welche überdurchschnittlich anfällig für Betrug (in der Studie mit engl. „Scam“ bezeichnet) sind, im allgemein keine schwachen Entscheidungsträger sind. Beispielsweise waren einige davon erfolgreiche Geschäftsleute oder Akademiker. In der Tat ist Aufgeschlossenheit eine wichtige Charaktereigenschaft in unserer Gesellschaft und oftmals eine Grundlage für Erfolg. Die Grenze zwischen Aufgeschlossenheit und einer Schwäche gegenüber Überredungskünsten zu ziehen ist ausgesprochen diffizil. Eine andere typische Ursache von Fehlentscheidungen ist Selbstüberschätzung, ein Sachverhalt der mehrfach experimentell nachgewiesen wurde (zum Beispiel [CLOE99]). Aus einer breiten Basis wissenschaftlicher Analysen ist bekannt, dass Selbstüberschätzung zu Befangenheit bei der Entscheidungsfindung und Informationsgewinnung führt. [FGFS08] Es zeigt sich, je mehr Wissen Personen über ein spezifisches Fachgebiet verfügen, umso kompetenter fühlen sie sich in diesem Bereich. Daraus ergibt sich konsequenterweise eine Selbstüberschätzung bei der Entscheidungsfindung. Dieser Schluss findet sich auch bei [ScFi08] wieder. Je mehr Informationen einem Entscheidungsträger zur Verfügung stehen (vor allem wenn sie alle in die gleiche Richtung weisen), umso selektiver ist er in der Informationssuche und umso schlechter ist die Qualität der dann getroffenen Entscheidung (siehe auch [KrGa03]).

Wissenschaftliche Untersuchungen ergaben auch, je mehr Informationen Personen zu einem bevorzugten Standpunkt finden, umso mehr sind sie von der Qualität dieser Informationen überzeugt. [ScFi08]. In [OFT09] wird daraus gefolgert, dass Personen leichter in der Domäne ihres Wissensbereichs betrogen werden können. Sie sind aufgrund ihrer Selbstüberschätzung voreingenommen und neigen dazu, Warnzeichen zu

ignorieren, welche die Intention des Betrügers entlarven würden. Dieser Schluss wurde auch von [ShSc07] bestätigt, wobei das Phänomen von [DuSh04] entdeckt wurde. Deren Untersuchung ergab, dass Personen mit mehr Erfahrung mit dem Internet gefährdeter von Internetbetrug waren, was sich aus Selbstüberschätzung ergab.

Bestandteil des ITIL Rahmenwerks ist die Konzentration von Expertenwissen innerhalb der Prozessbehandlung. Der Service Desk stellt beispielsweise einen Single Point of Contact zur Behandlung von Incidents dar. Die Gefahr von Selbstüberschätzung aufgrund der vorhandenen Expertise ist ein stetiges Risiko, dem nur durch Maßnahmen entgegengewirkt werden kann, die das Wollen und Können von Mitarbeitern in Bezug auf Sicherheit überprüfen. Des Weiteren soll durch die Anwendung einer adäquaten Eignungsdiagnostik sichergestellt werden, dass auch im Bezug auf Sicherheit geeignete Mitarbeiter gefunden werden (siehe Kapitel 5.7). Aus der der Unschärfe der Eignungsdiagnostik und der Effektivität der Maßnahmen zur Prüfung und Steigerung des Wollens und Könnens ergibt sich ein effektives Risiko für Human- based Social Engineering.

Neben der menschlichen Komponente muss man auch den technologischen Eckpfeiler von ITIL bei der Restrisikobestimmung von Human- based Social Engineering betrachten. Hierbei stellen die durch ITIL etablierte Technologie eines Ticket Tools und die geschaffenen zentralen Informationspools wie die SKMS, die CMDB und das Ticket Tool selbst neue Angriffsvektoren für einen Social Engineer dar. Gelingt es einem Angreifer, das Ticket Tool zu manipulieren, so kann er Prozessabläufe verändern, Fehlinformationen einschleusen und Handlungsanweisungen verändern, entfernen oder hinzufügen. Die Integrität des Ticket Tools ist also von entscheidender Wichtigkeit. Zusätzlich stellt der Zugriff auf die geschaffenen Informationspools ein neues, begehrtes Ziel für Social Engineering Angriffe dar. Die Konfiguration aller Systemkomponenten, Informationen zu den Mitarbeitern, Ablaufbeschreibungen, Service Level Agreements, Störungsbehebungsstrategien, Wiederanlaufpläne im Katastrophenfall und vieles mehr stellen definitiv sensible Informationen dar. Abgesichert werden die Informationspools und das Ticket Tool gegen Angriffe von außen primär durch technische Maßnahmen. Intern muss eine (Risiko-)Abwägung getroffen werden, ob alle Mitarbeiter Zugriff auf die Informationspools haben oder ob Einschränkungen getroffen werden und wie diese konkret realisiert werden. Darf zum Beispiel ein Mitarbeiter des Windows Supports nur SKMS Einträge aus seinem Arbeitsbereich einsehen? Bei Schnittstellenproblemen zu Unix Systemen wären aber

gegebenenfalls weitere Informationen außerhalb des Windows Bereichs hilfreich. Noch schwieriger gestaltet sich eine etwaige Differenzierung eines 1st und 2nd Level Mitarbeiters im selben Tätigkeitsbereich.

Ebenfalls ergeben sich Restrisikoüberlegungen auf Prozessebene. Ein Prozess wird durch den Prozessverantwortlichen entworfen und gegebenenfalls angepasst. Die Sicherheit ist vom Design des Prozesses abhängig, welches primär von Service Level Agreements als auch weiterführend von der Unternehmenspolitik und verschiedenen Normen (Policies) beeinflusst wird. Risikobewertungen bilden sowohl eine Grundlage für die Erstellung der Service Level Agreements, der Unternehmenspolitik, der Normen als auch für das Design jedes Prozesses. Die Bewertung ist hierbei spezifisch durchzuführen, was sich auch aus dem Wesen von ITIL als Rahmenwerk ergibt. ITIL beinhaltet eine Reihe von Best Practices, welche eine Struktur darstellen, innerhalb derer geplant, implementiert, kontrolliert und verbessert wird. Das Rahmenwerk ist somit kontextunabhängig, für eine Risikobestimmung muss der Gesamtkontext insbesondere der Kundenanforderungen aber herangezogen werden.

Ein besonderes Risiko ergibt sich aus der Nichteinhaltung der Prozesse durch einzelne Mitarbeiter. Verschiedene Maßnahmen, wie beispielsweise aus dem Sicherheitsprinzip des Infragestellens stellen (siehe Kapitel 5.9) oder der Einfachheit (siehe Kapitel 5.6), versuchen dem entgegen zu wirken.

Im Kontext von Social Engineering muss eine neue Gefahrenquelle betrachtet werden, die sich erst in den letzten Jahren entwickelt hat. Soziale Netzwerke wie beispielsweise Facebook, Twitter, MySpace oder Xing haben eine unglaubliche Popularität erreicht. Facebook wird täglich von 35% aller Internet Benutzer weltweit besucht. 8% der österreichischen Internet Benutzer besuchen täglich Twitter, 0,4% täglich Xing [Alex10].


**Abbildung 77: Soziale Netzwerke**

In [Sieg09], der die Gefahren in Sozialen Netzwerken in Bezug auf Social Engineering aufzeigt, wird zunächst festgestellt, dass das wesentliche Element eines Sozialen Netzwerks das Bekanntmachen und Teilen von Informationen mit einem unbekannten Personenkreis ist. Das Problem ergibt sich insofern, als oftmals Benutzer von Sozialen Netzwerken sehr sensible Informationen in ihr Profil stellen. Hierzu wird in [Sieg09] beispielsweise auf [BrHo08] verwiesen. Des Weiteren wird ausgeführt, dass basierend auf [SIT08] die Daten zentral vom Betreiber des jeweiligen Sozialen Netzwerks gespeichert werden und der Benutzer somit die Kontrolle über seine Daten verliert.

Zu beachten ist, dass immer eine Relation zwischen Benutzer und Daten möglich ist und Menschen identifiziert werden können. Das Sicherheitsprinzip der Anonymität ist also nicht effektiv gegeben. In [WoHo10] wird dazu die Angriffsmöglichkeit der De-Anonymisierung unter Ausnützung den Gruppenmitgliedschaften von Benutzern Sozialer Netzwerke praktisch nachgewiesen.

Ein Social Engineer kann eine Reihe wertvoller Informationen aus Sozialen Netzwerken beziehen, durch Interpretationen und Relationen noch weitere Informationen gewinnen, welche insgesamt eine gefährliche Basis für einen Angriff darstellen. Beispielsweise könnte man die Bedrohung durch Einbrecher aufzeigen, Fotos zum Ausspionieren von potentiellem Diebesgut nutzen und Statusmeldungen heranziehen, um den optimalen Zeitpunkt des Einbruchs zu planen. Durch Tools können diese Recherchen automatisiert

werden, was in [Hube09] detailliert analysiert und deren Effizienz nachgewiesen wird.

Neben der passiven Recherche kann ein Social Engineer Soziale Netzwerke auch aktiv nutzen, um Mitarbeiter zur Herausgabe sensible Informationen zu bringen. Das Soziale Netzwerk dient dann als Angriffsmedium, in dem Identitätsdiebstahl und die Ausnutzung menschlicher Faktoren von Social Engineering (wie in Kapitel 4.3 zusammengefasst) dazu führen, dass „Mitarbeiter im Privatleben“, also außerhalb der Sicherheitsmaßnahmen des Unternehmens und dem Sicherheitsbewusstsein der Arbeit, Opfer von einem Social Engineer werden. Vergleichen könnte man diesen Angriff mit einem scheinbar harmlosen Gespräch über die Arbeit beim Heurigen. Soziale Netzwerke sind allerdings deshalb so gefährlich, da die Annahme einer falschen elektronischen Identität vergleichsweise viel einfacher ist. Ein Social Engineer kann im Sozialen Netzwerk auch die Identität einer dem Opfer bekannten und vertrauten Persönlichkeit annehmen. Zusätzlich stellen Soziale Netzwerke ein sehr effizientes Medium dar, indem der Angreifer mit wenig Aufwand selbst in kurzer Zeit viele Opfer attackieren kann. Gleichzeitig ist das eingegangene Risiko relativ gering, jedenfalls signifikant geringer, als wenn der Social Engineer seinem Opfer physisch beim Heurigen gegenübersitzt.

