Piller

TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

MASTERARBEIT

IT - Security Management für Klein- und Mittelbetriebe

ausgeführt am Institut für

Softwaretechnik und Interaktive Systeme

der Technischen Universität Wien

unter der Anleitung von

Univ.Doz. DI Dr. Ernst Piller

durch

Gernot Deischler

Simmeringer Hauptstrasse 119/3/12

1110 Wien

28.04.2008
Datum

Gernot Deischler
Unterschrift (Student)

Danksagung

Diese Masterarbeit möchte ich meinen Eltern widmen, die mich während des gesamten Studiums emotional und finanziell unterstützten.

Weiters möchte ich mich bei meiner Freundin Katharina für das Verständnis und die seelische Unterstützung bedanken.

IT – Security Management für Klein- und Mittelbetriebe

Zusammenfassung

Diese Arbeit bietet eine fundierte Aufbereitung von IT - Sicherheitsmaßnahmen, die auf Klein- und Mittelbetriebe bezogen sind. Die IT – Sicherheitsmaßnahmen werden theoretisch aufgearbeitet und es wird ein Instrument entwickelt, mit dem eine fundierte Sicherheitsanalyse durchgeführt werden kann.

Ausgangspunkt für die Sicherheitsanalyse des Unternehmens ist ein Fragebogen, mit dem das Sicherheitsniveau des Unternehmens bestimmt wird. Aufgrund der gewählten Antworten im Fragebogen werden konkrete Sicherheitsmaßnahmen vorgeschlagen, die im jeweiligen Betrieb umgesetzt werden sollten.

Weiters ist dieses Werk zu Trainingszwecken für Unternehmensverantwortliche einsetzbar, damit diese gegenüber dem Thema IT – Security sensibilisiert werden.

Inhaltsverzeichnis

1 Aufgabenstellung

Ziel dieser Diplomarbeit ist es, die wichtigsten Aspekte der IT – Security für Klein- und Mittelbetriebe aufzuzeigen. Weiters ist diese Arbeit dazu gedacht, den Verantwortlichen der angesprochenen Unternehmen gegenüber der IT – Security zu sensibilisieren.

Neben der theoretischen Aufarbeitung der IT – Sicherheitsmaßnahmen, ist es das Ziel ein Instrumentarium zu entwickeln, mit dem der jeweilige Verantwortliche, ein für seinen Betrieb maßgeschneidertes Sicherheitskonzept entwickeln kann. Die beiden Kernpunkte dieses Werkzeuges sind eine Fragetabelle, mit der das Sicherheitsniveau ermittelt wird, und ein Maßnahmenkatalog mit präzisen Verhaltensregeln.

2 Einleitung

Dem Bereich IT – Security wird von vielen kleineren Unternehmen zu wenig Aufmerksamkeit geschenkt. Es wird noch übersehen, dass IT – Security ein wesentliches Kriterium für den Unternehmenserfolg darstellt. Diesen Unternehmen ist auch nicht bewusst, welches Risiko Hackangriffe, Serverausfälle oder Datendiebstahl darstellen. Laut einer Studie vom Austrian Security Forum verwenden Klein- und Mittelbetriebe (KMU) in Österreich veraltete Betriebssysteme, verschlüsseln ihre W-Lan Verbindungen nicht und haben keine räumliche Trennung zwischen Server- und Archivräume. [1]

> Während es für die meisten KMUs selbstverständlich ist, zum Beispiel ihr Lager zuzusperren, vernachlässigen die meisten die Fragen der IT – Security und setzen sich damit unnötigen existenziellen Gefahren aus.
>
> *Hans-Jürgen Pollirer, Obmann der Bundessparte „Information und Consulting“ der Wirtschaftskammer Österreich*

Mit Hilfe der folgenden Kapitel wird versucht den Verantwortlichen[1] der KMUs auf die diversesten Gefahren im IT – Bereich hinzuweisen. Als Einstiegspunkt für die Sicherheitsanalyse dient der Fragebogen im Kapitel 4. Mit Hilfe des Fragebogens kann man die Schutzmaßnahmen, die auf dem deutschen Grundschutzhandbuch aufbauen, bestimmen.

[1] Geschlechtsneutrale Formulierung:
Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, zum Beispiel Verantwortlicher/Verantwortliche oder Absender/In verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

3 Grundlagen

3.1 Grundbegriffe der IT-Security

In diesem Kapitel werden die Grundbegriffe der IT – Security erklärt, die dem besseren Verständnis der folgenden Kapitel dienen.

IT – Security ist der Oberbegriff für *Safety* (Funktionssicherheit, Schutz vor Fehlfunktionen des Systems bzw. Sicherheit für die Umgebung eines Informationssystems), *Security* (Informationssicherheit, Schutz vor ungültigen Systemzuständen), *Protection* (Datensicherung, Schutz vor Datenverlust) und *Privacy* (Datenschutz). [10]

Die IT – Security hat folgende Hauptziele:

1. Authentizität:
   Gibt Auskunft darüber, ob die Glaubwürdigkeit und Echtheit einer Person oder eines Dienstes nachweisbar ist.
2. Integrität:Gibt Auskunft darüber, ob Daten unbemerkt verändert wurden bzw. ob alle Änderungen nachvollziehbar sind.
3. Verfügbarkeit:Gibt Auskunft darüber, ob der Zugriff auf Daten bzw. auf das System innerhalb eines gewissen Zeitrahmens gewährleistet ist.
4. Vertraulichkeit:Gibt Auskunft darüber, das Daten nur von autorisierten Benutzern gelesen bzw. modifiziert werden dürfen.

Neben diesen Hauptzielen sind noch, je nach Anforderung bzw. Anwendung, folgende Ziele von Bedeutung:

- Anonymität:
  Bei gewissen Anwendungen, vor allem im Internet, gewinnt dieser Punkt immer mehr an Bedeutung (Ohne Schutzmaßnahmen gibt man beim Surfen im Internet Information, wie eigene IP – Adresse, Betriebssystem, Browser, etc., preis).
- Nicht – Anfechtbarkeit:
  Dieser Punkt hat vor allem Geltung beim E – Mail Verkehr. Es soll ein Nachweis geliefert werden, dass die Information abgesendet und auch beim Empfänger angekommen ist.
- Verbindlichkeit/Nachvollziehbarkeit:
  Der Urheber von Änderungen an Dokumenten/Daten darf diese nicht abstreiten können und die Änderungen müssen erkennbar sein.

- Zugriffssteuerung:
  Der Zugriff auf Dateien, IT – Komponenten und IT – Systeme muss geregelt sein.

  Die Prioritäten der IT – Security sind folgende Punkte: [12]

  - Gesetzliche Anforderungen erfüllen (Compliance)
  - Geschäftsbetrieb aufrecht erhalten (Business Continuity)
  - Datenlecks abdichten (Information Leakage Prevention)
  - Viren und Spyware abwehren
  - Benutzerverwaltung (Identity Management)
  - Einbruchsabwehr (Intrusion Detection / Prevention)
  - Content- und Spam-Filterung

4 Fragenkatalog

Durch die folgenden Fragen kann man das Sicherheitskonzept festlegen. Die Sicherheitsmaßnahmen 5.1.1 bis 5.1.81 sind allgemein gültig und sind einzuhalten. Bei den Fragen von 1 - 4 mit den jeweiligen Unterfragen gelten bei Zutreffen die jeweiligen Sicherheitsmaßnahmen.

1. Haben Sie ein Netzwerk im Einsatz? Wenn ja, welche der folgenden Punkte treffen auf Sie zu?		Von 5.2.1 bis 5.2.17
• Internet		Von 5.2.18 bis 5.2.36
• WLAN		Von 5.2.37 bis 5.2.39
• Mailserver		Von 5.2.40 bis 5.2.42
• Webserver		Von 5.2.43 bis 5.2.45
• Datenbankserver		Von 5.2.46 bis 5.2.49
• Proxyserver		5.2.50
2. Haben Sie mobile Systeme im Einsatz? Wenn ja, welche der folgenden Geräte haben Sie im Einsatz?		Von 5.3.1 bis 5.3.4
• Laptop		Von 5.3.5 bis 5.3.9
• Mobiltelefon		Von 5.3.10 bis 5.3.11
• PDA		5.3.12
3. Benötigen Sie für Ihr Unternehmen erhöhte Sicherheit?		Von 5.4.1 bis 5.4.18
4. Benötigen Sie für Ihren Betrieb erhöhte Verfügbarkeit?		Von 5.5.1 bis 5.5.3

5 Maßnahmen

Im folgenden Kapitel sind die Maßnahmen beschrieben, die einzuhalten sind. Jede Beschreibung einer Maßnahme schließt mit einem oder mehreren Gefahrenpunkten ab, die bei Zuwiderhandlung auftreten können. Die Gefahrenpunkte sind an der etwas kleineren Schrift ersichtlich.

5.1 Grundlegende Sicherheitsmaßnahmen

In diesem Kapitel werden die Sicherheitsmaßnahmen beschrieben, die jeder Betrieb einzuhalten hat.

5.1.1 Wahl des Standortes

Falls der Standort des Unternehmens noch zu wählen ist bzw. ein neuer Standort entstehen soll, sind folgende Punkte zu beachten:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen.
- Gebäude, die direkt an Hauptverkehrstrassen (Bundesbahn, Autobahn, Bundesstraße) liegen, können durch Unfälle beschädigt werden.
- Die Nähe zu optimalen Verkehrs- und somit Fluchtwegen kann die Durchführung eines Anschlages erleichtern.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z. B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.

Auflistung, Quelle siehe [4]

5.1.2 Grundstückspezifische Sicherheitsmaßnahmen

Eine äußere Umschließung des Grundstücks durch z.B. einen Zaun oder Mauer ist empfehlenswert. Weitere Maßnahmen zur Sicherung des Grundstücks sind u.a.

1. Zufahrtssperren
2. Beleuchtung des Grundstücks und des Gebäudes
3. Videoüberwachung und Bewegungsmelder im Außenbereich des Gebäudes
4. Videogegensprechanlage am Eingang

- Einbruch und Diebstahl

5.1.3 Blitzschutz

Zusätzlich zu einem äußeren Blitzschutz, wie Blitzableiter, ist ein innerer Blitzschutz (Überspannungsschutz) erforderlich. Auflagen von Behörden und Versicherung sind hinsichtlich Blitzschutzes zu erfüllen.

- Schaden der IT - Infrastruktur durch Blitzschlag

5.1.4 Diebstahlschutz

Bei Abwesenheit von Mitarbeitern sind Fenster und Türen stets zu schließen. Bei nicht abschließbaren Büros, wie Großraumbüros, haben die Mitarbeiter bei Verlassen ihres Arbeitsbereichs wichtige Unterlagen, transportable IT - Geräte und Datenträger zu verschließen. Des Weiteren ist der Rechner runter zufahren bzw. bei kurzzeitigen Verlassen ist der Rechner mit Passwort - geschützten Bildschirmschoner zu versehen.

- Diebstahl von IT - Geräten
- Einfacher Zugang zu firmeninternen Information (z.B. Diebstahl von Datenträger oder Kopieren der Daten von Medien)

5.1.5 Einbruchschutz

Es ist auch zu klären, welcher Raum in welchem Maß schutzbedürftig ist, aber auch welche IT - Systeme im Gesamten (z.B. Rechner, Mobiltelefon, etc), Teile von IT - Systemen (z.B. Drucker, SIM - Karten, etc.) oder Betriebsmittel (Toner, Ladegeräte etc.) schutzbedürftig sind. Da Einbrecher ihr Ziel nach dem Gesichtspunkt auswählen, wie hoch das Risiko und Aufwand zum erwarteten Gewinn sind, sollte man versuchen den Aufwand für den Einbruch so zu erhöhen, damit sich dieser nicht mehr lohnt. Die wesentlichen Maßnahmen um den Aufwand für den Einbrecher zu erhöhen sind folgende:

- Rollladensicherungen bei einstiegsgefährdeten Türen oder Fenster,
- besondere Schließzylinder, Zusatzschlösser und Riegel,

- Sicherung von Kellerlichtschächten,
- Verschluss von nichtbenutzten Nebeneingängen,
- einbruchgesicherte Notausgänge (soweit seitens der örtlichen Bauaufsicht zugelassen),
- einbruchhemmende Türen, beispielsweise in der Qualität ET1 oder höherwertig, wenn die Gefährdungslage es erforderlich macht,
- Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit
  Auflistung, Quelle siehe [4]

- Einbruch

5.1.6 Brandschutz

Regionale Brandschutzvorschriften, wie Feuerpolizeiverordnungen, müssen eingehalten werden. Man sollte darauf achten, dass in Räumen mit hoher IT - Infrastruktur keine leicht brennbaren Materialien gelagert werden bzw. sich nicht viele Materialien mit hohem Brennwert befinden (z.B. Serverraum nicht als Aktenarchiv verwenden). Zusätzlich sollte man Brandmelder und Rauchmelder installieren, dabei ist zu beachten, dass die Melder von Außen lokalisiert werden kann. Die Brandmelder gehören regelmäßig gewartet. Neben dem Brandschutz sollte man auch auf den Rauchschutz achten. Es sollten regelmäßig Brandschutzbegehungen gemacht werden, bei denen u.a. kontrolliert wird, ob Fluchtwege nicht blockiert sind, Brandschutztüren oder Rauchschutztüren nicht durch Keile offen gehalten werden, alle Rauchmelder funktionstüchtig sind etc.