In gewisser Weise muss der Ansatz der systemischen Sicherheit, welcher entsprechend [KiBe06] sich auch dadurch auszeichnet, dass er über das Unternehmen hinaus geht, nicht nur andere Unternehmen, Kunden und Lieferanten betreffen, sondern auch Mitarbeiter als Privatperson verstärkt inkludieren.

Abschließend muss in Zuge der Restrisikobestimmung auch festgestellt werden, dass diese Arbeit auf Attacken eines Social Engineers in Service Operations beschränkt war. Daraus ergibt sich, dass basierend auf dieser Arbeit in gleicher Weise die Sicherheit der anderen Phasen des ITIL Service Lifecycles, insbesondere von Service Transition, in weiterführenden Arbeiten analysiert werden sollte. Bietet das Change Management durch die Analyse und Dokumentation von Changes, der Bewertung der Geschäftsauswirkungen (engl. „Business Impact Analysis“), der Risikobestimmung und Sicherheitsanalyse eine ausreichende Sicherheit? Wie muss die CMDB des Asset and Configuration Managements aufgebaut werden, um effektiv gegen Angriffe eingesetzt zu werden?

Auch wurde bei dieser Arbeit eine klare Abgrenzung von Technology-based Social Engineering Attacken gemacht. Weiterführend analysieren sollte man also, ob ITIL gegen Schadsoftware und Trojaner Schutz bietet.

Sowohl die aufgezeigte Weiterführung dieser Arbeit als auch das Beispiel einer neuen Gefahr durch Soziale Netzwerke, welche auf der stetigen Weiterentwicklung der Informationstechnologie und dem Wandel der Nutzung basiert, verdeutlichen die Notwendigkeit einer kontinuierlichen Neubewertung von Gefahren, Risiken und Gegenstrategien.

Bruce Schneier [Schn00]: „*Sicherheit ist ein Prozess, kein Produkt.*“

# 8 Conclusio

Social Engineering stellt eine stetige Gefahr dar, die den Faktor Mensch ausnützt, um Sicherheitsmechanismen auszuhebeln. Verschiedene Konstanten menschlichen Verhaltens ermöglichen es dem Social Engineer, unberechtigten Zugang zu Informationen oder Systemen durch Aushorchen zu erlangen oder eine Person dazu zu bringen, eine gewisse Aktion zu setzen. Da die vom Angreifer ausgenützten Aspekte wie etwa Konsistenz, soziale Bewährtheit, Sympathie, Autorität oder Knappheit, tief im menschlichen Verhalten verankert sind, bleiben jene Ansätze klassischer Sicherheitsmodelle, die auf die alleinige Stärkung menschlichen Verhaltens gegen Social Engineering abzielen, oftmals unzureichend. Schulungen von Mitarbeitern und Sensibilisierungsmaßnahmen stellen keine ausreichende Sicherheit gegen Social Engineering Angriffe dar.

Moderne Sicherheitsmodelle zeichnen sich zum einen durch die Ausrichtung der Informationssicherheit entsprechend der Unternehmensziele und -strategien in Form von IS Governance aus. Zum anderen folgen sie einem multi-dimensionalen Ansatz, der unterschiedliche Aspekte und deren Wechselwirkungen berücksichtigt.

ITIL ist ein Modell, das die Ziele, Rollen, Aktivitäten sowie die notwendigen Prozesse innerhalb einer IT Organisation in Form eines Best Practice Rahmenwerks beschreibt. Wenn man die Notwendigkeit zur Absicherung vor Social Engineering Attacken als Teil des zu erbringenden Services eines Unternehmens betrachtet, so ist der Schluss nahe, dass ITIL ein geeignetes Rahmenwerk für ein multi-dimensionales Sicherheitsmodell gegen Social Engineering darstellen könnte. In ITIL wurden im Rahmen dieser Arbeit allgemeine Sicherheitsgrundsätze gegen Social Engineering in Service Operation Prozessen identifiziert. Sicherheitsgrundsätze wie Choke Points verwenden, Authentizität sicherstellen, gut planen und sich daran halten, Risiko durch Aufteilung verringern, gestaffelte Abwehr, Einfachheit, das schwächste Glied sichern und in Frage stellen sind wesentliche Eckpfeiler von Sicherheit.

Beispielsweise stellt der in ITIL definierte Service Desk ein dem Sicherheitsprinzip – Chokepoints verwenden – entsprechendes, bewusst eingerichtetes Nadelöhr dar. Jegliche Anfragen und Störungen müssen darüber eingebracht, erfasst und verfolgt werden. Sicherheitsmerkmale und Mechanismen können an dieser einen Stelle etabliert werden und schützen damit das gesamte Unternehmen. Dies erfüllt nicht nur das Kriterium der

ökonomischen Effizient, sondern ist auch Grundvoraussetzung zum effektiven Erkennen und Behandeln von Attacken eines Social Engineers.

Auch ergeben die in ITIL definierten Prozesse ein Vorgehensmodell, welches Social Engineering Angriffe entscheidend erschwert. Dadurch ist es nämlich einem Social Engineer theoretisch nicht mehr möglich, den Mitarbeiter beispielsweise durch Knappheit, Autorität oder Sympathie in seinen Handlungen zu beeinflussen, da die Aktivitäten, Akteure und Schnittstellen genau definiert sind.

Die in ITIL identifizierten Sicherheitsprinzipien und -maßnahmen erschweren, erkennen oder verhindern gänzlich Attacken eines Social Engineers. Aus der Summe der Maßnahmen wurde ein Maßnahmenkatalog gegen Social Engineering abgeleitet. Der Wirkungsbereich der Maßnahmen liegt primär in der systemischen Ebene, welche als multi-dimensionales Modell aus Mensch, Technik und Organisation im prozessorientierten Kontext verstanden wird. Die Umsetzung der Maßnahmen führt zu mehr Sicherheit in den einzelnen Dimensionen. Die Begrifflichkeit des Wirkungsvektors wurde in dieser Arbeit genutzt, um die Verschiebung innerhalb der Dimensionen zu mehr Sicherheit im Bereich Technik, Mensch und Organisation zu veranschaulichen. Die Länge der Verschiebung ist hingegen von vielen Faktoren abhängig, wie etwa von der Art der zu erbringenden Dienstleistungen. Des Weiteren wurde in der Arbeit gezeigt, dass die Ausrichtung der Betriebsprozesse in Anlehnung an die Best-Practice Empfehlungen von ITIL keinen automatischen Schutz vor Social Engineering darstellt. ITIL muss als Methode verstanden werden, in gewisser Weise ein Werkzeug, das gegen Social Engineering Attacken eingesetzt werden kann, insofern man das Werkzeug auch dementsprechend gebrauchen möchte. Die Steuerung und Kontrolle entsprechend dem in ITIL fest verankerten Deming PDCA Zyklus setzt auf Service Level Agreements. Neben dem Maßnahmenkatalog stellen die in dieser Arbeit angeführten Kontrollen zur Wirkungssteuerung und -kontrolle in Verbindung mit den Service Level Agreements die Umsetzungsgrundlage für den kontinuierlichen Qualitätskreislauf dar.

Nach der Analyse der Wirkungsweise, des Wirkungsbereichs, des Wirkungsvektors sowie der Wirkungssteuerung und -kontrolle der auf ITIL basierenden Maßnahmen gegen Social Engineering wurde in dieser Arbeit die harmonische Integration von ITIL ins moderne Informations-Sicherheitsmanagement dargestellt. Damit ist die Anwendbarkeit im unternehmensweiten IT Sicherheitsmanagement gegeben. Zusätzlich zeigten Fallbeispiele aus dem Banken und dem E-Government Bereich die

praktische Umsetzung der dargestellten Konzepte und aufgelisteten Maßnahmen.

In dieser Arbeit wurde gezeigt, dass ITIL eine effiziente, effektive und praktikable Möglichkeit zum Management von mehr Sicherheit gegen Social Engineering in Service Operations darstellt.

# Literaturverzeichnis

Die Internetadressen wurden im Februar 2011 verifiziert.

[Alex10] Alexa: The Web Information Company – Facebook Statistics. Abgerufen 2010. http://www.alexa.com/siteinfo/facebook.com

[Andr09] Andres, Martina: Konzeption einer Assessment Methode auf Basis von CMMI für kleine Software-Unternehmen. Diplomarbeit an der Technischen Universität Wien, 2009

[Anle02] Anley, Chris: Advanced SQL Injection in SQL Server Applications. NGSSoftware Insight Security Research (NISR) Publication, 2002. http://www.nextgenss.com/papers/advanced_sql_injection.pdf

[APWG09] The Anti-Phishing Working Group (APWG), Phishing Activity Trends Report, Jänner - Juni 2009. http://www.antiphishing.org

[ArMe02] Arkes, Hal R.; Mellers, Barbara A.: Do Juries Meet Our Expectations? In: Law and Human Behavior, 26, 6, 625-639, 2002.

[ASW10] AG für Sicherheit der Wirtschaft (ASW), WirtschaftsWoche Konferenz Risiko Wirtschafts- und Wettbewerbsspionage, 2010.

[Ayal06] Ayalp, Serdar: IT-Sicherheitsbewertung und ISO/IEC TR 13335. Ausarbeitung an der Universität Koblenz, 2006

[Ayni08] Ayni, Qais: State of the Art und Trends desr digitalen Signatur. Diplomarbeit an der Universität Wien, 2008.

[BaGe05] Barnum, Sean; Gegick, Michael: Least Privileges. Homeland Security, 2005.

[BeBe04] Belser, Sandra; Berchtold, Oliver: Einführung eines Internen Kontrollsystems. Fachartikel IKS, 2004.