Die folgenden Empfehlungen sollten zum Rauchschutz berücksichtigt werden: [4]

- Brandschutztüren sollten Rauchschutzqualität aufweisen.
- Rauchschutztüren in Fluren sollten durch Rauchschalter gesteuert werden. Solche Türen können immer offen stehen, da sie bei Rauchdetektion selbsttätig schließen.
- Die Lüftungsanlage bzw. die Klimaanlage sollte eine Entrauchung von IT-Räumen gestatten.
- In Klimakanälen (Zu- und Abluft) sollten Kanalmelder installiert sein.
- In der Frischluftansaugung sollten Melder installiert sein, die automatisch diese sperren, wenn Störgrößen (Rauch) erkannt werden.

- Stärkere Brandentwicklung
- Eine Lokalisierung der Brandstelle ist nicht möglich
- Keine rechtzeitige Branderkennung möglich

- Personenschaden
- Schaden an IT - Infrastruktur

5.1.7 Dokumentation der Versorgungsleitungen

Vollständige Dokumentation der Versorgungsleitungen ist sinnvoll. Man sollte auch versuchen die Versorgungspläne immer auf dem aktuellem Stand zu halten.

Folgende Details sind aufzunehmen: [4]

- genaue Führung der Leitungen (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- genaue technische Daten (Typ und Abmessung),
- evtl. vorhandene Kennzeichnung,
- Nutzung der Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,

Verteiler sollten neutral dokumentiert werden, es sollten keine Hinweise auf Nutzungsart der Leitungen gegeben werden.

- Bei Umbauarbeiten ist Verletzung der bestehenden Leitung möglich
- Erschwerung von Modifikation, da man nicht den Überblick über bisherige Versorgungsleitungen hat
- Im Notfall keine rasche, effiziente Lokalisierung der Schadstelle

5.1.8 Dokumentation Infrastruktur- und Baupläne

Nach jeder Umbaumaßnahme und Erweiterung sind die Baupläne, Fluchtwegpläne etc. am neuesten Stand zu bringen.

- Im Schadensfall ev. kein Versicherungsschutz
- Im Notfall keine geeigneten Pläne zur Fehlerlokalisierung
- Erschwerung von Modifikation, da man nicht den Überblick über bisherige Tätigkeiten hat

5.1.9 Beurteilung der Lage von schützenswerten Gebäudeteilen

Schützenswerte Gebäudeteile sollten nicht an besonders gefährdeten Stellen untergebracht sein. Beispiele für gefährdete Stellen sind:

- Keller, wegen möglichen Wassereinbruch
- Räume im Erdgeschoss zu öffentlichen Verkehrsflächen hin, wegen erhöhter Einbruchsgefahr und Gefahr des Vandalismus

Als Faustregel sollte gelten, je weiter der schützenswerte Raum im Inneren des Gebäudes ist, desto besser.

- Einfacher Einstieg in das Gebäude
- Bei heftigem Regen kommt es zu Wassereinbruch im Keller

5.1.10 Vermeidung von Lagehinweisen

Man sollte, soweit wie möglich, auf Lagehinweise auf schützenswerte Gebäudeteile (wie Serverraum, Chefbüro, Archiv...) verzichten. Die Verzichtung der Beschilderung bezieht sich, sowohl auf das Innere des Gebäudes, als auch auf das Äußere.

- Bei Einbruch leichtes Spiel für den Dieb schützenswerte Räume zu finden
- Bei Publikumsverkehr erleichterte Möglichkeiten schützenswerte Räume zu finden um Diebstahl zu begehen bzw. einen Schaden an Geräten in schützenswerten Räumen zu tätigen

5.1.11 Verwaltung von physikalischen Schlüsseln

Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind gesichert aufzubewahren. Einen bestimmten Schlüssel ist nur jener Personen auszuhändigen, die diesen zur Ausübung ihrer Funktion benötigt (siehe Kapitel 5.1.21). Die Ausgabe ist zu dokumentieren, von der erhaltenden Person ist die Schlüsselübergabe zu quittieren und bei Entzug des Zugangsrechtes (z.B. Ausscheiden aus dem Unternehmen) ist der Schlüssel wieder einzuziehen. Bei Verlust oder Diebstahl von Schlüsseln ist entsprechend zu reagieren (z.B. Austausch von Schlössern etc.).

- erleichterter Einbruch
- Diebstahl

5.1.12 Diebstahlsicherungen

Zu jedem Raum mit schützenswerten IT - Systemen sollten nur Befugte Zutritt haben und eine geeignete Zutrittskontrolle ist umzusetzen. Des Weiteren sollten auch Peripherie - Geräte des IT - Systems gesichert werden. Je nach schützenswertem Gut sollte man sich überlegen, ob man einen mechanischen (z.B. Schloss, Kette, etc.), elektronischen (akustischer Abschreckungsalarm, etc.) oder einen softwaremäßigen Schutz (Verschlüsselung bei Benutzung eines Wechselmediums, etc.) zur Sicherung einsetzt.

- Datendiebstahl
- Diebstahl des IT - Systems oder Teilen davon

5.1.13 Bereitstellung einer ausreichenden Stromversorgung

Die Elektroinstallation sollte zu jedem Zeitpunkt für die versorgten Geräte ausreichend sein, daher sind laufende Kontrollen durchzuführen und die Elektroversorgung ist an die Anzahl der angeschlossen Geräte anzupassen.

- Zusammenbruch des Stromnetzes wegen Überlastung (mehr IT - Geräte angeschlossen als vorgesehen)

5.1.14 Wahl eines geeigneten Kabeltyps

Es ist entscheidend, dass man für die jeweilige Begebenheit den richtigen Kabeltyp wählt, z.B. Unterscheidung zwischen Kabel für den Innen- oder Außenbereich; Kabel in einem feuergefährdeten Bereich etc.

- Funktionalität eines Kabels in „kabelfremden“ Bereichen nicht gegeben

5.1.15 Sicherung von Leitungen

Die Verlegung der Leitungen unter Putz oder in mechanisch festen und abschließbaren Kanälen ist empfehlenswert. Ebenso wichtig ist der Verschluss von Verteilern und beim Verschluss sind die Zutrittsrechte möglichst streng zu vergeben. Man sollte auch darauf achten, dass schützenswerte Leitungen eine möglichst geringe Länge aufweisen. Wasserführende Leitungen, wie Wasserleitungen, Heizungsrohre, sollten überhaupt in Bereichen mit hoher IT - Infrastruktur vermieden werden. Bei unbedingter Erforderlichkeit von Wasserleitungen sollten Vorkehrungen getroffen werden den Wassereintritt zu minimieren. Heizungsrohre sollten bei Nichtbenützung durch ein Ventil geschlossen werden.

- Einfaches Herauslesen von Daten von nicht materiell gesicherten Datenleitungen
- Unproblematischer Zugang von Unbefugten zum Verteiler zwecks Manipulation von Daten
- Gefährdung von externen Personen bei Publikumsverkehr bzw. Mitarbeitern wegen herumhängender Kabel
- Zerstörung von IT - Infrastruktur durch Wassereinbruch

5.1.16 Abschaltung des Stroms im Notfall

Eine Installation eines Not-Aus-Schalters ist empfehlenswert. Diese Not-Aus-Schalter sollten gegen unbeabsichtigte Betätigung gesichert sein.

- Bei entstehenden Bränden ist kein Wegschalten der elektrischen Energie möglich

5.1.17 Bereitstellung eines Handfeuerlöschers

Es sind Handfeuerlöscher in ausreichender Zahl und Größe erforderlich. Bei elektronisch gesteuerten Geräten sind Kohlendioxyd - Löscher empfehlenswert (Pulverlöscher nicht verwenden). Über den Standort des Feuerlöschers sollten die Mitarbeiter Bescheid wissen. Des Weiteren ist über die Handhabung des Feuerlöschers eine Einschulung notwendig.

- Sofortige Brandbekämpfung nicht möglich
- Mögliche Ausbreitung kleiner Brandherde
- Löschschäden bei Einsatz von Pulverlöschern unverhältnismäßig hoch

5.1.18 Richtige Kabelführung

Grundsätzlich sind alle Kabel so zu verlegen, dass sie vor mechanischer Beschädigung geschützt sind. Wenn möglich sind sie in dafür vorgesehene Kabelschächte zu verlegen.

In Bereichen mit hoher Brandgefahr sollten Kabeln generell vermieden werden.

Weiters sollten alle Kabel vor Zugriff durch Fremde geschützt werden.

Leitungen die im Freien verlegt werden müssen gegen sind gegen Witterungseinflüsse abzusichern.

- Beschädigung von Leitungen
- Sabotage der Leitungen
- Ausfall des Netzwerks, oder des Stromnetzes
- Diebstahl von Informationen

5.1.19 Zutrittsregelung

Wie in Kapitel 5.1.21 beschrieben, sind Zutrittsberechtigungen je nach Funktion zu verteilen. Man muss außerdem regeln für welchen Raum bzw. welche Räume und für welchen Zeitraum diese Zutrittsberechtigungen gelten Bei Bedarf kann man die Zutritte mitprotokollieren.

- Diebstahl
- Datendiebstahl

5.1.20 Verantwortlichkeiten für den IT - Einsatz und IT - Sicherheit

Für den „IT-Einsatz“ ist eine Festlegung der Fachverantwortung und der Betriebsverantwortung vorzunehmen. Der Fachverantwortliche ist zuständig für die Erarbeitung der fachlichen Vorgaben, die es in einem IT-Verfahren umzusetzen gilt.

Hingegen umfasst die Betriebsverantwortung unter anderem folgende Aufgaben: [4]

- Datenerfassung,
- Arbeitsplanung und -vorbereitung,
- Datenverarbeitung,
- Nachbereitung von Datenausgaben,
- Datenträgerverwaltung und
- Überwachung des Verfahrensbetriebes.

Übergreifende Regelungen zur ÏT-Sicherheitäls ein Aspekt des IT-Einsatzes müssen verbindlich festgelegt werden. Es empfiehlt sich, Regelungen über

- Datensicherung,
- Datenarchivierung,
- Datenträgertransport,
- Datenübertragung,
- Datenträgervernichtung,
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
- Gebrauch von Passwörtern,
- Zutrittsberechtigungen,
- Zugangsberechtigungen,
- Zugriffsberechtigungen,
- Betriebsmittelverwaltung,
- Kauf und Leasing von Hardware und Software,
- Wartungs- und Reparaturarbeiten,
- Software: Abnahme und Freigabe,
- Software: Anwendungsentwicklung,
- Datenschutz,
- Schutz gegen Computer-Viren,
- Revision,
- Notfallvorsorge und
- Vorgehensweise bei der Verletzung der Sicherheitspolitik

zu treffen.

Daneben dürfen die Regelungen für Informationssicherheit nicht vernachlässigt werden. Diese sollten mit denen für IT-Sicherheit und auch Geheimschutz in geeigneter Weise zusammengeführt werden. Hierzu gehören beispielsweise:

- geeigneter Umgang mit geschäftskritischen Informationen,
- Vertraulichkeitsvereinbarungen,
- Einbeziehung des Sicherheitsbeauftragten bei Aufträgen und Projekten, die geschäftskritische Informationen betreffen,
- Unterrichtungen über den geeigneten Umgang mit geschäftskritischen Informationen, beispielsweise im Kontakt mit Kunden oder auf Reisen.

5.1.21 Personelle Regelungen

Es ist zu festzulegen welche Person für welche Funktion zuständig ist (z.B. Wer hat Rechteverwaltung inne; Wer ist zuständig für Datenerfassung, Netzadministration, Programmierung etc.). Man sollte versuchen operative und kontrollierende Funktionen zu trennen (z.B. Programmierer der Buchhaltung sollte nicht gleichzeitig Datenerfasser für Buchhaltung und kontrollierendes Organ der Buchhaltung sein).