[Beck90] Becker, G. Fred: Anreizsysteme für Führungskräfte: Möglichkeiten zur strategisch-orientierten Steuerung des Managements. Poeschel Verlag, 1990.

[GrBe09] Grechenig, Thomas, Bernhart, Mario; Breiteneder, R.; Kappel, Karin: Softwaretechnik - Mit Fallbeispielen aus realen Entwicklungsprojekten. Verlag Pearson Studium, 2009.

[BMWF05] Bundesministerium für Wissenschaft und Forschung (BMWF): Hochschülerinnen- und Hochschülerschaftswahlordnung 2005 (HSWO 2005). http://www.bmwf.gv.at/wissenschaft/national/gesetze/studienrecht/

[BMWF10] Bundesministerium für Wissenschaft und Forschung (BMWF): E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009 – Evaluierungsbericht. 29. März 2010. http://www.oeh-wahl.gv.at/

[BoJo08O] Van Bon, Jan; De Jong, Arjen; Kolthof, Axel; Pieper, Mike ; Tjassing, Ruby; van der Veen, Annelies: Service Operation basierend auf ITIL V3. Van Haren Publishing, 2008.

[BoJo08S] Van Bon, Jan; De Jong, Arjen; Kolthof, Axel; Pieper, Mike ; Tjassing, Ruby; van der Veen, Annelies: Service Strategy basierend auf ITIL V3. Van Haren Publishing, 2008.

[BoJo08T] Van Bon, Jan; De Jong, Arjen; Kolthof, Axel; Pieper, Mike ; Tjassing, Ruby; van der Veen, Annelies: Service Transition basierend auf ITIL V3. Van Haren Publishing, 2008.

[BoMa06] Bock, Wolfgang; Macek, Günter; Oberndorfer, Thomas; Pumsenberger, Robert: ITIL - Zertifizierung nach BS 15000/ ISO 20000. Galileo Press, 2006.

[Bon08C] van Bon, Jan: Continual Service Improvement basierend auf ITIL V3. Van Haren Publishing, 2008.

[Bon08D] van Bon, Jan: Service Design basierend auf ITIL V3. Van Haren Publishing, 2008.

[Born89] Bornstein, R. F.: Exposure and affect - Overview and meta-analysis of research, 1968-1987. In: Psychological Bulletin, 106, 265-289, 1989.

[Breit09] Breitner, Michael H.: Ein ganzheitliches Konzept für Informationssicherheit unter Berücksichtigung des Schwachpunkt Mensch. Diplomarbeit an der Universität Hannover, 2009.

[BrHo08] Brown, Garrett; Howe, Travis; Ihbe, Micheal; Prakash, Atul; Borders, Kevin: Social Networks and Context-Aware Spam. In: CSCW ’08: Proceedings of the ACM 2008 conference on Computer supported cooperative work, 403-412, New York, 2008.

[Brig95] Briggs-Myers, Isabel: Gifts Differing – Understanding Personality Type. Davies-Black Publishing, 1995.

[Brig98] Briggs-Myers, Isabel: Introduction to Type – A Guide to Understanding Your Results on the Myers-Briggs Type Indicator, Center for Applications Publishing, 1998.

[BrMc98] Briggs-Myers, Isabel; McCaulley, Mary H.: Manual - A Guide to the Development and Use of the Myers-Briggs Type Indicator. Consulting Psychologists, 1985.

[Broe07] Böttcher, Roland: IT-Servicemanagement mit ITIL V3: Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen. Heise, 2007.

[BSI06] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheit von Webanwendungen. Version 1, August 2006. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/WebSec/WebSec_pdf.pdf?__blob=publicationFile

[BSI08] Bundesamt für Sicherheit in der Informationstechnik (BSI): Grundschutzkatalog. Stand 2008. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[BSI89] Bundesamt für Sicherheit in der Informationstechnik: ZSIEC Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems. Bundesanzeiger-Verlag Köln, 1989.

[BSI98] Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/cln_136/ContentBSI/Themen/Zertifi

zierungundAkkreditierung/ZertifierungnachCCundITSEC/ITSicherheitskriterien/ITSEC/itsec_eval.html

[Buch06] Buchholz, Stefan: Evaluation von Remote-Angriffsmethodiken auf vernetzte IT-Systeme. Bachelorarbeit an der Albert-Ludwigs-Universität Freiburg, 2006.

[Buhl05] Buhl, Ulrike: ITIL Praxisbuch, Beispiele und Tipps für die erfolgreiche Prozessoptimierung. MITP, 2005.

[BuKe98] Buss D. M., Kenrick D. T.: Evolutionary Social Psychology. In: Handbook of Social Psychology, 2, 4th Edition, 982-1026, 1998.

[Buss89] Buss, D. M.: Sex differences in human mate preferences: evolutionary hypotheses tested in 37 cultures. In: Behavioral. Brain Science, 12, 1-49, 1989.

[CaCa04] Calluzzo, Vincent J.; Cante, Charles J.: Ethics in Information Technology and Software Use. In: Journal of Business Ethics, 51, 3, 301-312, 2004.

[CaOv99] Cazenier, Jacques A.; Overbeek, Paul L., Peter, Louk M. C.: Best Practice for Security Management. Office of Government Commerce (OGC), 1999.

[CC06] Common Criteria for Information Technology Security Evaluation (CC)

Offizielle Webseite: http://www.commoncriteriaportal.org/

Bund für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/cln_134/ContentBSI/Themen/ZertifizierungundAkkreditierung/ZertifierungnachCCundITSEC/ITSicherheitskriterien/CommonCriteria/cc.html"

[Cert03] CERT: Advisory CA-2003-19 Exploitation of Vulnerabilities in Microsoft RPC Interface. 2003. http://www.cert.org/advisories/CA-2003-19.html

[CESG89] Communications-Electronics Security Group (CESG): UK Systems Security Confidence Levels, CESG Memorandum No. 3, Großbritannien, Jänner 1989

[Chau87] Chaum, D.: Sicherheit ohne Identifizierung – Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen. In: Informatik-Spektrum 10/5, 262-277, 1987 und Datenschutz und Datensicherung, DuD/1, 26-41, 1988.

[ChDu08] Chiesa, Raoul; Ducci, Stefania; Ciappi, Silvia: Profiling Hackers - The Science of Criminal Profiling as Applied to the World of Hacking. Auerbach; 1st Edition; 2008.

[Chur06] Von Chur, Beat Affolter: Realoptionsanalyse zur Bewertung von IT-Outsourcing-Projekten. Diplomarbeit an der Universität Zürich, 2006.

[Cial07] Cialdini, Robert B.: Die Psychologie des Überzeugens. Ein Lehrbuch für alle, die ihren Mitmenschen und sich selbst auf die Schliche kommen wollen. Huber Verlag, 2007.

[CoE01] Council of Europe (CoE): Decision, Adopting the Council's Security Regulations. 19. März 2001, 2001/264/EC. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:101:0001:0066:EN:PDF

[CoRo09] Comelli, Gerhard; von Rosenstiel, Lutz: Führung durch Motivation. Vahlen Verlag, 2009.

[CrCe05] Craig, Symons; Cecere, Mark; Young, G. Oliver; Lambert, Natalie: IT Governance Framework: Structures, Processes and Communication. White Paper, Forester Research, März 29, 2005.

[CuMa10] Cusick, J.J.; Ma, G.: Creating an ITIL inspired Incident Management approach: Roots, response, and results. In IEEE/IFIP Network Operations and Management Symposium Workshops, 2010, 142-148, 2010.

[Cunn86] Cunningham, Michael R.: Measuring the physical in physical attractiveness – Quasi-experiments on the sociobiology of female facial beauty. In: Journal of Personality and Social Psychology, 50, 5, 925-935, 1986.

[DaBe87] Darley, J. M.; Berscheid, E.: Increased liking caused by the anticipation of interpersonal contact. In: Human Relations, 10, 29-40, 1967.

[DeCl01] Devine, E.; Clayton, L. D.; Dunford, B. B.; Seying, R.; Pryce, J.: Jury decision making – 45 years of empirical research on deliberating groups. In: Psychology, Public Policy and Law, 7, 622-727, 2001.

[Deit90] Deitel, Harvey M.: An introduction to operating systems. 2. Aufl., Addison-Wesley Longman Publishing Co., 1990.

[DeKe05] Desney, S. Tan; Keyani, Pedram; Czerwinski, Mary: Spy-resistant keyboard: more secure password entry on public touch screen displays. In: OZCHI '05, Proceedings of the 19th conference of the computer-human interaction special interest group (CHISIG) of Australia on Computer-human interaction, Canberra, 1-10, 2005.

[Demi86] Deming; W. E.: W. E. Out of the Crisis. Cambridge, MA: MIT CAES, 1986

[Diem08] Diemer, Marco: Berücksichtigung des Menschen in der Informationssicherheit mit dem Persönlichkeitsmodell von Julius Kuhl. Diplomarbeit an der Universität Hannover, 2008.

[DeSt85] DePaulo, B.M.; Stone, J.I.; & Lassiter, G.D.: Deceiving and Detecting Deceit". In: B.R. Schlenker (Ed.), The self and social life. 1985, 323-370, New York: McGraw-Hill.

[Diers01] Dierstein, Rüdiger: Datenschutz und IT-Sicherheit. Vorlesung an der Technischen Universität München, Wintersemester 2001/2002.

[DiPi09] Dimkov, Trajce; Pieters, Wolter; Hartel, Pieter: Two methodologies for physical penetration testing using social engineering. In: Technical Report TR-CTIT-09-48, Centre for Telematics and Information Technology, University of Twente, Enschede.

[DTI89] Department of Trade and Industry Großbritannien (DTI): DTI Commercial Computer Security Centre Evaluation Levels Manual, V22, Februar 1989.

[DoCa07] Dodge, Ronald C.; Carver, Curtis; Ferguson, Aaron J.: Phishing for user security awareness. In: Computers & Security, 26, 1, 73-80, 2007.

[DuSh04] Dutton, W. H.; Shepherd: Confidence and risk on the Internet. Oxford Internet Institute, 2004.