Entsprechend der vergebenen Funktion sollte die jeweilige Person nur Zutrittsrechte zu jenen Räumlichkeiten bekommen, die für die Ausübung dieser Funktion benötigt werden. Mit Zugangsrechten und Zugriffsrechten ist ähnlich zu verfahren (z.B. Zugang zu bestimmten IT - Systemen wie Server, Zugriff auf bestimmte IT - Anwendungen oder Daten etc.). Die Zutritts-, Zugriffs- und Zugangsrechte sollten, von einer jeweiligen zentralen Stelle, vergeben, dokumentiert, kontrolliert und gegebenenfalls wieder entzogen werden. Bei diesen Rechten sind Vertretungsregeln festzulegen.

- Keine klare Unternehmensstruktur
- Ausführendes Organ kontrolliert sich selber
- Keine rechtzeitige Wartung, dadurch Beeinträchtigung der Funktionsfähigkeit des Betriebssystem und ev. Verlust des Versicherungsschutzes
- Jeder hat Zugang und Zutritt zu allem
- Keine klaren Verantwortlichkeiten
- „Alte“ Zugangsberechtigungen und Zutrittsberechtigungen gelten immerfort (z.B. ausgeschiedene Person hat noch immer Zugang ins firmeninternes Netz oder Zutritt zum Unternehmen)

5.1.22 Wartungs- und Reparaturarbeiten

Es sollte ein Verantwortlicher festgelegt werden, der für die rechtzeitige Einleitung von Wartungs- bzw. Reparaturarbeiten verantwortlich ist. (siehe Kapitel 5.1.21)

Die IT – Geräte sollten regelmäßig gereinigt werden und verpflichtende Reinigungsintervalle sind festzulegen. Wartungsarbeiten durch externe Mitarbeiter müssen ständig und Beaufsichtigung erfolgen und außerdem muss kontrolliert werden, ob der Wartungsvertrag vollständig erfüllt wurde. Des Weiteren müssen sich Wartungsarbeiter

auf Verlangen ausweisen. Den Zugriff auf sensible Daten des Unternehmens sollte dem Wartungsarbeiter nicht möglich sein und seine Zutritts- und Zugriffsrechte sollten während der Wartungstätigkeit auf ein Minimum beschränkt werden. Bei Beendigung der Wartungsarbeiten sind die durchgeführten Wartungsarbeiten, sowie eventuelle Reparaturarbeiten zu dokumentieren und ein Test der vollständigen Funktionstüchtigkeit sollte gemacht werden.

Bei externen Wartungsarbeiten müssen sensitive Daten physikalisch gelöscht werden und ev. ein Vertrag auf Geheimhaltung der Daten abgemacht werden. Vor der Durchführung muss protokolliert werden, wann und wem das Gerät zur Wartung/Reparatur gegeben wurde und auf einen sicheren Transport sollte Wert gelegt werden. Bei Beendigung der Wartung/Reparatur müssen alle Passwörter geändert werden. Weiters ist wichtig, dass ein Testlauf die Funktionalität prüft und ein aktuelles Virensuchprogramm die Festplatten nach Viren untersucht. Die vom Hersteller vorgegeben Wartungsintervalle sind einzuhalten.

- Einschränkung der Funktionalität der IT - Geräte
- Datendiebstahl
- Missbrauch von Daten
- Manipulation des IT – Systems
- Verlust des IT – Gerätes
- Virenverseuchung

5.1.23 Vorsichtsmaßnahmen bei Reinigung

Auch für Reinigungspersonal gelten die gleichen Zugangsbeschränkungen, wie für das restliche Personal des Unternehmens (siehe Kapitel 5.1.19). Es sind regelmäßig Stichprobenkontrollen durchzuführen, ob alle Sicherheitsmaßnahmen eingehalten werden. Reinigungskräfte sollten auf die Einhaltung folgender Punkte hingewiesen werden:

- Bei der Reinigung von Tastaturen von laufenden Geräten ist auf versehentliches Drücken der einzelnen Tasten zu achten.
- Bei Benutzen von Reinigungsflüssigkeit ist darauf zu achten, dass keine Kurzschlüsse bei stromführenden Hardware – Komponenten entstehen.
- Achten auf unabsichtliches Ausschalten von IT – Komponenten.
- Auf Kommunikationskabel und Stromkabel ist bei der Reinigung besonders zu achten.

Sensible Bereiche, wie Datenträgerarchiv, sind nur unter Anwesenheit des jeweilig Verantwortlichen zu reinigen.

- Zugriff auf Daten durch unbefugte Dritte
- Systemausfälle
- Einschränkung bzw. Verlust der Kommunikationsfähigkeit

5.1.24 Betreuung und Beratung

Neben der Einschulung der Benutzer bedarf es einer laufenden Betreuung und Beratung ebendieser. Es sollte eine Person oder ein Personenkreis festgelegt werden, an die sich der IT - Benutzer bei Problemfällen wenden kann.

- Keine effiziente Nutzung der IT - Infrastruktur
- Keine Aufrechterhaltung des laufenden Betriebs
- Hardware und Software Defekte
- Bedienungsfehler

5.1.25 Bestimmen eines Administrators

Es sollte mindestens ein kompetenter Verantwortlicher für die Administration des IT - Systems und der Netze ernannt werden. Der Administrator sollte auch regelmäßig geschult werden. Bei mehreren Administratoren im Betrieb ist der Zuständigkeitsbereich abzuklären.

- IT - System nicht funktionstüchtig
- Administrator nicht am aktuellen Stand der Technik
- Konfliktpotenzial zwischen verschiedenen Administratoren

5.1.26 Festlegung von Verantwortlichkeiten bei Software

Es ist festzulegen welche Person, welche Abteilung oder welche Fremdfirma für die folgenden Punkte im Lebenszyklus von Software zuständig ist.

- Erstellen eines Anforderungskatalogs (was soll die Software leisten?)
- Vorauswahl
- Testen der Software
- Entscheidungsfindung und Beschaffung
- Installation, Konfiguration
- Versionskontrolle, Besorgen von Updates
- Kontrolle des IT – Betriebs
- Deinstallation
- Einsatz von nicht funktionstüchtiger Software
- Einsatz von Software, die nicht die Anforderungen erfüllt
- Einsatz von Software mit Sicherheitslücken, da keine Updates ausgeführt werden

5.1.27 Bestimmung eines Notfallverantwortlichen

Für den Eintritt eines Notfalls muss ein Verantwortlicher bestimmt werden, der sowohl über die Berechtigung verfügt Notfallmaßnahmen einzuleiten, als auch darüber die Entscheidung zu treffen, ob ein Notfall vorliegt.

- Keine Koordination bei Eintritt eines Notfalls
- Notfallgegenmaßnahmen werden zu spät oder gar nicht eingeleitet

5.1.28 Vertraulicher Umgang mit Informationen

Die Mitarbeiter sind auf Restriktion im Umgang mit firmeninternen Informationen hinzuweisen und diese Restriktionen sind von den Mitarbeitern einzuhalten. Es besteht die Möglichkeit Dokumente mit Weitergaberestriktionen („nur für internen Gebrauch) einzuführen und diese Dokumente dürfen ohne Genehmigung nicht vervielfacht werden.

- Zugriff auf Daten durch unbefugte Dritte
- Finanzieller Verlust durch unbefugte Vervielfältigung

5.1.29 Aufenthalt betriebsfremder Personen

Betriebsfremde Personen, wie Handwerker, Besucher etc., dürfen sich nicht unbeaufsichtigt im Betrieb bewegen, außer in dafür vorgesehen Räumen, wie den Besucherraum. Falls eine ständige Beaufsichtigung nicht möglich ist, z.B. bei Reinigungspersonal, sind Tische, Schränke etc. abzuschließen.

- Diebstahl
- Datendiebstahl

5.1.30 Regelungen für den Einsatz von Fremdpersonal

Beim kurzfristigen Einsatz des Fremdpersonals sind diese, wie Besucher zu behandeln. (siehe Kapitel 5.1.29). Beim langfristigen Einsatz sind die Mitarbeiter auf die internen Sicherheitsvorschriften hinzuweisen und schriftlich auf die Einhaltung zu verpflichten. Beim Ausscheiden des Mitarbeiters sind seine Zugangs- und Zutrittsberechtigungen zu löschen.

- Diebstahl von Daten bzw, IT – Komponenten

5.1.31 Richtlinien zum Outsourcing

Bei der Wahl des Dienstleisters ist darauf zu achten, dass das eigene Qualitäts- und Sicherheitsniveau eingehalten wird.

Das Sicherheitskonzept des eigenen Unternehmens muss mit den Outsourcing – Unternehmen abgestimmt werden.

Regelmäßige Kontrollen zu folgenden Aspekten sind durchzuführen: [4]

- Durchführung der vereinbarten Audits
- Umsetzungsstand der vereinbarten IT-Sicherheitsmaßnahmen
- Wartungszustand von Systemen und Anwendungen
- Rechtezuweisung durch den Dienstleister (Missbrauch von Rechten)
- Einsatz von Mitarbeitern, die dem Auftraggeber nicht gemeldet wurden, z. B. bei Vertretungen
- Performance, Verfügbarkeit, Qualitätsniveau
- Datensicherung

Es ist des Weiteren wichtig festzulegen, welche Rechte dem Outsourcing – Dienstleister eingeräumt werden. Bei Beendigung des Dienstleistungsverhältnisses muss eine geregelte Übernahme stattfinden. Es sind u.a. die Eigentumsrechte an Hard- und Software zu klären. Eine Übergangsfrist ist empfehlenswert.

- Spionagerisiko
- Keine Einhaltung des eigenen Sicherheitsniveaus
- Datendiebstahl

5.1.32 Zweckmäßige Aufstellung von IT - Systemen

Das IT - System sollte vor direkter Sonneneinstrahlung geschützt werden und es sollte so aufgestellt werden, dass es nicht in der Nähe einer Heizung ist. Der Bildschirm des IT - Systems sollte für Unbefugte uneinsichtbar ist. Zu Räumen mit dem IT - System sollten nur Befugte Zutritt haben und bei Publikumsverkehr müssen weitere Sicherheitsvorkehrungen zum Schutz des IT - Systems veranschlagt werden Des Weiteren muss das System vor starken Verschmutzen und Staub geschützt werden. Bei Aufstellung von Netzwerkkomponenten ist darauf zu achten, dass die Konfiguration nicht von Unbefugten manipuliert werden kann.

- Durch Erwärmung wird das System funktionsunfähig bzw. in seiner Funktionalität eingeschränkt
- Diebstahl von wichtigen Daten bei Publikumsverkehr
- Durch Einsatz auf einer Baustelle werden die mechanischen Bauteile, wie Maus, Festplatten etc., durch erhöhtes Staubaufkommen, ruiniert

5.1.33 Zweckmäßige Aufstellung von Druckern

Den Drucker oder Kopierer sollte man nicht in Räume stellen, wo Externe Zugang haben. Am Besten ist es den Drucker an einem Platz aufzustellen, der von Mitarbeitern eingesehen werden kann. Empfehlenswert ist auch eine Aufstellung eines Papiervernichters neben dem Drucker/Kopierer.

- Diebstahl von ausgedruckten Daten
- Diebstahl aus Papierkorb von nicht - vernichteten Ausdrucken
- Manipulation des Druckers

5.1.34 Zweckmäßige Aufbewahrung von dienstlichen Datenträgern

Nur befugte Benutzer sollten Zugriff auf dienstliche Datenträger (wie USB - Stick, Wechselmedium, etc.) haben. Sowohl am betrieblichen, als auch häuslichen Arbeitsplatz sollte es eine Möglichkeit geben den Datenträger bei Abwesenheit zu verschließen. Bei Dienstreisen ist es ratsam den Datenträger in einem versperrbarren Aktenkoffer oder Ähnlichem zu transportieren. Es sollten überhaupt alle Datenträger mit Softwareschutz versehen werden (z.B. Verschlüsselung bei Benutzung eines USB - Sticks).

- Datendiebstahl

5.1.35 Zweckmäßige Aufstellung von Archiv- und Speichersystemen

Archiv- und Speichersysteme sollten in gesicherten Räumen untergebracht werden und zu diesem Räumen dürfen nur Berechtigte einen Zutritt haben. Besonders ist auf die infrastrukturelle Zuverlässigkeit (z.B. Stromversorgung, Notfall - Stromversorgung, siehe ..) und auf Redundanzen zu achten. Im gesamten Raum sollte ein Rauchverbot gelten. Zur Erhöhung der Haltbarkeit und Verfügbarkeit ist eine Klimatisierung von Nöten. Weiters muss man das Archiv vor folgenden Umwelteinflüssen schützen:

- Feuer
- Wasser
- Unzulässige Temperatur bzw. Luftfeuchtigkeit
- Staub, Verschmutzung
- Diebstahl von Daten
- Ausfall der Verfügbarkeit
- Zerstörung der Daten

5.1.36 Verwaltung der Betriebsmittel

Die Betriebsmittelverwaltung muss von einer zentralen Stelle geregelt werden. Die zentrale Stelle übernimmt die Prüfung der Vollständigkeit bei der Anschaffung und falls möglich sollte durch Testläufe kontrolliert werden, ob die Ware funktionstüchtig, ob diese kompatibel zum bestehenden IT - System ist. Weitere wichtige Aufgabengebiete der zentralen Stelle sind die Bestandsführung der bestehenden Betriebsmittel und Entscheidungsfindung, ob und wann neue Betriebsmittel angeschafft werden sollen. Es sollte bei der Bestandsführung ein Bestandsverzeichnis angelegt werden. Diese zentrale Stelle sollte auf sachgerechte Lagerung achten und muss auch regeln, was mit den be-

nutzen Betriebsmittel bzw. Verbrauchsgüter geschehen soll (z.B. Toner zu Sondermüll oder Zurücklieferung an Lieferanten, Schreddern von Papier, Vernichtung von Datenträgern etc.). Datenträger müssen so entsorgt werden, dass diese absolut unbrauchbar für Externe werden, d.h. Daten dürfen nicht wiederhergestellt werden können (z.B. Mechanische Zerstörung von CD - ROMs). Weiters ist bei Datenträgern eine sachgerechte Bezeichnung von Nöten (z.B. Magnetband Abt. Buchhaltung etc.). Grundlegend ist es noch zu regeln, wer Zutritt zu den Räumen mit den Betriebsmitteln (vor allem bei Datenträgern) hat. Bei der Ausgabe der Betriebsmittel ist das Bestandsverzeichnis [2] zu aktualisieren und es sollte eine regelmäßige Inventur stattfinden.

- Keine koordinierte Beschaffung möglich; Jede Abteilung beschafft was gerade gebraucht wird.
- Keine Wirtschaftlichkeit im Unternehmen
- Schäden an der Umwelt bzw. Verletzung der Umweltauflagen
- Missbrauch von Daten, wenn keine Vernichtung vorgesehen
- Datendiebstahl
- Bestellte Betriebsmittel finden keine Verwendung
- Kein schnelles Auffinden von Datenträgern
- Lieferung nicht vollständig
- Zerstörung der Betriebsmittel durch unsachgerechte Lagerung
- Schwund
- Kein Überblick über vorhandene Betriebsmittel

5.1.37 Dokumentation der IT - Konfiguration

Das vorhandene IT - System sollte dokumentiert werden und immer auf aktuellem Stand sein. Die Dokumentation sollte im Bedarfsfall verfügbar sein und der Zugriff auf die Dokumentation darf nur von autorisierten Personen erfolgen.

- Im Notfall kein geordnetes Hochfahren des IT - Systems möglich

---

[2] Ein solches Bestandsverzeichnis muss Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib der Betriebsmittel,
- Lagervorhaltung,
- Aushändigungsvorschriften und
- Wartungsverträge, Wartungsintervalle,
- Berechtigte Empfänger.

5.1.38 Sicherer Arbeitsplatz

Der Arbeitsplatz ist nach Verlassen (Dienstschluss, Kaffeepause, Mittagsessen etc.) „aufgeräumt“ zu verlassen, d.h. es dürfen keine Unterlagen oder Datenträger (wie USB - Sticks etc.) unversperrt auf dem Tisch liegen. Das IT - System muss gegen unbefugten Zugriff (z.B. Abmelden vom System) geschützt werden. Diese Maßnahmen gelten auch für kurzzeitiges Verlassen des Arbeitsplatzes.

- Diebstahl von firmeninternen, sensiblen Daten
- Fremde greifen auf IT - System zu und kopieren/stehlen Daten

5.1.39 Sichere Verwendung von FAX - Geräten

Ein Fax sollte immer mit einem Deckblatt versehen werden, welches zumindest folgende Punkte enthält:

- Name und Faxnummer des Empfängers
- Name Adresse und Telefonnummer des Absenders
- Seitenanzahl einschließlich Deckblatt
- Dringlichkeitsvermerk
- Unterschrift des Absenders

Der ordnungsgemäße Versand ist auf dem jeweiligen Sendebericht zu kontrollieren und dieser ist mit dem Fax aufzubewahren.

Weiters sind die Protokolle der Empfangenen und versendeten Faxe (Kommunikationsjournale) auszudrucken zu archivieren und stichprobenartig auf Unregelmäßigkeiten zu kontrollieren.

Bei einem wichtigen Fax ist es notwendig dieses vorher telefonisch anzukündigen und sich auch den Empfang bestätigen zu lassen.

- Empfänger kann Fax nicht zuordnen
- Fax geht beim Empfänger verloren
- Fax kommt beim Empfänger nicht an

5.1.40 Festlegung von FAX – Richtlinien

Es sollte für jedes Fax – Gerät ein Fax – Verantwortlicher ernannt werden, der für die Verteilung der eingehenden Nachrichten, Versorgung des Fax – Gerätes mit notwendigen Verbrauchsgütern (wie Toner, Papier, etc.) und für die gelegentliche Kontrolle von programmierten Zieladressen (besonders nach Wartungs- und Reparaturarbeiten) verantwortlich ist. Der Fax – Verantwortliche ist ebenfalls zuständig für die Entsorgung von Verbrauchsgütern und Ersatzteilen. Weiters sollte festgelegt werden, welche Personen das Fax – Gerät benutzen dürfen. Das Fax – Gerät ist nach Dienstschluss abzuschalten.

- Unkontrollierte Verteilung von Fax – Sendungen
- Wichtige Fax – Sendungen gehen verloren
- Fax – Sendungen werden an Konkurrenten geschickt
- Nach Dienstschluss kommen unkontrollierte Sendungen hinein

5.1.41 Festlegung von Anrufbeantworter - Richtlinien

Die Fernabfrage sollte mechanisch oder elektronisch deaktivierbar sein. Bei Einsatz der Fernabfrage ist ein frei programmierbarer Sicherungscode regelmäßig zu ändern (siehe Kapitel 5.1.51). In Ansagetext ist darauf hinzuweisen, dass keine schutzbedürftigen Informationen hinterlassen werden dürfen. Die Nachrichten auf dem Anrufbeantworter sollten regelmäßig abgehört und gelöscht werden.

- Interne Nachrichten werden von Externen abgehört

5.1.42 Richtlinien zur Aufbewahrung der Backups

Die Backups müssen so aufbewahrt werden, dass nur befugte Personen auf diese Zugriff haben. Im Notfall müssen die Sicherungen schnell verfügbar sein. Die Lagerung der Backups hat so zu erfolgen, dass eine längere Aufbewahrung ohne Beschädigung der Datenträger gewährleistet ist. Weiters sollten die Backups in einem anderen Brandabschnitt aufbewahrt werden

- Gelöschte Daten können nicht wieder hergestellt werden
- Bei Ausfall von Speichermedien sind die gespeicherten Daten verloren

5.1.43 Testen von neuen IT – Komponenten

Bei größeren Eingriffen in das bestehende IT – System (wie Installation neuer Software oder Austausch von IT – Komponenten) ist darauf zu achten, dass die Gesamtsicherheit nicht gefährdet ist. Die neuen Komponenten sollten vor Einsatz in einer Testumgebung geprüft werden und dann erst in das Gesamtsystem integriert werden.

- Instabilität des IT – Systems
- Unerwartetes Systemverhalten
- Sicherheitslücken
- Systemausfälle

5.1.44 Überprüfung der Batterien

Bei Geräten, die für ihre Funktion Batterien benötigen, aber auch bei Geräten die Batterien als Notstromversorgung verwenden, ist eine regelmäßige Überprüfung der Batterien notwendig.

- Geräte sind nicht mehr funktionsfähig

5.1.45 Gewährleistung einer Datenrekonstruktion

Es sollte in sporadischen Abständen und bei Änderung des Datensicherungsverfahrens überprüft werden, ob mittels der vorhandenen Sicherungen eine vollständige Wiederherstellung der Daten möglich ist.

- Gelöschte Daten können nicht wieder hergestellt werden
- Bei Ausfall von Speichermedien sind die gespeicherten Daten verloren

5.1.46 Umgang mit Wechselmedien

Es sollten Richtlinien für die Nutzung von Wechselmedien(USB-Sticks, Externe Festplatten, usw.) erstellt werden. Die Richtlinien sollten genau festlegen, wofür die Wechselmedien genutzt werden dürfen und welche Wechselmedien an den PC angeschlossen werden dürfen. Das Booten von solchen Medien sollte im BIOS deaktiviert werden.

- Unbefugte erhalten Zugriff auf sensible Daten
- Das Betriebssystem kann manipuliert werden
- Virenbefall
- Zugriffsbeschränkungen und Sicherheitsrichtlinien können umgangen werden

5.1.47 Richtlinien bei Ersteinsatz von neuer Hard- und Software

Neue Hardware und Software sollte vor dem Einsatz im Echtbetrieb in einer isolierten Testumgebung geprüft werden. Ebenfalls sind neue Komponenten auf Viren zu überprüfen.

- Virenbefall
- Systemabsturz

5.1.48 Richtlinien für Verlust von IT – Komponenten

Es ist umgehend Meldung an den jeweiligen Ansprechpartner zu richten. Wenn möglich ist sofort der Zugang für die betroffenen IT – Systeme zu sperren (z.B. MAC – Adresse des entwendeten Laptops für das interne Netz sperren). Beim gleichzeitigen Verlust von vertraulichen Informationen sind die betroffenen Bereiche zu informieren.

- Zugriff auf sensible Daten durch unbefugte Dritte

- Zugriff auf sensible Bereiche durch unbefugte Dritte
- Manipulation und Fälschung von Daten

5.1.49 Richtlinien zur Installation von neuen IT - Komponenten

Bei größeren Eingriffen in das bestehende IT – System (wie Installation neuer Software oder Austausch von IT – Komponenten) ist darauf zu achten, dass die Gesamtsicherheit nicht gefährdet ist.

Bei Installation von neuen sind, die vom Hersteller vorgegeben, Grundeinstellungen zu überprüfen und an die eigenen Sicherheitsleitlinien anzupassen. Ebenfalls sind die Standardbenutzernamen und Standardpasswörter zu ändern. Unnötige Benutzer - Accounts sind zu deaktivieren bzw. zu löschen. Netzdienste, die nicht verwendet werden, sind auszuschalten. Auf Servern und Clients mit erhöhtem Schutzbedarf sollte zusätzlich noch ein lokaler Paketfilter installiert und so konfiguriert werden, dass nicht benötigte Dienste herausgefiltert werden.

Die neuen Komponenten sollten vor Einsatz in einer Testumgebung geprüft werden und dann erst in das Gesamtsystem integriert werden.

- Instabilität des IT – Systems
- Unerwartetes Systemverhalten
- Sicherheitslücken
- Systemausfälle

5.1.50 Nutzungsverbot von privater Soft- und Hardware

Private Software darf nicht auf Rechnern des Unternehmens installiert werden, außer nach Rücksprache mit IT - Verantwortlichen. Genauso wenig darf private Hardware an Unternehmensrechner angeschlossen werden (z.B. Anschluss privater Festplatte über USB - Port). Falls nötig sollten Ausnahmegenehmigungen schriftlich fixiert werden (z.B. Erlaubnis Dokumente am USB - Stick heim mitzunehmen um Arbeit weiterzuführen etc.)

Es sollten Firmenrechner, falls technisch möglich, so konfiguriert werden, dass unautorisierte Software nicht eingespielt werden kann. Des Weiteren sollten die Firmenrechner regelmäßig, stichprobenartig auf betriebsfremde Hard- und Software überprüft werden. Diese Untersuchungen sollten dokumentiert werden um Wiederholungsfälle feststellen zu können. Auf diese Nutzungsverbote sind die Mitarbeiter hinzuweisen.