[Dvwe05] dv werk: Thinking Services for You. 2005. http://www.dv-werk.de/fw_itil/syllabus/index.html

[EhNa10] Ehringfeld, Andreas; Naber, Larissa; Grechenig, Thomas; Krimmer, Robert; Traxl, Markus; Fischer, Gerald: Analysis of Recommendation Rec(2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria. In: Proceedings of the 4th International Conference on Electronic Voting, 225-237, 2010.

[EhNa11] Ehringfeld, Andreas; Naber, Larissa; Kappel, Karin; Fischer, Gerald; Pichl, Elmar; Grechenig, Thomas: "Learning from a Distributed Denial of Service Attack against a Legally Binding Electronic Election: Scenario, Operational Experience, Legal Consequences." In EGOVIS 2011, 2nd International Conference on Electronic Government and the Information Systems Perspective, 2011.

[Ehri03] Ehringfeld, Andreas: Durchführbarkeit und Nutzen von Sicherheitsanalysen nach Grundschutz in KMUs. Diplomarbeit an der Technischen Universität Wien, 2003.

[Ehri07] Ehringfeld, Andreas: Vorlesungseinheit: Betriebliche Aspekte und Vorlesung Advanced Internet Security. Technische Universität Wien, 2007.

[Ehri10] Ehringfeld, Andreas: "First legally binding Election in Austria - the Student Union Election";In: 4th International Conference on eDemocracy (EDEM 2010), Krems, 2010.

[Ehri10A] Ehringfeld, Andreas: "ITIL als Methode gegen Social Engineering Attacken". In: Hacking - IT Security Magazin, Hackin9 10/2010.

[EhNK11] Ehringfeld, Andreas; Naber, Larissa; Kappel, Karin; Fischer, Gerald; Grechenig, Thomas: "Toward a Management Catalog of Security Measures against Social Engineering Attacks." In ICEIM 201, International Conference on Engineering and Information Management, 2011.

[Elsa06] Elsässer, Wolfgang: ITIL einführen und umsetzen - Leitfaden für effizientes IT-Management durch Prozessorientierung. Hanser Fachbuchverlag, 2. Aufl., 2006.

[EsGa10] Esmaili, H.B.; Gardesh, H.; Sikari, S.S.: Strategic alignment - ITIL perspective. In: 2nd International Conference on Computer Technology and Development (ICCTD), 550-555, 2010.

[Euro95] Europäisches Parlament: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT

[Farn05] Farner, Nicole: Integration of Security Engineering Principles into the Software Lifecycle Management. Diplomarbeit an der Universität Zürich, 2005.

[Fars09] Farshchi, Jamil: Intrusion Detection FAQ: Statistical based approach to Intrusion Detection. SANS Institute. http://www.sans.org/security-resources/idfaq/statistic_ids.php

[Feik08] Feik, Jan: Strategien für global diversifizierte Immobilienportfolios. Diplomarbeit an der Universität Leipzig, 2008.

[Fels01] Felser, Georg: Werbe- und Konsumentenpsychologie. Spektrum-Akademischer Verlag; 2. Aufl., 2001.

[FiSc05] Fink, A.; Schneidereit, G.; Voß, S.: Grundlagen der Wirtschaftsinformatik. Physica, 2. Aufl., 2005.

[FoZo06] Fox, Christpher; Zonneveld, Paul; IT Governance Institute: IT Control Objectives for Sarbanes-Oxley - The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting. ISACA, 2. Aufl., 2006.

[Fran07] Franker, Leif Thorvald: Erstellung eines Kriterienkataloges zur Gewährleistung der technischen Sicherheit von E-Commerce-Webseiten. Diplomarbeit an der Universität Koblenz, 2007.

[Franc97] France, E.: European initiatives in privacy and data protection. In: Computer-Fraud-&-Security, 12-16, 1997.

[Frie05] Fries, Alexander: Konsistenz und Inkonsistenz im psychischen Geschehen der Menschen - Konzepte und Zusammenhänge mit der Gesundheit. Doktorarbeit an der Universität Bern, 2005.

[FrLa03] Friedmann, Mattern; Langheinrich, Marc: Die Informatisierung des Alltags. In: Bulletin ETH Zürich, 291, 15-18, 2003.

[FTC09] Federal Trading Commission (FTC): Annual Report. FTC´s Identity Thief Site, http://www.ftc.gov/bcp/edu/microsites/idtheft/

[Gartn02] Gartner: Six Human Behaviors for Positive Response. In: Social Engineering- Exposing the Danger Within, 1, 1, 2002. http://www.gartner.com/gc/webletter/security/issue1/index.html

[GaTo93] Gardner, R. M.; Tockerman, Y. R.: Body dissatisfaction as a predictor of body size distortion: A multidimensional analysis of body image. In: Genetic, Social, and General Psychology Monographs, 119, 125-145, 1993.

[Gauv05] Gauvin, Tony: Profiling a Hacker. Capstone Project, 2005. http://ciag.umfk.maine.edu/Shane%20Durost.pdf

[Gelb03] Gelbmann, Ulrike: IL Management als integrative Disziplin. Institut für Innovations- und Umweltmanagement, 20.10.2003. http://www-classic.uni-graz.at/inmwww/gelbmann/MIDWS0304EH1u2.pdf

[Gette07] Getter, J.R.: Enterprise Architecture and IT Governance: A Risk-Based Approach. In: 40th Annual Hawaii International Conference on System Sciences (HICSS), 2007, 220, 2007.

[Graw04] Grawe, Klaus: Neuropsychotherapie. Hogrefe, Göttingen 2004.

[Graw98] Grawe, Klaus: Psychologische Therapie. Hogrefe, Göttingen 1998.

[Grec07] Greco, Riccardo: Unsicherheit bei der Verhaltensbeobachtung und -bewertung im Assessment Center. Mögliche Einflussfaktoren und ihr Zusammenhang zur Beurteilungsgenauigkeit. Diplomarbeit an der Universität Bielefeld, 2007.

[HaBi94] Hamermesh, Daniel S.; Biddle, Jeff E.: Beauty and the Labor Market. In: American Economic Review, 84, 1174-1194, 1994

[HaPr09] Hasan, Mosin; Prajapati, Nilesh: An Attack Vector for Deception Through Persuasion Users by Hackers and Crackers. In: NETCOM '09 Proceedings of the 2009 first International Conference on Networks & Communications, 2009.

[Harr96] Harrington, Susan J.: The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. In: MIS Quarterly, 20, 3, 257-278, 1996.

[Hein08] Heinz, Andreas: Optimierung des Business Continuity Managements von Klein- und Mitelunternehmens mittels ITIL V3. Magisterarbeit an der Technischen Universität Wien, 2008.

[HeKa05] Hentze, Joachim; Kammel, Andreas; Lindert, Klaus; Graf, Andreas: Personalführungslehre - Grundlagen, Funktionen und Modelle der Führung. UTB, Haupt Verlag, 2005.

[Henni98] Henning, Pagnia: Seminar WS98/99 Technische Grundlagen elektronischer Geschäftsbeziehungen. http://www.informatik.tu-armstadt.de/BS/Lehre/Sem98_99/T4/ElekGeld.html

[Herb00] Herbst, Dieter: Erfolgsfaktor Wissensmanagement. Cornelsen Verlag, 2000.

[Herk96] Herkner, Werner: Lehrbuch Sozialpsychologie. Huber Bern Verlag, 5. Aufl., 1996.

[Hewi09] Hewitt: Studie und Ranking von 160.000 Mitarbeitern und 4.000 Top Managern aus 700 Unternehmen über 2 Jahre in 11 zentral- und osteuropäischen Ländern. 2009. http://www.hewittassociates.com/

[HeYe08] Ho-Yeol, Kwon: Security Engineering in IT Governance for University Information System. In: Conference on Information Security and Assurance (ISA), 2008, Seite 501-504, April 2008.

[Hone04] The Honeynet Project: Know Your Enemy: Learning about Security Threats. Addison-Wesley Professional; 2 Edition, 2004.

[HoPr03] Hoppe, Gabriela; Prieß, Andreas: Sicherheit von Informationssystemen. NWB Verlag, 2003.

[HP00] Hewlett Packard (HP): The HP IT Service Management Reference Model (HP ITSM). Whitepaper, Version 2.0, 2000. http://www.nga.org/cda/files/HPITWhite.pdf

[Hube09] Huber, Markus: Automated Social Engineering Proof Of Concept. Masters thesis an der DSV SecLab, SU/KTH Stockholm, 2009.

[HuKo09] Huber, Markus; Kowalski, Stewart; Nohlberg, Marcus; Tjoa, Simon: Towards Automating Social Engineering Using Social Networking Sites. In: 2009 International Conference on Computational Science and Engineering, Vancouver, August 2009.

[IBM01] IBM: Managing Information Technology Services. Version 1.0, 2001. http://www-935.ibm.com/services/us/its/pdf/managing_it_services_white_paper.pdf

[IBM08] IBM: IBM Service Management - IBM® Tivoli® Unified Process (ITUP). Publiziert November 2008. http://www-01.ibm.com/software/tivoli/governance/servicemanagement/itup/tool.html

[ICCC09] Internet Crime Complaint Center (IC3): Annual Report. 2009. http://www.ic3.gov/

[IDW02] Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW), Düsseldorf: IDW PS 330 - Abschlussprüfung bei Einsatz von Informationstechnologie. In: WPg, 21, 1167 ff., 2002.

[IDW99] Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW), Düsseldorf: IDW PS 880 – Erteilung und Verwendung von Softwarebescheinigungen. In: WPg, 23-24, 1066 ff., 1999.

[Info07] Infosecurity: Infosecurity Bericht 2007. Teil der Information Security Awareness Week, beginnend am 21. April 2007.

[IRM03] The Institute for Risk Management (IRM): A Risk Management Standard, 2002. http://www.theirm.org/publications/PUstandard.html

[ISACA09] Information Systems Audit and Control Association (ISACA): An Introduction to the Business Model for Information Security. 2009. http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf

[ISACA10] Information Systems Audit and Control Association (ISACA):

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit, 2008.

COBIT Mapping: Mapping of ITIL V3 With COBIT 4.1, 2008.

COBIT Mapping: Mapping of NIST SP800-53 Rev 1 With COBIT 4.1, 2007.

COBIT Mapping: Mapping of TOGAF 8.1 With COBIT 4.0, 2007.

COBIT Mapping: Mapping of CMMI® for Development V1.2 With COBIT 4.0, 2007.

COBIT Mapping: Mapping of ITIL With COBIT 4.0, 2007.

COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0, 2007.

COBIT Mapping: Mapping of ISO/IEC 17799:2005 With COBIT 4.0, 2006.

COBIT Mapping: Mapping PMBOK to COBIT 4.0, 2006.

COBIT Mapping: Mapping SEI's CMM for Software to COBIT 4.0, 2006.

COBIT Mapping to ISO/IEC 17799:2000 With COBIT, 2nd Edition May 2006.

COBIT Mapping Overview of International IT Guidance 2nd Edition, 2006.

MOF to COBIT/Val IT Comparison and Cross Implementation Guide: How to Leverage MOF in a COBIT/Val IT Environment, 2009.

http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=30523"

[ISO04] International Organization for Standardization (ISO): Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets. ISO/ IEC 15466, 2004.

[ISO04A] International Organization for Standardization (ISO): Information technology – Security techniques – Management of information and communications technology security. ISO/ IEC 13335, 2004.

[ISO05] International Organization for Standardization (ISO): International Standard for IT Service Management. ISO/ IEC 20000, 2005.

[ISO05A] International Organization for Standardization (ISO): Information technology – Security techniques – Information security management systems – Requirements. ISO/ IEC 27001, 2005.

[ISO05B] International Organization for Standardization (ISO): Information technology – Security techniques – Code of practice for information security management. ISO/ IEC 27002, 2005.

[ISO06] International Organization for Standardization (ISO): Ergonomie der Mensch-System-Interaktion. ISO/ IEC 9241, 2006.

[ISO07] International Organization for Standardization (ISO): Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit. ISO/ IEC 15408, 2007.

[ISO98] International Organization for Standardization (ISO): Information Technology. ISO/ IEC 2382, 1998.

[ISO98] International Organization for Standardization (ISO): Software Process Improvement and Capability Determination (SPICE). ISO/IEC 15504, 1998.

[ITGI07] IT Governance Institute (ITGI): Cobit 4.1. 2007. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[ITGI07a] IT Governance Institute (ITGI): IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance. ISACA, 2007. http://www.isaca.org

[ITGI08] IT Governance Institute (ITGI): The Val IT Framework 2.0. ISACA, 2008. http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx

[ITRC09] Identity Thief Resource Center (ITRC): Data Breaches in 2009. http://www.idtheftcenter.org/

[itSMF02] IT Service Management Forum Deutschland (itSMF): IT Service Management. Van Haren Publishing, 2002.

[JaEe06] Jantti, M.; Eerola, A.: A Conceptual Model of IT Service Problem Management. In International Conference on Service Systems and Service Management, 2006, 798-803, 2006.

[JaFa07] Jablonski, Stefan ; Faerber, Matthias: Integrated Management of Company Processes and Standard Processes: A Platform to Prepare and Perform Quality Management Appraisals. IEEE Computer Society, 2007.

[JiYu06] Jianjia, He; Yuhui, Ge; Guangyuan, Zhang: A Study on Organizational Change and IT Governance. Commercial Research, 17, 2006.

[Kain08] Kainz, Christoph: Anwendbarkeit von ITIL Incident Management im Bereich von IT-Betrieben des Banksektors. Magisterarbeit an der Technischen Universität Wien, 2008.

[Kams77] Kamschilow, M. M.: Das Leben auf der Erde – Evolution der Biosphäre. Harri Deutsch, 1977.

[KaZe66] Kalven, Harry, Jr.; Zeisel, Hans: The American Jury. Univ of Chicago Pr, 1966.

[Kee08] Kee, Jared: Social Engineering: Manipulating the Source. SANS Institute, Whitepaper, 2008.

[Kers09] Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung. Vieweg+Teubner; 2. Aufl., aktualisierte und erweiterte Aufl., 2009.

[KiBe06] Kiely, Laree; Benzel, Terry V.: Systemic Security Management. In: Security & Privacy, 4, 6, 74-77, 2006.

[Klai10] Klaic, Aleksandar: Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies. In: Office of the National Security Council MIPRO, 2010 Proceedings of the 33rd International Convention, 1203-1208, 2010.

[KlRi06] Kleiner, Fritz; Riegler, Günter: Workshop: Internes Kontroll-System. Stadtrechnungshof, Magistrat Graz Vermögens-und Finanzdirektion, 2006.

[KoCh95] Koehler, J. J.; Chia, A.; Lindsey, J. S.: The Random Match Probability (RMP) in DNA Evidence. Irrelevant and Prejudicial? In: Jurimetrics Journal, 35, 201-219, 1995.

[KoKu07] Kopperger, D.; Kunsmann, J.; Weisbecker, A.: Servicemanagement; Handbuch IT-Management. 2. überarbeitete. Aufl., Hanser Verlag, 2007.

[Kras06] Kraszka, Andrzej: Untersuchung alternativer Schnittstellen des Problem Managements nach ITIL. Diplomarbeit an der Universität Hannover, 2006.

[KrEh10] Krimmer, Robert; Ehringfeld, Andreas; Traxl, Markus: The Use of E-Voting in the Austrian Federation of Students

Elections 2009. In: Proceedings of the 4th International Conference on Electronic Voting, 33-44, 2010.

[Kres05] Kresse, Michael: IT Service Management Advanced Pocket Book. Fokus – ITIL Infrastructure Library. Serview GmbH; 1. Aufl., 2005.

[KrGa03] Kray, L. J.; Galinsky, A. D.: The debiasing effect of counterfactual mind-sets: Increasing the search for disconfirmatory information in group decisions.. In: Organizational Behavior and Human Decision Processes, 91, 69-81, 2003.

[Krim07] Krimmer, R: Machbarkeitsstudie. – Durchführung der Hochschülerinnen- und Hochschülerschaftswahlen mittels elektronischer Abstimmungsverfahren, 2007.

[KrEh10] Krimmer, R.; Ehringfeld, A., Traxl, M.: Die Einführung eines elektronischen Wahlkanals bei den ÖH-Wahlen. In: Pichler, J.: Überlegungen zur Hebung demokratischer Partizipation – Provokationen und Optionen. Neuer Wissenschaftlicher Verlag, Wien, 133-148, 2010.

[KrET10] Krimmer, R.; Ehringfeld, A.; Traxl, M.: Die Hochschülerinnen- und Hochschülerschaftswahlen 2009 mit E-Voting. In: Karl, B., Mantl, W., Piza, H., Poier, K., Prisching, M., Schilcher, B. (Eds.): Steirisches Jahrbuch für Politik 2009, 175-188, 2010.

[Krol05] Krolak-Schwerdt, Sabine: Sozialpsychologie der Liebe. Lehrstuhls für Sozialpsychologie an der Universität des Saarlandes, Vorlesungsunterlagen SS 2005. http://www.uni-saarland.de/fak5/wintermantel/media/SS2005/SPI/folien11.pdf

[Kuhn07] Kuhn, Janet: 6 Steps to Making Your Security Policies Work - ITIL v.3 Access Management. In: itSM Solutions, Vol. 3.33, August 2007. http://www.itsmsolutions.com/newsletters/DITYvol3iss33.htm

[Kurl95] Kurland, Nancy B.: Ethical Intentions and the Theories of Reasoned Action and Planned Behavior. In: Journal of Applied Social Psychology, 25, 4, 297-313, 1995.

[Lach07] Lachapelle, Eric: Control Objectives for Information and related Technology. White Paper, Veridion Inc., Montreal, Canada, 2007. http://www.veridion.net\ITIL+COBIT\cobit_en_wp.pdf

[LaKa00] Langlois, J. H.; Kalakanis, L.; Rubenstein, A. J.; Larson, A.; Hallam, M.; Smoot, M.: Maxims or myths of beauty? A meta-analytic and theoretical review. In: Psychological Bulletin, 126, 3, 390-423, 2000.

[LaMi10] Larrocha, E.R.; Minguet, J.M.; Di´ az, G.; Castro, M.; Vara, A.: Filling the gap of Information Security Management inside ITIL®: Proposals for posgraduate students. In IEEE Education Engineering (EDUCON), 2010, 907-912, 2010.

[Lari06] Laribee, Lena ; Barnes, David S.; Rowe, Neil C.; Martell, Craig H.: Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems. In: Proceedings of the 2006 IEEE, Workshop on Information Assurance, United States Military Academy, West Point, NY.

[Lauf04] Laufer, Jochen: Mitarbeitermotivation – Eine kritische Beurteilung betrieblicher Anreizsysteme. Diplomarbeit an der Fachhochschule Kaiserslautern, 2004.

[LePi10] Lemus, S.M.; Pino, F.J.; Velthius, M.P.: Towards a model for information technology governance applicable to the banking sector. In: 5th Iberian Conference on Information Systems and Technologies (CISTI), 2010, 1-6, 2010.

[Lerd06] Lerdorf, Rasmus; Tatroe, Kevin; MacIntyre, Peter: Programming PHP. O'Reilly, 2. Aufl., 2006.

[LiBa02] Li, N. P.; Bailey, J. M.; Kenrick, D. T.; Linsenmeier J. A.: The necessities and luxuries of mate preferences: Testing the trade-offs. In: Journal of Personality & Social Psychology, 82, 947-955, 2002.

[LiHe07] von der Linde, Boris; von der Heyde, Anke: Psychologie für Führungskräfte. Rudolf Haufe Verlag, 2007.