- Virenverseuchung
- Ablenkung der IT - Benutzer durch private Software
- Datendiebstahl
- Einschränkung der Funktionsfähigkeit des Rechners

5.1.51 Richtlinien für sichere Passwörter

Die Passwörter müssen so komplex gewählt werden, dass sie nicht einfach zu Erraten sind. Daher sollten z.B. keine Geburtsdaten, Wohnadressen, Namen der Ehepartner, Kinder etc. als Passwort gewählt werden. Vom System vorgegebene Standardpasswörter sind sofort durch eigene Passwörter zu ersetzen. Das Passwort sollte aus alphanumerischen Zeichen und Sonderzeichen bestehen, dabei sollten die alphanumerischen Zeichen auch Groß- und Kleinbuchstaben enthalten. Die Mindestlänge hat 8 Zeichen zu betragen. Wenn der Benutzer auf verschiedenen Systemen arbeitet, sind auch verschiedene Passwörter zu benutzen. Das Authentisierungssystem sollte den Zugang nach wenigen Fehlversuchen sperren und vom Benutzer verlangen, dass er sein Passwort regelmäßig ändert. Nach Passwortwechsel sind die alten Passwörter vom Authentisierungssystem nicht zu erlauben. Trivialpasswörter, wie 1234, ABC, QWERTZ, etc. sind strikt untersagt.

Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein. Das Passwort sollte auch nicht notiert werden.

Ein Passwort, das einem neuen Benutzer für die erstmalige Systemnutzung mitgeteilt wird, muss danach gewechselt werden. Dies sollte vom System initiiert werden.

- Zugang zum System von Unbefugten
- Datendiebstahl

5.1.52 Anlegen Benutzer und Benutzergruppen

Um die Vergabe von Zugriffsberechtigungen zu ermöglichen müssen Benutzer bzw. Benutzergruppen (z.B. Buchhaltung, Einkauf, etc.) angelegt werden. Bei der Vergabe muss festgehalten werden, wer der neue Benutzer ist (Name, Vorname), wie er zu erreichen ist (Mail-Adresse, Tel. Nr., Arbeitsraum), seine Organisationseinheit und seine Benutzerkennung bzw. Gruppenkennung. Es sollten mehrere Rechteprofile existieren und jeder Benutzer bzw. Benutzergruppe muss einem Rechteprofil zugeordnet werden. Die Dokumentation über die Benutzergruppen bzw. Benutzer muss gesichert aufbewahrt werden und regelmäßig (1/2 jährlich, jährlich) überprüft werden, ob die Benutzerrechte den aktuellen Anforderungen entsprechen.

- Benutzer nicht eindeutig identifizierbar
- Benutzer hat alle bzw. mehr Rechte als vorgesehen
- Zugriff auf Dateien bzw. IT - Ressourcen ohne Berechtigung

5.1.53 Festlegung der Zugangs- und Zugriffsrechte

Anhand der Funktion und der Aufgaben der jeweiligen Mitarbeiter sollte dieser bestimmte Zugriffs- und Zugangsrechte erhalten. Bei der Vergabe der Rechte muss auch auf die Sensitivität der Daten Rücksicht genommen werden.

Der Zugriff auf IT – Systeme muss durch geeignete Identifikations- und Authentifizierungsverfahren abgesichert werden.

- Zugriff aus sensitive Daten durch Unbefugte
- Datendiebstahl

5.1.54 Aktivieren eines Passwortschutzes für IT-Komponenten

Auf jeder IT-Komponente (auch bei Laptops) muss der Passwortschutz aktiviert werden. Der Schutz ist so zu konfigurieren, dass unmittelbar nach dem Einschalten des Systems eine Authentifizierung erfolgen muss. Der Zugang zu einer IT-Komponente ohne Authentifizierung darf nicht möglich sein. Die Wahl des richtigen Passwortes wird in dem Kapitel 5.1.51 erläutert.

- Personen haben Zugriff auf das IT-System
- Unbefugte Dritte erhalten Zugriff auf sensible Daten
- Das IT-System kann manipuliert oder sogar zum Absturz gebracht werden

5.1.55 Aktivieren der Bildschirmsperre

Auf jedem Clientbetriebssystem sollte die Bildschirmsperre aktiviert werden.

Die Sperre ist so zu konfigurieren, dass sie vom Benutzer als auch durch einen vorgegebenen Inaktivitäts-Zeitraum aktiviert wird. Weiters sollte sie nur durch die Eingabe des richtigen Passwortes aufgehoben werden können. Die Wahl des richtigen Passwortes wird in dem Kapitel 5.1.51 erläutert.

- Personen haben Zugriff auf das Betriebssystem
- Unbefugte Dritte erhalten Zugriff auf sensible Daten
- Das Betriebssystem kann manipuliert oder sogar zum Absturz gebracht werden

5.1.56 Ändern der Standardpasswörter

Bei den einzelnen Komponenten des IT-Systems ist vor Inbetriebnahme das Standardpasswort auf ein neues Passwort zu ändern. Die Wahl des richtigen Passwortes wird in dem Kapitel 5.1.51 erläutert.

- Zugriff auf sensible Daten durch unbefugte Dritte
- Manipulation der IT-Komponente

5.1.57 Konfiguration des Logins

Der Login sollte so konfiguriert werden, dass sich die Wartezeit bis zur nächsten Login-Aufforderung vergrößert, wenn ein falscher Anmeldeversuch erfolgt ist. Weiters sollte beim Login der letzte fehlgeschlagene Anmeldeversuch angezeigt werden. Bei einer vorher festgelegten Anzahl von Fehlanmeldungen ist der Benutzerzugang zu sperren und nur der Administrator sollte in der Lage sein, diesen Zugang wieder zu aktivieren.

- Zugriff auf sensible Daten durch unbefugte Dritte
- Manipulation der IT-Komponente

5.1.58 Einsatz von Antiviren - Programmen

Auf jedem Rechner(Client und Server) im Unternehmen muss ein Antivirenprogramm installiert werden. Dieses Antivirenprogramm muss laufend aktualisiert werden und es müssen regelmäßige Virenprüfungen stattfinden. Die Ergebnisse der Prüfungen sollten dokumentiert werden. Wenn es möglich ist, sollte das Antivirenprogramm so konfiguriert werden, dass es für den Benutzer unbemerkt im Hintergrund läuft und die Aktualisierungen und die Prüfungen automatisch erfolgen. Weiters ist darauf zu achten, dass bei der Prüfung alle am Computer befindlichen Dateien auf Virenbefall überprüft werden.

- Virenbefall
- Verlust von Daten
- Unbefugte Dritte erhalten Zugriff auf sensible Daten
- Ausfall von Komponenten des IT-Systems

5.1.59 Vorgehensweise bei Auftreten eines Computer-Virus

Wird ein Virus auf einem PC von der Antivirussoftware erkannt und nicht automatisch gelöscht oder in Quarantäne verschoben, dann sollte der Benutzer folgende Punkte beachten.

- Ruhe bewahren
- Alle laufenden Programme beenden
- Wenn vorhanden, den Systemadministrator benachrichtigen

5.1.60 Erstellung eines Virenschutzkonzeptes

Als ersten Schritt sollte alle IT – Systeme identifiziert werden, die von einem Virenbefall gefährdet sind. Besonders IT – Systeme mit dem Betriebssystem Windows, den Programmen Word, Excel (aufgrund Makro Viren) und IT – Systeme mit Internetzugang sind vom Virenbefall bedroht. Für die bedrohten Rechner sollte man versuchen

den Infektionsweg zu erkennen (z.b. Diskettenlaufwerk, Streamer, Internetzugang etc.) und diesen für den Notfall zu tabellieren.

Nachfolgend ist das Inhaltsverzeichnis eines Virenschutzkonzeptes vom deutschen Grundschutzhandbuch angeführt. [4]

Teil A: Sensibilisierung

- Abhängigkeit der Institution vom IT-Einsatz
- Beschreibung des Gefährdungspotentials
  - Computer-Viren
  - Makro-Viren
  - Trojanische Pferde
  - Hoax
- Schadensszenarien
- Potentiell betroffene IT-Systeme

Teil B: Erforderliche Schutzmaßnahmen

- Computer-Virenschutz-Strategie
  - Nicht-vernetzte IT-Systeme
  - Vernetzte Endgeräte
  - Server
- Aktualisierung der Computer-Viren-Suchprogramme
  - Nicht-vernetzte IT-Systeme
  - Vernetzte Endgeräte
  - Server

Teil C: Regelungen

- Regelungen zum Schutz vor Computer-Viren
  - Nutzungsverbot nicht freigegebener Software
  - Schulung der IT-Benutzer
  - Umstellung der Boot-Reihenfolge
  - Anlegen einer Notfalldiskette
  - Verhaltensregeln bei Auftreten eines Computer-Virus
  - Maßnahmen bei nicht-resident virenkontrollierten IT-Systemen
  - Regelmäßiger Einsatz eines Computer-Viren-Suchprogramms
  - Virenkontrolle bei Datenträgeraustausch und Datenübertragung
  - Prüfung eingehender Dateien auf Makro-Viren
- Regelung der Verantwortlichkeiten
  - Ansprechpartner für Computer-Viren
  - Verantwortlichkeit von Administratoren

- Verantwortlichkeit des einzelnen IT-Benutzers
- Verantwortlichkeit des IT-Sicherheitsmanagements

Teil D: Hilfsmittel

- Verhaltensregeln bei Auftreten eines Computer-Virus
- Meldewege bei Auftreten eines Computer-Virus
- Benutzerhandbuch des Computer-Viren-Suchprogramms
- Virenbefall
- Datenverlust
- Schaden an Software und Hardware

5.1.61 Auswahl einer Virenschutzstrategie

Ausgehend vom Bedrohungsrisiko und je nach finanziellen und personellen Einsatz sollte mindestens eines der folgenden Virenschutzstrategien gewählt werden.

- *Virensuchprogramm auf jedem Rechner*
  Schutzprogramm läuft ständig im Hintergrund auf jedem Rechner.
- *Virensuchprogramm auf allen Servern*
  Keine Übertragung von Viren von einem Endgerät auf eine Anderes, daher lokale Isolierung.
- *Virensuchprogramme auf Rechnern und Endgeräten*
- *Virensuchprogramme auf den Kommunikationsservern*
  Schützt vor Viren, die von externen IT – Systemen kommen (z.B: Mailserver, Router etc.).
- *Virensuchprogramme auf Endgeräten mit externen Schnittstellen*
- *Datenhygiene und zentrale Prüfung*
  An einer zentralen Stelle sollen alle eingehenden Daten (externe Kommunikation und auch Datenträger) auf Viren untersucht werden.

Bei der Wahl des Virenschutz - Programms sollte man darauf achten, dass der Umfang der erkannten Viren groß ist, auch Viren in komprimierten Dateien erkannt werden und vor allem eine regelmäßige Aktualisierung der Virensoftware gewährleistet ist

Darüber hinaus können Computer-Viren-Suchprogramme verschiedener Hersteller eingesetzt werden, um so die Erkennungsrate zu erhöhen.

E – Mails sollten nicht im HTML – Format gelesen werden bzw. versendet werden.

Der Mail - Client ist so einzustellen, dass eine Warnmeldung erscheint bevor Anhänge in Mails geöffnet werden und Mails sind vor Öffnung auf Viren zu prüfen. Überhaupt sind ausführbare Dateien (z.B. EXE, COM, etc.) im Anhang nicht zu öffnen.

- Virenbefall

- Datenverlust
- Schaden an Software und Hardware

5.1.62 Öffnen von Komprimierten Dateien

Selbstextrahierende Dateien sind nicht vom Benutzer zu öffnen, weiters sind komprimierte Dateien bevor sie entpackt werden auf Viren zu prüfen.

- Viren, Trojaner, Würmer auf dem jeweiligen Rechner

5.1.63 Richtlinien zum Einsatz eines Client PCs

Jeder Client PC, egal ob mit dem Internet verbunden oder nicht, sollte mit einer Antivirussoftware, die regelmäßig aktualisiert wird, ausgestattet sein. Wenn der Rechner Zugang zum Internet besitzt, dann ist zusätzlich noch eine Antispy-Software zu installieren, die auch regelmäßig upgedatet wird. Die Konfiguration des E-Mail-Client sollte nach diesen Richtlinien 5.2.41 erfolgen. Der richtige Umgang und die richtige Konfiguration des Web-Browsers wird im Kapitel 5.2.24 erläutert.

- Gefährdung des internen Netzes durch Viren, Würmer und Trojaner
- Spammails
- Überlastung des Netzes
- Vergeudung von unnötigen Speicherplatz
- Gefahr, dass unbefugte an interne sensible Daten gelangen

5.1.64 Erstellen eines Datensicherungsplans

Es sollte ein Datensicherungsplan erstellt werden. Dieser Plan muss laut [4] folgende Informationen enthalten:

  - Speicherungsort der Daten im Normalbetrieb (Plattenspeicher-Belegungsplan),
  - den Bestand der gesicherten Daten (Bestandsverzeichnis),
  - die Zeitpunkte der Datensicherungen,
  - Art und Umfang der Datensicherung (logische/physikalische, Teil-/Vollsicherung),
  - das Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten und
  - den Ort der Aufbewahrung (Hinweis auf ggf. erforderliche Zutrittsmittel).
- Gelöschte Daten können nicht wieder hergestellt werden
- Bei Ausfall von Speichermedien sind die gespeicherten Daten verloren

5.1.65 Datensicherung am PC

Wenn kein Fileserver vorhanden ist auf dem, die wichtigen Daten zentral gespeichert werden und auf dem auch regelmäßige Backups durchgeführt werden, dann muss jeder einzelne PC separat gesichert werden. Die Sicherung der PC's muss laufend erfolgen und es müssen alle für den Betrieb wichtigen Daten gesichert werden. Jeder Mitarbeiter muss dazu angehalten werden seine Daten zu sichern. Es sollte eine regelmäßige Erinnerung und Kontrolle der Einhaltung durchgeführt werden.

- Gelöschte Daten können nicht wieder hergestellt werden
- Bei Ausfall von Speichermedien sind die gespeicherten Daten verloren

5.1.66 Erstellen von Sicherungskopien der verwendeten Software

Von der eingesetzten Originalsoftware ist eine Sicherungskopie zu erstellen. Die Sicherungskopie und die Originalsoftware sind getrennt voneinander aufzubewahren. Es muss gewährleistet werden, dass kein unbefugter Zugriff auf die Originale und den Kopien hat.

- Bei einem Notfall kann die Systemsoftware nicht mehr eingespielt werden
- Unerlaubte Vervielfältigung der firmeneigenen Software

5.1.67 Gewährleistung der Wiederherstellbarkeit von Backups

Die Backups sollten vereinzelnd auf Wiederherstellbarkeit der Daten überprüft werden.

- Die Wiederherstellung der Daten kann nicht gewährleistet werden

5.1.68 Datensicherungskonzeption

Bei der Beschaffung einer geeigneten Datensicherungseinrichtung ist darauf zu achten, dass diese mit der vorhandenen Hardware problemlos zusammenarbeitet. Weiters sollte es möglich sein Sicherungen zu vorwählbaren Zeiten durchzuführen. Das Sicherungsmedium ist durch Passwort oder Einsatz einer zweckmäßigen Kryptographie zu verschlüsseln. Neben der physischen vollständigen Sicherung sollte die Sicherungssoftware auch eine Änderungssicherung (inkrementelle Sicherung) vornehmen können.

- Verluste von Daten
- Keine aktuellen Sicherung
- Zeitintensive Sicherungen

5.1.69 Strukturierte Haltung von Daten

Es sind die IT – Benutzer darauf hinzuweisen ihre Daten strukturiert auf den lokalen bzw. Netzwerk – Platten zu speichern. Es könnte auch Pflicht sein, eine vorgegebene Verzeichnisstruktur einzuhalten. Es sollte ebenfalls eine Trennung von Programmen und Daten durchgeführt werden. Bei vernetzten Systemen sind Programme mit hoher Verfügbarkeit lokal zu installieren. In diesem Fall ist auch eine Datensicherung auf diesen Rechnern regelmäßig durchzuführen.

- Daten und Programme werden nicht gefunden
- Überschreiben von Daten

5.1.70 Notfallhandbuch Erstellung

Es muss ein Notfallhandbuch erstellt werden in dem alle für den Notfall vorgesehenen Maßnahmen eingetragen werden. Bei der Erstellung des Handbuchs ist darauf zu achten, dass eine Sachverständige Person in der Lage ist die im Handbuch aufgeführten Maßnahmen einzuleiten.

Es folgt eine beispielhafte Inhaltsangabe eines Notfallhandbuchs [4].

Welche Einträge übernommen werden hängt vom jeweiligen Bedarfsfall ab.

1	Alarmierung im Notfall
1.1	Alarmierungsplan und Meldewege
1.2	Adresslisten betroffener Mitarbeiter
1.3	Festlegung konkreter Aufgaben für einzelne Personen/Funktionen im Notfall
1.4	Notrufnummern
...	
2	Handlungsanweisung für spezielle Ereignisse
2.1	Brand
2.2	Wassereinbruch
2.3	Stromausfall
2.4	Ausfall der Klimaanlage
2.5	Explosion
2.6	Sabotage
2.7	Ausfall der Datenfernübertragungseinrichtung
2.8	Einbruch
2.9	Vandalismus
2.10	Bombendrohung
2.11	Streik / Demonstrationen
2.12	...

Teil B: Regelungen für den Notfall

3	Allgemeine Regelungen
3.1	Notfall-Verantwortliche
3.2	Benennung der an der Durchführung der Notfallpläne beteiligten Organisationseinheiten
3.3	Organisationsrichtlinien, Verhaltensregeln
...	
4	Tabelle der Verfügbarkeitsanforderungen

Teil C: Wiederanlaufpläne für kritische Komponenten

5	Wiederanlauf-Planung
5.1	Wiederanlauf-Plan für Komponente 1 (z. B. Host)
5.1.1	Wiederbeschaffungsmöglichkeiten
5.1.2	Interne / externe Ausweichmöglichkeiten
5.1.3	DFÜ-Versorgung
5.1.4	Eingeschränkter IT-Betrieb
5.1.5	Wiederanlaufreihenfolge
5.2	Wiederanlauf-Plan für Komponente 2 (z. B. Drucker)
...	

Teil D: Dokumentation

6	Beschreibung der IT-Systeme
6.1	Beschreibung des IT-Systems A (im Überblick)
6.1.1	Beschreibung der Hardware-Komponenten
6.1.2	Beschreibung der Software-Komponenten
6.1.2.1	Bestandsverzeichnis der Systemsoftware
6.1.2.2	Bestandsverzeichnis der zu dem IT-System gehörenden Systemdaten
6.1.3	Beschreibung der Netzanbindungen des IT-Systems
6.1.4	Beschreibung der IT-Anwendungen
6.1.4.1	Bestandsverzeichnis der Anwendungssoftware
6.1.4.2	Bestandsverzeichnis der zu einer IT-Anwendung gehörenden Daten
6.1.4.3	Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall
6.1.4.4	Minimale Kapazitätsanforderungen der IT-Anwendungen für den Notfall
6.1.4.5	Wiederanlaufverfahren der IT-Anwendungen
6.1.5	Datensicherungsplan
6.1.6	Beschreibung der notwendigen Infrastruktureinrichtungen
6.1.7	Sonstige Unterlagen (Handbücher etc.)
...	
7	Wichtige Informationen
7.1	Ersatzbeschaffungsplan
7.2	Hersteller- und Lieferantenverzeichnis
7.3	Verzeichnis der Dienstleistungsunternehmen des Fachgebiets SSanierung-

- Notfallgegenmaßnahmen werden zu spät oder gar nicht eingeleitet

5.1.71 Alarmierungs- und Notfallpläne

Es sollte ein Alarmierungsplan erstellt werden, der eine Beschreibung des Meldeweges der Personen enthält, die im Notfall informiert werden müssen.

Dieser Alarmierungsplan ist allen notfallverantwortlichen Personen zugänglich zu machen. Die Personen die in diesem Plan Erwähnung finden, müssen den Teil der sie betrifft kennen. Es kann einen Alarmierungsplan für verschiedene Arten von Notfällen geben, oder es gibt je Notfall einen Alarmierungsplan.

Weiters ist ein Notfallplan zu erstellen, der die Verhaltensregeln für bestimmte Schadensereignisse wie Brand, Wassereinbruch, Stromausfall beinhaltet. Nach Erstellung des Notfallplans ist seine Wirksamkeit durch eine Notfallübung zu überprüfen

- Bei Eintritt eines Notfalls können die zu informierenden Personen nicht erreicht werden, dadurch werden die Gegenmaßnahmen zu spät oder gar nicht eingeleitet
- Da keine Verhaltensregeln deklariert wurden wird möglicherweise bei einem Notfall falsch vorgegangen

5.1.72 Fehlerbehandlung

Wenn Fehler auftauchen, sind diese zu protokollieren und zu melden. Die Fehleruntersuchung und Beseitigung ist nur von geschultem Personal zu erledigen. Falls Updates und Patches notwendig sind, sind diese nur vom Hersteller bzw. autorisierten Stellen zu beziehen.

- Fehler nicht beseitigt
- Absturz von IT – Komponenten
- Unsachgemäße Fehlerbehebung
- Verlust der Garantie

5.1.73 Erstellung eines Notfallbootmediums

Es sollte ein Notfallbootmedium erstellt werden, welches zur Wiederherstellung eines abgestürzten Systems dient. Das Notfallbootmedium kann entweder eine Diskette, ein USB-Stick, eine externe Festplatte, eine CD oder eine DVD sein.
Auf diesem Notfallbootmedium sollten zumindest ein Virenscanner, ein Tool zur Wiederherstellung des Bootsektors, ein Tool zur Bearbeitung der Systemkonfigurationsdateien, Backup - und Recoveryprogramme und alle benötigten Treiber die zum Zugriff auf die Festplatten des Rechners benötigt werden, sich befinden.
Weiters ist darauf zu achten, dass das Notfallbootmedium frei von Viren ist.

- Abgestürztes System kann nicht wiederhergestellt werden
- Virenbefall

5.1.74 Erfassen der Kapazitätsanforderungen

Die Kapazitätsanforderungen der gesamten IT-Anwendungen sind zu dokumentieren.

Punkte die berücksichtigt werden müssen sind, die CPU-Leistung, die Arbeitsspeicherkapazität, die Festplattenkapazität, die Kapazität der TK-Anlage, Kapazitäten zusätzlicher Peripheriegeräte wie Drucker, Scanner, usw.

Für den Eintritt eines Notfalls ist zu untersuchen, ob diese Anforderungen für einen kürzeren Zeitraum reduziert werden können. Diese Einschränkungen sind ebenfalls zu dokumentieren. Weiters sind interne und externe Ausweichmöglichkeiten zu untersuchen

- Finden von Ausweichmöglichkeiten um den IT-Betrieb im Notfall aufrecht zu erhalten wird erschwert, oder ist gar unmöglich
- Bei einem Ausfall von Teilen des IT-Systems fällt möglicherweise das komplette System aus

5.1.75 Erstellen eines Ersatzbeschaffungsplans

Ein Ersatzbeschaffungsplan der die Bezeichnungen der einzelnen Komponenten, den Hersteller, den Lieferanten, die Lieferzeit und die Dauer der Neuinstallation beinhaltet, muss erstellt werden.

Der Ersatzbeschaffungsplan sollte laufend aktualisiert werden. Für eingetragene Komponenten, die sich noch im Einsatz befinden, mittlerweile aber veraltet sind, sollten in dem Plan Alternativkomponenten als Ersatz eingetragen werden.

Im Plan sind die einzelnen IT-Komponenten nach Prioritäten zu sortieren, nicht jede Komponente ist für den Betrieb gleich wichtig, für manche ist sofort Ersatz zu beschaffen, für manche wird erst später oder gar kein Ersatz benötigt.

Bei der Anschaffung von neuen IT-Geräten ist abzuwiegen, welche Serviceleistungen des Verkäufers für den Betrieb am besten geeignet sind (Leasingverträge, Supportverträge, Garantieverlängerungen).

- Bei Ausfall steht der Betrieb länger Still, da kein Ersatz vorhanden ist

5.1.76 Abschliessen von Versicherungen

Zusätzlich zur Notfallplanung sind Versicherungen abzuschließen, die die Restrisiken abdecken. Je nach Art des Betriebes sind unterschiedliche Versicherungen notwendig.

Nachfolgend eine Aufstellung der verschiedenen Versicherungsarten laut [4]:

- Sachversicherungen
  - Feuerversicherung
  - Leitungswasserversicherung
  - Einbruchdiebstahlversicherung
  - Montage-/Demontage-Versicherung
  - Transportversicherung
  - Datenträgerversicherung
  - Elektronik-Versicherung
- Folgekostenversicherungen
  - Feuer-Betriebsunterbrechungs-Versicherung
  - Maschinen-Betriebsunterbrechungs-Versicherung
  - Mehrkostenversicherung
  - Elektronik-Betriebsunterbrechungs-Versicherung
- Personenbezogene Versicherungen
  - Vertrauensschadenversicherung
  - Computer-Missbrauch-Versicherung
  - Datenschutzversicherung

- Ein Notfall tritt ein der durch den Notfallplan nicht abgedeckt ist
- Der Betrieb steht für längere Zeit still und muss darauffolgend geschlossen werden

5.1.77 Endgültiges Löschen von Datenträgern

Bei Weitergabe von Datenträgern an Dritte ist darauf zu achten, dass diese total physikalisch gelöscht sind bzw. mit „sinnlosen“ Daten überschrieben sind, damit Daten vom Datenträger von Dritten nicht zu lesen sind.