[LiTs09] Lin, J. Y.; Tsai, Y.; Tsai, Wu: Optimal capital investment, uncertainty and outsourcing. China Center for Economic Research, Peking University, National University of Kaohsiung, Taiwan.

http://www.eaber.org/intranet/documents/40/450/CCER Lin 03.pdf

[Mank07] Manko, Christian Peter: Aufbau und Untersuchung einer 10 Gbit/s Glasfaserübertragungsstrecke zur Übertragung digitalisier-ter Analogsignale mit hohen Bandbreiten. Diplomarbeit an der Fachhochschule Bonn-Rhein-Sieg, 2007.

[Mann08] Mann, Ian: Hacking the Human. Gower Publishing Limited, 2008.

[Marq08] Marquis, Hank: 11 Ways ITIL Improves Security. In: itSM Solutions, 4, 32, 2008. http://www.itsmsolutions.com/newsletters/DITYvol4iss32.htm

[McCo04] McConnell, Steve: Code Complete: A Practical Handbook of Software Construction. Microsoft Press, 2004.

[McDo09] McDowell, Mindi: Avoiding Social Engineering and Phishing Attacks. Cyber Security Tip ST04-014, Carnegie Mellon University, 2009. http://www.us-cert.gov/cas/tips/ST04-014.html

[MeFe03] Meng-Hsiang Hsu; Feng-Yang Kuo: An investigation of volitional control in information ethics. In: Behaviour Information Technology, 22, 1, 53-62, 2003.

[Mint92] Mintzberg, Henry: Five Ps for Strategy in The Strategy Process. Prentice-Hall International Editions, Englewood Cliffs NJ, 1992.

[MiSi02] Mitnick, Kevin D.; Simon, W. L.: The Art of Deception: Controlling the Human Element of Security. Wiley Verlag, 2002.

[MS08] Microsoft (MS): Microsoft Operations Framework (MOF). Version 4, 2010. http://technet.microsoft.com/en-us/library/cc506049.aspx

[NaRo08] Na-Yun, Kim; Robles, R.J.; Sung-Eon, Cho; Yang-Seon, Lee; Tai-hoon, Kim: SOX Act and IT Security Governance. In: International Symposium on Ubiquitous Multimedia Computing, UMC '08, 218-221, 2008.

[NaSa08] Nabiollahi, Akbar; bin Sahibuddin, Shamsul: Considering service strategy in ITIL V3 as a framework for IT Governance. In: International Symposium on Information Technology, ITSim, 1, 1-6, 2008.

[Nels06] Nelson, Rick: Methods of Hacking – Social Engineering. Paper, Institute for Systems Research, University of Maryland, 2006.

[Nerd03] Nerdinger, F. W.: Motivation von Mitarbeitern. Hogrefe Verlag, 2003.

[Newc61] Newcomb, Theodore Mead: The Acquaintance Process. Holt, Rinehart and Winston, 1961.

[Niel93] Nielsen, Jokob: Usability Engineering. Academic Press, 1993.

[NoMu03] Noopur, Davis; Mullaney, Julia.: The Team Software Process in Practice - A Summary of recent Results. Technical Report, CMU/SEI-2003-TR-014, ESC-TR-2003-014, 2003. http://www.sei.cmu.edu/reports/03tr014.pdf

[NoZe03] Nothcutt, Stephen; Zeltser, Lenny; Winters, Scott; Frederick, Karen Kent; Ritchey, Ronald W.: Network Perimeter Security. New Riders Publishing, 2003.

[NyHo07] Nyamsuren, E.; Ho-Jin Choi: Preventing Social Engineering in Ubiquitous Environment. In: Future Generation Communication and Networking, FGCN, 2, 573-577, 2007.

[OeH07] Hochschülerinnen- und Hochschülerschaft: Bedenken der ÖH Bundesvertretung zu E-Voting bei Hochschülerinnen- und Hochschülerschaftswahlen. September 2007.

[Oest00] Österreichisches Parlament: Datenschutzgesetz 2000 (DSG). Fassung vom 02.09.2010. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

[Oest09] Österreichisches Parlament: Sicherheitspolizeigesetz (SPG). Fassung vom 02.09.2010. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792

[Oest09a] Österreichisches Parlament: E-Government-Gesetz (E-GovG). Fassung vom 12.10.2009. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230&ShowPrintPreview=True

[Oest10] Österreichisches Parlament: Strafgesetzbuch (StGB). Fassung vom 30.12.2010. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296

[Oest98] Österreichisches Parlament: Hochschülerinnen- und Hochschülerschaftsgesetz 1998 (HSG 1998). Fassung vom 18.04.2011. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=1001011

[OFT09] Office of Fair Trading (OFT): The Psychology of Scams – Provoking and Committing Errors of Judgement. Erstellt durch University of Exeter School of Psychology, Mai 2009. http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf

[OGC05S] Office of Government Commerce (OGC): ITIL – Der Schlüssel für die Steuerung von IT Services: Für Service Support. Publiziert durch TSO (The Stationery Office Ltd.) für OGC, 2005.

[OGC07D] Office of Government Commerce (OGC): Service Design Book. 2. Aufl., TSO (The Stationery Office), 2007.

[OGC07I] Office of Government Commerce (OGC): Continual Service Improvement Book. 2. Aufl., TSO (The Stationery Office), 2007.

[OGC07L] Office of Government Commerce (OGC): The Official Introduction to the ITIL Service Lifecycle. 2. Aufl., TSO (The Stationery Office), 2007.

[OGC07O] Office of Government Commerce (OGC): ITIL Version 3 Service Operation. TSO (The Stationery Office), Mai 2007.

[OGC07S] Office of Government Commerce (OGC): Service Strategy Book. 2. Auflage, TSO (The Stationery Office), Mai 2007.

[OGC07T] Office of Government Commerce (OGC): Service Transition Book, 2. Auflage. TSO (The Stationery Office), Mai 2007.

[Open10] The Open Group: TOGAF Version 9. Enterprise Edition. http://www.opengroup.org/togaf/

[Otto03] Otto, Ulrich: Der Stellenwert von Reziprozität, Anmerkungen zu Austauschkalkülen in zwischenmenschlicher Hilfe. Aufsatz an der Universität Tübingen, Fakultät für Sozial- und Verhaltenswissenschaften, 2003.

[Paci94] Pacioli, Luca: Summa de Arithmetica, Geometria, Proportioni et Proportionalità. 1494, 2. Aufl. 1523.

[PeBe99] Perline, A. H.; Bertoliggi, S.; Lind, D. L.: The effects of women´s age and physical appearance on evaluations of attractiveness and social desirability. In: The Journal of Social Psychology, 139, 343-354, 1999.

[Petr07] Petrovic, Marc: Implikatoren und Wirkungen der Personenwahrnehmung in der Werbepsychologie. GRIN Verlag, 2007.

[Press09] Medienberichte: Spiegel Online http://www.spiegel.de/panorama/justiz/0,1518,615704,00.html, Sueddeutsche.de: http://www.sueddeutsche.de/panorama/445/463057/text/, DiePresse.at: http://diepresse.com/home/panorama/welt/464832/index.do

[QiJu10] Qian, Wang; Junde, Song; Lianru, Liu; Xiaoxiang, Luo; XinHua, E.: Building IT-based incident management platform. In 5th International Conference on Pervasive Computing and Applications (ICPCA), 2010, Dezember 2010, Seite 359-364.

[Raep01] Raepple, Martin: Sicherheitskonzepte für das Internet – Grundlagen, aktuelle Technologien, Methoden und Lösungskonzepte für die kommerzielle Nutzung. 2. Aufl. , dpunkt.Verlag, 2001.

[RaPf96] Rannenberg, K.; Pfitzmann, A.; Müller, G.: Sicherheit, insbesondere mehrseitige IT-Sicherheit. In: it+ti Informationstechnik und technische Informatik, 38, 4, 5-10, 1996.

[Raym03] Raymond, Eric: A Portrait of J. Random Hacker. In: The Jargon File, Version 4.4.7. http://www.catb.org/jargon/html/

[Real08] Realfsen, Asmund: Developing a Model for Conformity checking small and medium-sized Organizations with common IT Operations Standards. Diplomarbeit an der Technischen Universität Wien, 2008.

[Reas94] Reason, James: Menschliches Versagen – psychologische Risikofaktoren und moderne Technologien, Spektrum, 1994.

[Rega71] Regan, T. Dennis: Effects of Favor and Liking on Compliance. In: Journal of Experimental Social Psychology, 7, 6, 627-39, 1971.

[ReMu00] Reimann, Peter; Müller, Katja; Starkloff, Phillip: Kognitiv kompatibel? Wissensmanagement: Brückenschlag zwischen Technik und Psyche. In: ct, 4, 275, 2000.

[RhZe01] Rhodes, Gillian; Zebrowitzb, Leslie A.; Clark, Alison; Kalick, S. Michael; Hightower, Amy; McKay, Ryan: Do facial averageness and symmetry signal health? In: Evolution and Human Behavior 22, 31-46, 2001. http://homepage.mac.com/ryantmckay/EHB01.pdf

[Robe93] Roberts, D.W.: Evaluation Criteria for IT Security. In: Computer Security and Industrial Cryptography, State-of-the-Art-and-Evolution, ESAT-Course, 151-61, 1993,

[Roes02] Roessler, Thomas Gert: Identification and Authentication in Networks enabling Single Sign-On. Diplomarbeit an der Technischen Universität Graz, 2002.

[RoRi04] Roth, Volker; Richter, Kai; Freidinger, Rene: A PIN-entry method resilient against shoulder surfing. In: Proceedings of the 11th ACM conference on Computer and communications security, CCS '04, 236-245, 2004.

[Rose02] Von Rosenstiel, Lutz: Mitarbeiterführung in Wirtschaft und Verwaltung. Anstöße zur Ermutigung. Bayerisches Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen, 3. Aufl., 2002.

[Rowl07] Rowley, Jennifer: The wisdom hierarchy: representations of the DIKW hierarchy. In: Journal of Information Science, 33, 2, 163-180, 2007.

[SAICA09] South African Institute of Chartered Accountants (SAICA): The King Report on Corporate Governance

Zusammenfassung von King I, King II und King III Report

http://www.saica.co.za/TechnicalInformation/LegalandGovernance/King/tabid/626/language/en-ZA/Default.aspx

Ernst and Young: Final King III Synopsis. http://www.saica.co.za/Portals/0/Technical/EY%20Final%20King%20III%20Synopsis.pdf

PricewaterhouseCoopers: King´s Counsil. http://www.saica.co.za/Portals/0/documents/PWC%20Exec%20Guide%20to%20KING%20III.pdf

Deloitte: King III. http://www.saica.co.za/Portals/0/documents/Deloitte%20King%20III%20Brochure.pdf

KPMG: King III Summary. http://www.saica.co.za/Portals/0/documents/KPMG%20King%20III%20Summary.pdf"

[Sar02] Sarbanes, Paul: Sarbanes- Oxley Act 2002. http://www.legalarchiver.org/soa.htm

[SaSc09] Saltzer, Jerome H.; Schroeder, Michael D.: The Protection of Information in Computer Systems. http://web.mit.edu/Saltzer/www/publications/protection/

[SaSh08] Sahibudin, S.; Sharifi, M.; Ayat, M.: Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. In: Second Asia International Conference on Modeling & Simulation, AICMS, 749-753, 2008.

[ScFi08] Schulz-Hardt, S.; Fischer, P.; Frey, D.:Selective exposure to information: A new explanation based on argument evaluation. In: British Journal of Social Psychology, 49, 4, 871-881, 2010.

[Scha10] Schaub, Harald: Menschliches Versagen – Die Rolle des Faktors "Mensch" bei großtechnischen Katastrophen aus psychologischer Sicht. Institut für Theoretische Psychologie, Otto-Friedrich-Universität, 2010.

[Schm03] Schmidt, Tom: Analyse der Zusatzfunktionalitäten verschiedener Firewalls. Diplomarbeit an der Fachhochschule Zentralschweiz, 2003.

[Schn00] Schneier, Bruce: Crypto-Gram Newsletter. Mai 2000. http://www.schneier.com/crypto-gram-0005.html

[Schn01] Schneier, Bruce: Secret and Lies, Sicherheit in der vernetzten Welt. dpunkt.verlag / Wiley, 2001.

[Schn08] Schneier, Bruce: Social-Engineering Bank Robbery. Blog. 16. Jänner 2008. http://www.schneier.com/blog/archives/2008/01/socialengineeri.html

[Scho08] Schöllhuber, Marlene: Benchmarking von Projektmanagement mit Hilfe von Reifegrad- und Kompetenzmodellen. Diplomarbeit an der Technischen Universität Wien, 2008.

[Schu02] Schulz, B.: Die autoritäre Persönlichkeit – Aggression. Referat, 2002. Referenziert von http://www.stangl.eu/psychologie/definition/Autoritaet.shtml

[Schu05] Schuler, Heinz: Lehrbuch der Personalpsychologie. Hogrefe-Verlag, 2005.

[Schu97] Schulz, Daniela: Diversifikation von Unternehmungen, Überlegungen zur Vorteilhaftigkeit für die Kapitalgeber. Diplomarbeit an der Christian-Albrechts-Universität zu Kiel, 1997.

[ScMi08] Scheeres, J. W.; Mills, R. F.; Grimaila M. R.: Establishing the Human Firewall. Reducing an Individual’s Vulnerability to Social Engineering Attacks. In: 3rd International Conference on Information Warfare and Security, 2008.

[Semm09] Semmelhaack, Björn: Ein ganzheitliches Konzept für Informationssicherheit unter besonderer Berücksichtigung

des Schwachpunktes Mensch. Diplomarbeit an der Universität Hannover, 2009.

[ShSc07] Shadel D. P.; Schweitzer-Pak K. B.: The Psychology of Consumer Fraud. Dissertation an der University of Tilburg, 2007.

[Sieg09] Siegel, Daniel: On the New Threats of Social Engineering Exploiting Social Networks. Bachelorarbeit an der Technischen Universität München, 2009.

[Sieg99] Siegmund, Gerd: Technik der Netze. 4. neubearbeitete und erweiterte Aufl., Hüthig Verlag, 1999.

[Sing01] Singh, Simon: Geheime Botschaften - Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. dtv 2001.

[SIT08] Fraunhofer Institut für Sichere Informationstechnologie (SIT): Privatsphärenschutz in Soziale-Netzwerke-Plattformen. Technical Report, 2008. http://www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf

[SoPa03] Sofsky, Wolfgang; Paris, Rainer: Figurationen sozialer Macht. Autorität, Stellvertretung, Koalition. Leske und Budrich Verlag, 1993.

[Steph07] Stephan, Michael: LinkZero-footprint authentication system for national ID smart-cards. Diplomarbeit an der Technischen Universität Wien, 2007.

[StNa90] Straub, Detmar W.; Nance, William D.: Discovering and disciplining computer abuse in organizations. In: MIS Quarterly, 14, 1, 45-60, 1990.

[StWe98] Straub, D. W.; Welke, R. J.: Coping with systems risk – Security planning models for management decision-making. In: MIS Quarterly, 22, 441-469, 1998.

[SuSe11] Susanti, F.; Sembiring, J.: The mapping of interconnected SOA governance and ITIL v3.0. In International Conference on Electrical Engineering and Informatics (ICEEI), 2011, Seite 1-5, Juli 2011.

[Sunz88] Sunzu: Die Kunst des Krieges. Droemersche Verlagsanstalt, 1988.

[Swap77] Swap, Walter C.: Interpersonal Attraction and Repeated Exposure to Rewarders and Punishers. Personality and Social Psychology Bulletin, 3, 2, 248-251, 1977.

[TaCl10] Talib, S.; Clarke, N.L.; Furnell, S.M.: An Analysis of Information Security Awareness within Home and Work Environments. In: International Conference on Availability, Reliability and Security, ARES '10, 196-203, 2010.

[Tian07] Tiantian Qi: An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. In: IEEE Intelligence and Security Informatics, 152-159, 2007.

[Tim08] Tim, Peters: Exakte Erfassung der Behandlungsvariabilität durch den Einsatz standardisierter Patienten - Untersuchung in Hausarztpraxen am Beispiel des Kopfschmerzes. Studie der Universitätsklinik Düsseldorf, Leitung Prof. Dr. Heinz-Harald Abholz, 2008.

[Unbe01] Unbekannter Autor: A Proactive Defence to Social Engineering. SANS Institute, Whitepaper, 2001.

[US85] Regierung der Vereinigten Staaten: Trusted Computer Security Evaluation Criteria (Orange Book). http://csrc.nist.gov/publications/history/dod85.pdf

[Voss09] Voßbein, Reinhard: Normen und Standards für die IT-Sicherheit. UIMCert GmbH, Prüfstelle für die Norm ISO/IEC 27001.

[Vuci09] Vucievic, Stevica: Release Management in Betrieben – Projekt- und Prozesshafte Umsetzung von ITIL Release Management in einer österreichischen Großbank. Diplomarbeit an der Technischen Universität Wien, 2009.

[Weil08] Weil, Steven: How ITIL Can Improve Information Security. Blog Eintrag in Zen One, 27. Mai 2008. http://blog.zenone.org/2009/05/how-itil-can-improve-information.html

[WePo06] Webb, P.; Pollard, C.; Ridley, G.: Attempting to Define IT Governance: Wisdom or Folly? In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS), 2006, Seite 194a, Jänner 2006.

[Whit03] Whittaker, J.: Why secure applications are difficult to write. In: Security & Privacy, 1, 2, 81-83, 2003.

[WiDe95] Winkler, Ira S.; Dealy, Brian: Information Security Technology?...Don't Rely on It – A Case Study in Social Engineering. In: Proceedings of the Fifth USENIX UNIX Security Symposium, 1, 1995.

[WiWa06] Wiedenbeck, Susan; Waters Jim; Sobrado, Leonardo; Birget, Jean-Camille: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: Proceedings of the working conference on Advanced visual interfaces, AVI '06, ACM, 177-184, 2006.

[WoHo10] Wondracek, Gilbert; Holz, Thorsten; Kirda, Engin; Krügel, Christopher: A Practical Attack to De-anonymize Social Network Users. In: Symposium on Security and Privacy, 223-238, 2010.

[Wole08] Wolek, Heinz: Faktor Mensch in der IT-Sicherheit. Books on Demand, 2008.

[Worc75] Worchel, S.: Effects of supply and demand on ratings of objective value. In: Journal of Personality and Social Psychology, 32, 906-914, 1975.

[Yarm00] Yarmouk: Sozialpsychologie. In: Vorlesung an der Universität Wien, WS 08/09, Vortragender Andreas Olbrich-Baumann, verweisend auf Yarmouk, 2000.

[Zhan10] Zhang, Ying: Information Security Governance mit COBIT, ITIL und ISO 27002. Masterarbeit an der Otto-von-Guericke-Universität Magdeburg, 2010.

[ZhYu11] Jian Zhang; Wei-hua Yuan; Wen-jing Qi: Research on security management and control system of information system in IT governance. In: International Conference on Computer Science and Service System, CSSS, 668-673, 2011.

[Zins07] Zins, Chaims: Conceptual Approaches for Defining Data, Information, and Knowledge. In: Journal of the American Society for Information Science and Technology, 2007. http://www.success.co.il/is/zins_definitions_dik.pdf

[ZSI89] Zentralstelle für Sicherheit in der Informationstechnik (ZSI): IT-Sicherheitskriterien, Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik, 1. Fassung vom 11.1.1989.

[Zwat06] Zwattendorfer, Bernd: Single Sign-On unter Verwendung der Bürgerkarte. Magisterarbeit an der Technischen Universität Graz, 2006.