Die sicherste Variante zum Löschen von Daten auf Festplatten ist das mehrmalige Überschreiben mit verschiedenen Mustern ebendieser (Tools dazu gibt es im Internet). Bei Wegwerfen sind die Datenträger mechanisch zu vernichten.

- Konkurrenz liest Daten
- Datendiebstahl

5.1.78 Richtlinien zum richtigen Löschen am PC

Bei den meisten Betriebssystemen wird beim Löschen einer Datei diese in den Papierkorb verschoben. Der Papierkorb ist dann regelmäßig zu löschen und Dateien mit sensiblen Inhalt sind ohne Umweg des Papierkorbs sofort zu löschen (unter Windows mit zusätzlichen Aktiveren der Umschalt – Taste). Um Dateien unwiderbringlich (also ohne Möglichkeit der Wiederherstellung) zu löschen, sind spezielle Löschprogramme zu verwenden, die den Speicherort der zu löschenden Datei nach der Löschung nochmals überschreiben.

- Datendiebstahl

5.1.79 Richtlinien zur Beseitigung von Restinformation bei Dateien

Vor Veröffentlichung bzw. Versand von Dateien sind diese auf Restinformationen zu überprüfen. Besonders ist zu achten auf Kommentare und verborgenen Text.

- Unbeabsichtigte Weitergabe von sensiblen Informationen

5.1.80 Richtlinien für den Austausch von Datenträgern

Bevor ein Datenträger mit den zu übermittelten Daten beschrieben wird und weitergegeben wird, sollte er vollständig formatiert werden. Auch nach Erhalt des Datenträgers und Einspielen der Daten, sollte er wieder vollständig formatiert werden. Zusätzlich hat eine vollständige Virenprüfung stattzufinden. Bei Austausch von vertraulichen Informationen sollten diese vorher verschlüsselt werden.

- Daten die nicht für den Empfänger gedacht sind können sich noch auf dem Datenträger befinden

- Zugriff auf sensible Daten durch unbefugte Dritte
- Virenbefall

5.1.81 Maßnahmen zum sicheren Umzug

Auch beim Umzug ist auf die bestehenden Zugriffs und Zugangsrechte zu achten. Vor dem Umzug sind Datensicherungen vorzunehmen. Die Datensicherungen sollten getrennt vom IT – System transportiert werden. Um eine rasche Inbetriebnahme zu gewährleisten sollte am neuen Umzugsort die technische Infrastruktur (Server in Betrieb, Verkabelung etc.) schon zur Verfügung stehen.

- Zugriff auf sensitive Daten und Programme durch Dritte
- Datenverlust
- Diebstahl von IT – Komponenten
- Verzögerung der Inbetriebnahme des IT – Systems

5.2 Sicherheitsmaßnahmen im Bezug auf Netzwerke

5.2.1 Geeignete Netzwerktopographie und Kabeltypen

Das Netzwerk sollte strukturiert in Stern- oder Baumform verkabelt werden.

Hierzu sollten zur Verbindung von Gebäuden (Primärbereich) und zur Verbindung von Stockwerken (Sekundärbereich) Lichtwellenleiter verwendet werden. Für die Etagenverkabelung(Tertiärbereich) sollten Twisted-Pair-Kabel der Kategorie 5 oder höher verwendet werden.

- Netzwerk ist nicht erweiterbar
- Dokumentation des Netzwerkes ist schwierig

5.2.2 Dokumentation und Kennzeichnung der Netzwerkverkabelung

Die Verkabelung sollte genau dokumentiert werden. Weiters ist auch eine Kennzeichnung der Kabel am Patchfeld und auf der Netzwerkdose notwendig.

Die Dokumentation sollte zumindest folgende Punkte beinhalten [4]:

- genauer Kabeltyp,
- nutzungsorientierte Kabelkennzeichnung,
- Standorte von Zentralen und Verteilern mit genauen Bezeichnungen,
- genaue Führung von Kabeln und Trassen in der Liegenschaft (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- Trassendimensionierung und -belegung,
- Belegungspläne aller Rangierungen und Verteiler,

    - Nutzung aller Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
    - technische Daten von Anschlusspunkten,
    - Gefahrenpunkte,
    - vorhandene und zu prüfende Schutzmaßnahmen.
- Erschwerung der Wartung und Instandsetzung
- Fehlersuche fast unmöglich

5.2.3 Zweckmäßige Aufstellung von Netzwerkkomponenten

Aktive Netzwerkkomponenten (wie Router, Firewall, etc.) sollten vor unbefugten Zugriff geschützt werden, indem man diese Netzwerkkomponenten in einem eigenen Serverraum betreibt oder in einem Schutzschrank wegsperrt. Es ist auch beim Betrieb von Netzwerkkomponenten wichtig, dass man auf die Betriebsvorgaben, wie Toleranzgrenzen bei Temperatur und Feuchtigkeit, achtet. Außerdem müssen die Geräte so aufgestellt werden, damit sie vor elektromagnetischen und magnetischen Feldern geschützt sind.

- Beeinträchtigung der Funktionalität durch elektromagnetische Abstrahlung
- Auslesen bzw. Manipulation der Konfigurationsdaten durch unbefugten Zugriff
- Diebstahl von teuren Netzwerkkomponenten

5.2.4 Richtlinien zur sicheren Nutzung von Netzwerkkomponenten

Beim Router ist darauf zu achten, welche Protokolle weitergeleitet werden sollen und welche IT – Systeme in welche Richtung über den Router kommunizieren. Dies ist mit bestimmten Filterregelungen zu bewerkstelligen. Mittels MAC – Adresse der IT – Komponenten sollte der Zugriff auf Ports von Switches und Hubs geregelt werden. Die Routing – Updates der Routing Tabellen sind entweder durch Passwort oder kryptographische Prüfsumme zu sichern. Bei Routern sind Dienste abzuschalten, die nicht benötigt werden (z.B. Telnet, FTP, Pop3).

Bei allen Netzwerkkomponenten sind die Default – Passwörter und Einstellungen zu ändern. Bevor alle Netzwerkkomponenten in das Produktionsnetz gestellt werden, ist eine sichere Grundkonfiguration herzustellen und die jeweilige Netzwerkkomponente ist in einem gesicherten Testnetz zu testen. Nach der Grundkonfiguration ist ein Backup ebendieser auf einem gesicherten Medium durchzuführen (wichtig: Medium ist neutral zu beschriften). Die Administration der Netzwerkkomponente sollte nur lokal stattfinden und falls ein Remotezugriff notwendig ist, hat dieser nur über ein sicheres Protokoll stattzufinden. Falls ein Login – Banner mit wesentlichen Informationen des Gerätes, wie Versionsnummer, Modelnummer oder Softwareversion, angezeigt ist, ist dieser unbedingt abzuschalten bzw. mit Fehlinformationen zu füttern (z.B. Anzeige

unkorrekter Modelnummer). Speziell bei Routern und Switches sollte die Protokollierung aktiviert werden und laufend ausgewertet werden.

- Zugriff auf das Netz durch Fremde
- Manipulation der Routing – Tabellen

5.2.5 Sicherung der Konfigurationsdaten von Netzwerkkomponenten

Die Konfigurationsdaten aktiver Netzwerkkomponenten (Router, Firewall) müssen in regelmäßigen Abständen gesichert werden.

Weiters muss stichprobenmäßig eine Überprüfung der Sicherungen erfolgen und auch überprüft werden, ob mittels der Sicherungen die Konfiguration der Komponenten wiederhergestellt werden kann.

- Bei Absturz von Netzwerkkomponenten ist es schwer und langwierig die einzelnen Konfigurationen wiederherzustellen

5.2.6 Klimatisierung

Der Einsatz eines Klimagerätes ist erforderlich und um den laufenden Betrieb des Klimagerätes zu gewährleisten ist eine regelmäßige Wartung wichtig. Beim Einbau des Klimagerätes ist auf wasserführende Leitungen zu achten (siehe Kapitel 5.1.15)

- Bei Betrieb der IT - Infrastruktur außerhalb der zulässigen Betriebstemperatur kann es zu beeinträchtigter Funktionalität kommen oder gar zum Ausfall
- Bei nicht durchgeführter Wartungen kann es zum Ausfall des Klimagerätes kommen

5.2.7 Zweckmäßige Aufstellung von Schutzschränken

Bei Aufstellung von Schutzschränken ist auf die Tragfähigkeit des Fußbodens zu achten. Schutzschränke mit kleineren Dimensionen und Gewicht sollten mit der Wand verankert werden. Des Weiteren ist auf die elektromagnetische Strahlung, die eventuell von benachbarten Geräten (vor allem Geräte aus dem industriellen Bereich) ausgeht, zu achten. In diesem Fall ist ein Einbau von Filtern oder Türdichtungen im Schrank empfehlenswert.

Wichtiger Aspekt bei Schutzschränken ist noch der Austausch der Schlösser, da die meisten Schutzschränke einer „Produktionslinie“ mit dem gleichen Sicherheitsschloss versehen werden. Bei der Beschaffung des Serverschutzschrankes ist darauf zu achten, dass der Schutzschrank ausreichend Platz für Server, Tastatur und etwaige Peripheriegeräte bietet. Bei Nichtbenutzung ist der Schutzschrank abzuschließen.

- Durchbruch durch Fußboden
- Diebstahl des Schutzschrankes
- Diebstahl aus dem Schutzschrank

- Beeinträchtigte Funktionalität durch elektromagnetische Abstrahlung
- Zugang zum Schutzschrank mit Standardschlüssel

5.2.8 Serverraum

Bei der Standortwahl des Serverraums sollte man darauf achten bestimmte Gefährdungspotentiale, wie z.B. Wassereinbruch oder Störquellen durch Mobilfunk - Sendeeinrichtungen, zu minimieren. Bei der technischen Infrastruktur im Serverraum ist des Weiteren darauf zu achten, dass Redundanzen vorhanden sind. Der Zutritt zum Serverraum soll durch Kontrollenmechanismen geschützt werden und überhaupt sollte der Zugang nur auf einen bestimmten Personenkreis beschränkt werden, daher keine öffentlich zugänglichen Gerätschaften, wie Kopierer, im Serverraum aufstellen. Externe Mitarbeiter oder betriebsfremde Personen dürfen nur unter Aufsicht den Serverraum betreten. Diesen Personen sollte die Mitnahme von mobilen IT - Systemen, Kameras, mobilen Speichermedien (wie z.B. USB - Stick) und Mobiltelefonen verboten werden. Auf ein Rauchverbot ist zu achten!

- Manipulation von Daten
- Diebstahl von betriebswichtigen Daten
- Bei fehlender Redundanz kommt es durch Ausfall einer Komponente zu vollständigen Ausfall der gesamten technischen Infrastruktur
- Manipulation der technischen Infrastruktur im Serverraum

5.2.9 Protokollierung am Server

Am Server ist eine Protokollierung des Netzes erforderlich, diese sollte in regelmäßigen Abständen überprüft und ausgewertet werden. Vor allem sicherheitsrelevante Ereignisse wie falsche Passworteingabe, Sperrung eines Benutzeraccounts durch mehrmaliges falsches Einloggen und der Versuch eines nicht berechtigten Benutzers sich einzuloggen, sollten mitprotokolliert werden. Weiters ist die Netzauslastung aufzuzeichnen.

- Eindringen Unbefugter ins Netzwerk
- Überlastung des Netzes

5.2.10 Rechtevergabe

Die Benutzer im Netzwerk dürfen nur auf solche Dateien Zugriff erhalten, die sie für ihre Tätigkeit benötigen. Weiters ist auch auf die richtige Zugriffsart zu achten, das heißt wenn ein Benutzer eine Datei nur zum lesen benötigt, dann braucht er auch nur das Zugriffsrecht „lesen“ für diese Datei. Am Server sollte für jeden Benutzer eine Speicherplatzbeschränkung eingerichtet werden.

- Einsicht in sensible Daten von Unbefugten

- Unbeabsichtigtes Löschen oder Verfälschung von Daten
- Speicherkapazität des Servers wird aufgebraucht

5.2.11 Dokumentation der Netzsituation

Die Netztopographie ist hinsichtlich folgender Punkte

- Aktuelle Kabelführung
- Standorte der Netzteilnehmer
- Verwendete Kabeltypen und deren festgelegte Anforderungen an den Schutz

zu dokumentieren.

Bei der Netztopologie ist es notwendig, die Segmentierung der einzelnen OSI – Schichten zu erfassen. Für die einzelnen Segmente sind die verwendeten Netzprotokolle und die daraus folgenden Konfigurationen (z.B. IP – Adressen, Subnetmasken etc.) zu beschreiben. Weiters sollte dokumentiert werden, welche Dienste zugelassen sind und welche nicht (z.b. Telnet, SMTP, POP3, etc.).