## Webseiten

[APMG] APM Group: http://www.apmgroup.co.uk

[AIRMIC] Association of Insurance and Risk Managers (AIRMIC): http://www.airmic.com/

[ALARM] The Public Risk Management Association (ALARM): http://www.alarm-uk.org/

[COSO] Committee of Sponsoring Organizations of the Treadway Commission (COSO): http://www.coso.org/

[IRM] The Institute for Risk Management: http://www.theirm.org/

[ISACA] Information Systems Audit and Control Association (ISACA): http://www.isaca.org/

[ISO] International Organization for Standardization (ISO): http://www.iso.org/

[ITGI] IT Governance Institute (ITIG): http://www.itgi.org/

[itSMF] IT Service Management Forum. Gegründet 1991: http://www.itsmf.de/

[NTRSA] National Treasury der Republik Südafrika: http://www.treasury.gov.za/

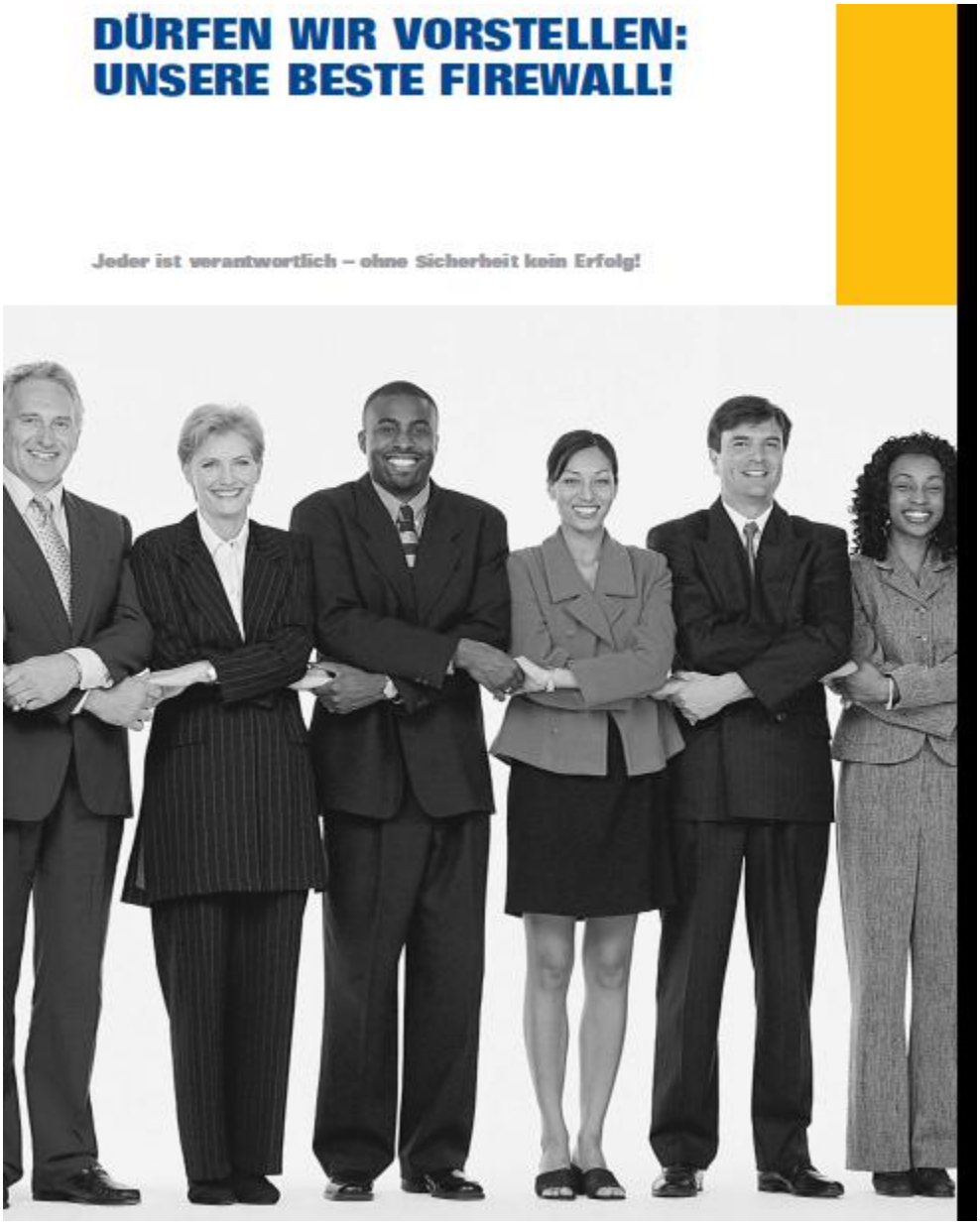
[OeBK] Die Österreichische Bürgerkarte: http://www.buergerkarte.at/

[OGC] Office of Government Commerce (OGC): http://www.ogc.gov.uk/

[theNSA] The National Speakers Association: http://www.nsaspeaker.org/

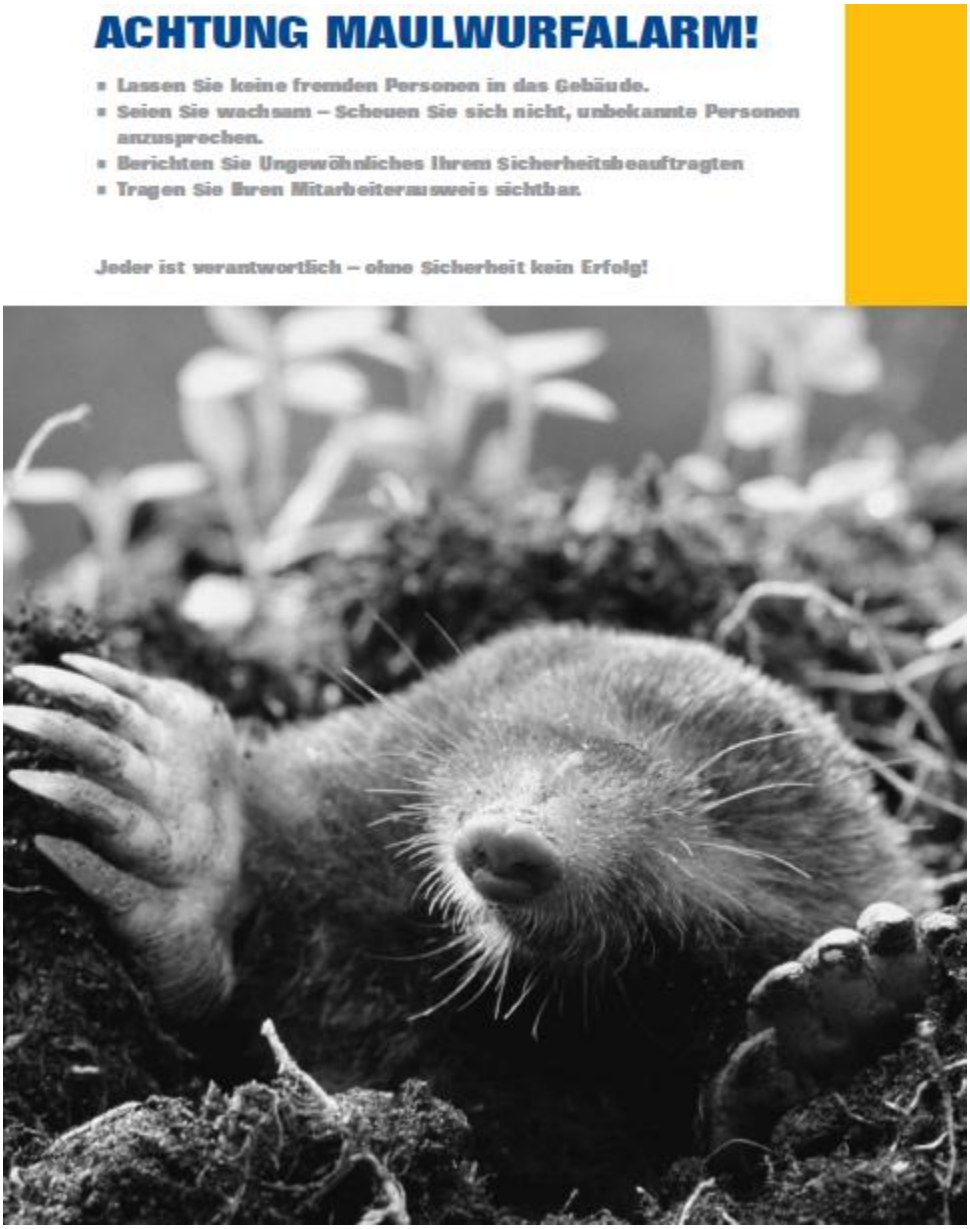
# Anhang

## Beispiele von Security Awareness Poster




Copyright SAP,

http://www.sap.com/




Copyright SAP,

http://www.sap.com/

Achtung Maulwurfalarm!

- Lassen Sie keine fremden Personen in das Gebäude
- Seien Sie wachsam – Scheuen Sie sich nicht, unbekannte Personen anzusprechen
- Berichten Sie ungewöhnliches Ihrem Sicherheitsbeauftragten
- Tragen Sie Ihren Mitarbeiterausweis sichtbar

Jeder ist verantwortlich – ohne Sicherheit kein Erfolg!

# Lebenslauf

***Dipl. Ing. Mag. Andreas Ehringfeld***

| | |
|---|---|
| Adresse: | 2463 Stixneusiedl, Neufeldergasse 13 |
| Telefon: | 0664 60 8444 1026 |
| E-Mail: | andreas@ehringfeld.at |
| Geburtsdatum: | 5. April 1979 |
| Geburtsort: | Mödling |
| Staatsbürgerschaft: | Österreich |

**Schulbildung**

| | |
|---|---|
| 1997 | Bundesrealgymnasium Bruck an der Leitha (Matura) |

**Akademische Laufbahn**

| | |
|---|---|
| 2004 | Abschluss des Studiums der Informatik an der Technischen Universität Wien |
| 2007 | Abschluss des Studiums Informatik Management an der Technischen Universität Wien |

**Berufserfahrung**

| | |
|---|---|
| Seit 2002 | Wissenschaftlicher Mitarbeiter und Lehrbeauftragter an der Technischen Universität Wien |
| Seit 2002 | Operations Specialist, IT-Security Expert, IT-Consultant |

**Sprachkenntnisse**

Deutsch (Muttersprache)

Englisch (Verhandlungssicher)