Jede Änderung der Netzsituation ist neuerdings zu dokumentieren und die erstellten Dokumente sind vor unbefugten Zugriff zu schützen.

5.2.12 Schutzbedarfserstellung des Netzes

Es sind die Anforderungen an Integrität, Verfügbarkeit und Vertraulichkeit an das Netz zu dokumentieren. Der darauf folgende Schritt sollte sein, dass man das Netz auf diese Anforderungen hin untersucht. Einen besonderen Augenmerk sollte darauf gerichtet werden, ob bestimmte Netzwerkkomponenten redundant vorhanden sind, d.h. bei Ausfall einer bestimmten Netwerkkomponente sollte automatische eine andere einspringen.

- Ausfall des Netzes

5.2.13 Datensicherung am Server

Die Sicherung des Servers muss in regelmäßigen Abständen erfolgen und es müssen alle für den Betrieb wichtigen Daten gesichert werden. Weiters muss stichprobenmäßig eine Überprüfung der Sicherungen erfolgen und auch überprüft werden, ob mittels der Sicherungen eine vollständige Wiederherstellung der Daten möglich ist.

- Gelöschte Daten können nicht wieder hergestellt werden
- Bei Ausfall von Speichermedien sind die gespeicherten Daten verloren

5.2.14 Notfallplan für den Server

Es sollte ein Notfallplan für den Ausfall des Servers erstellt werden, dabei sind folgende Aspekte zu berücksichtigen: [4]

- Die Notfallplanung für den Server muss in den existierenden Notfallplan integriert werden.
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist im Rahmen des allgemeinen Datensicherungskonzepts ein Datensicherungskonzept für den Server zu erstellen. Darin muss nicht nur der Server selbst berücksichtigt werden, sondern auch die Systeme, von denen der Betrieb des Servers abhängt.
- Im Rahmen von Wartungs- und Serviceverträgen oder durch eigene Lagerhaltung muss die Versorgung mit Ersatzteilen innerhalb einer Frist sichergestellt werden. Die Ausfallzeit ist daher auf ein tragbares Maß zu reduzieren. Bei besonderen Anforderungen an die Verfügbarkeit des Servers muss gegebenenfalls eine Hochverfügbarkeitslösung eingesetzt werden.
- Die Systemkonfiguration muss dokumentiert werden. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann. Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen, sondern Handlungsanweisungen sollten auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD gesondert hinterlegt werden.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.
- Alle notwendigen Vorgehensbeschreibungen müssen regelmäßig überprüft und geprobt werden. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Betriebssystemen berücksichtigt werden.

5.2.15 Regeln für Benutzer- Accounts

Die User-Accounts sollten, wenn das möglich ist, zeitlich beschränkt werden. Der User sollte nur zu seinen Arbeitszeiten Zugriff auf das System bekommen und außerhalb der Arbeitszeit sollte der Account gesperrt werden. Wenn ein User nur auf einem PC Zugang benötigt, dann sollte der Login für ihn auch nur auf diesem PC möglich sein.

Wenn ein Account länger nicht benötigt wird, dann ist dieser zu löschen. Weiters sind auch die Accounts von ehemaligen Mitarbeitern zu löschen.

- Zugriff auf sensible Daten durch unbefugte Dritte
- Manipulation der IT-Komponente

5.2.16 Richtlinien zum Einsatz eines Servers

Durch Partitionierung der Festplatte ist das Betriebssystem von den Anwendungsprogrammen zu trennen. Der Server ist nicht im gleichen IP – Subnetz, wie die Clients zu betreiben und ist durch einen Paketfilter oder Application Level Gateway vom anderen Netz zu trennen. Der Server sollte nur die Dienste zur Verfügung stellen, die auch wirklich benötigt werden. Die verwendeten Dienste sollte nur authentifizierten Benutzern zur Verfügung gestellt werden. Für die Rechtevergabe ist ein Benutzer- und Gruppenkonzept zu verwenden. Ein Zugriff über das Internet auf den Server hat nur gesichert (z.B. über VPN) zu erfolgen. Die Auslastung des Servers sollte überwacht werden (Monitoring). Weiters sollten alle Aktivitäten des Servers mit protokolliert und ausgewertet werden. Der Server sollte in einem abschließbaren Raum stehen und es ist zu regeln wer für die Administration des Servers zuständig ist. Empfehlenswert ist eine lokale Administration, falls eine Remote – Administration von Nöten ist, hat diese über ein sicheres Protokoll (z.B. ssh, https) stattzufinden. Vom Administrator ist zu regeln, wer welche Dienste des Servers in Anspruch nehmen darf. Wenn möglich sind Software – Updates zuerst in einer Test – Umgebung zu testen und dann erst dürfen diese auf dem Hauptsystem installiert werden.

- Absturz des Servers
- Zugriff auf Server durch Unbefugte
- Manipulation, Diebstahl und/oder Fälschung von Daten
- Überlastung des Servers

5.2.17 Richtlinien für den Client Betrieb

Es ist festzulegen, wer für die Administration der Clients zuständig ist. Durch Partitionierung der Festplatte ist das Betriebssystem von den Anwendungsprogrammen zu trennen. Es muss im Vorfeld der Installation geplant werden auf welche Dienste im Netz der Client Zugriff haben soll. Auch beim Client ist regelmäßig das Einspielen von Patches und Updates von Nöten. Es ist empfehlenswert eine Referenzinstallation zu erstellen um Updates und Patches vor dem Einspielen zu testen und um die Installation von neuen Clients zu vereinfachen (Image). Die Protokollierung sollte am Client aktiviert werden und auch regelmäßig ausgewertet werden. Weiters ist festzulegen, ob der Client von einem oder mehreren Benutzer verwendet werden soll. Der Benutzer darf keinen Zugriff auf Systemdateien haben. Der Client – Rechner ist am Ende des Arbeitstages ordnungsgemäß runterzufahren. Das Booten von externen Medien ist im BIOS zu unterbinden und nur für den Notfall ist ein Bootmedium zu benutzen. Bei Verwendung von verteilten Dateisystemen ist eine Regelung einzuführen um inkonsistente Daten zu vermeiden (z.B. nur ein Schreibzugriff zur gleichen Zeit, Abgleichung von Dokumenten etc., Transaktionen). Empfehlenswert ist eine lokale Administration, falls eine Remote – Administration von Nöten ist, hat diese über ein sicheres Protokoll (z.B. ssh, https) stattzufinden.

- Keine Konnektivität zum Server
- Ausfall des Clients
- Datenverlust
- Inkonsistenz von Daten
- Virenbefall

5.2.18 Zugang zum Internet

Verwenden sie für den Zugang zum Internet einen Router mit integrierter Firewall, die meisten ISP stellen solche Router zur Verfügung. Binden sie nie einen Rechner direkt an das Internet. Sperren Sie nicht benötigte Ports auf dieser Firewall. Wenn es die Einstellung „Protokollierung von Ereignissen“ auf dem Router gibt aktivieren sie diese und werten sie das Protokoll regelmäßig aus. Dokumentieren Sie die Konfigurationseinstellungen des Routers.

- Gefährdung des Internen Netzes durch Viren, Würmer und Trojaner
- Gefahr, dass unbefugte an interne sensible Daten gelangen

5.2.19 Wahl eines Mail – Providers

Bei der Wahl eines Mail – Providers ist darauf zu achten, dass dieser seinen Hauptsitz im Inland hat.

- Mail wird über viele Gateways weitergeleitet, daher erhöhte Gefahr des Mitlesens

5.2.20 Festlegung einer Mail – Richtlinie

Es ist festzulegen welchen Benutzer einen Mail – Account erhält. Dabei ist es sinnvoll Namenskonventionen bei den Mail – Adressen eines Betriebs aufzustellen bzw. einzuhalten. Die Mail – Programme sollten vom Administrator so konfiguriert werden, dass diese maximale Sicherheit für den Benutzer liefern. Bei Nutzung von Webmail siehe Kapitel 5.2.32. Für alle ausgehenden Mails ist eine Signatur zu verwenden. Bei Versand von Mails an mehrere Benutzer ist darauf zu achten, dass die komplette Empfängerliste nicht bei den einzelnen Empfängern zu sehen ist. Bei längerer Abwesenheit ist eine Weiterleitung von Mails einzurichten und eine Benachrichtigung über die Abwesenheit des Empfängers ist an den Absender zu senden. Bei Versand mit Anhang sollte der Empfänger über Art der Datei und den Inhalt ebendieser informiert werden. Ein Virenscanner ist sowohl bei ein-, als auch ausgehenden Mail einzusetzen.

- Virenverseuchung
- Mitlesen von Mails
- Nichtlesen von Mails

5.2.21 Auswahl eines Internet – Providers

Bei der Wahl sollte darauf geachtet werden, dass eine hohe Verfügbarkeit garantiert ist und wie dieser auf Ausfall der IT – Systeme vorbereitet ist. Weiters sollte der Provider eine regelmäßige Überprüfung auf Stabilität der Verbindungen vornehmen.

- Ausfall der Internet – Verbindung
- Eingeschränkte Verfügbarkeit

5.2.22 Zentraler Netzzugang

Der Zugang zum Internet muss über einen zentrale, gesicherte Stelle (z.b. Firewall) erfolgen. Diese Zugangsstelle darf auf keinen Fall umgangen werden (z.B. externen W – Lan Anbieter oder mitgebrachte Modems).

Für den Zugang zum Internet sollten folgende Punkte geklärt werden: [4]

- Zuständigkeiten für Installation, Wartung und Betreuung
- Festlegung des Benutzerkreises und der Nutzungsberechtigungen
- Vorgaben und Sicherheitsmaßnahmen für die Benutzung
- Festlegung der möglichen Kommunikationspartner
- Nutzungszeiten
- Vertretungsregelung
- Protokollierung
- Sichere Konfiguration der Datenübertragungseinrichtungen

5.2.23 Regelungen für PCs mit Internet – Zugang

Nur Mitarbeiter, die zur Erledigung ihrer Tätigkeit einen Internetzugang benötigen, sollen einen PC mit Zugang zum Internet erhalten.

Es sollte festgelegt werden welche Dienste (WWW, E-Mail, Internet-Telefonie etc.) im Internet genutzt werden dürfen und dies soll auch dokumentiert werden. Weiters soll auch dokumentiert ob aktive Inhalte (ActiveX, Java, etc.) auf dem Rechner ausgeführt werden dürfen. Bei Datenweitergabe (E-Mail, Ausfüllen von Formularen etc.) sind Regelungen für Mitarbeiter zu treffen, welche Daten sie über das Internet weitergeben dürfen. Rechner mit Internetzugang sind regelmäßig einer Virenprüfung zu unterziehen. Eine weitere Sicherheitsmassnahme ist die Installation einer Software - Firewall.

Es sind regelmäßig Updates und Patches zu installieren. Falls nicht benötigt sollte bei Windows – PCs die Datei- und Druckerfreigabe deaktiviert werden, ebenfalls deaktiviert werden sollte die automatische CD-Rom Erkennung. Weiters ist das Administrator – Konto umzubenennen und mit einen sicheren Passwort zu versehen (siehe Kapitel

5.1.51). Ebenfalls sollten die Standardnamen der Systemordner und der Datenverzeichnisse umbenannt werden.

Im Betrieb sind regelmäßige Kontrolle durchzuführen, ob Software-Komponenten entfernt bzw. zusätzlich installiert wurden, ob die BIOS- und Betriebssystemeinstellungen unerlaubt geändert wurden, sowie ob die Hardwarekonfiguration verändert wurde. Die Protokolldaten sind laufend auszuwerten.

Bei Benutzung von E-Commerce Anwendung ist darauf zu achten, dass bei Eingabe von persönlichen Daten, diese über eine gesicherte Verbindung (SSL) passiert. Ein Hinweis auf eine sichere Verbindung ist ein geschlossenes Schloss in der Statuszeile des Browsers.

- Gefahr von Viren, Trojanern und Würmern
- Zugriff auf Firmendaten durch unbefugte Dritte
- Angriff von Schadprogrammen auf Standardverzeichnisse

5.2.24 Sicherheit von WWW - Browsern

Beim herunterladen von Dateien ist Vorsicht geboten. Man sollte nur Dateien von vertrauenswürdigen Quellen herunterladen. Das gleiche gilt für die Installation von Plug - Ins. Weiters sollten in den Browsereinstellungen die Annahme von Cookies deaktiviert werden, ActiveX und JavaScript sollten ebenfalls deaktiviert werden. Die temporären Internetdateien sowie die Verlaufliste sind regelmäßig zu löschen. Wenn sensible Daten wie Kreditkartennummern und der Gleichen über das Internet übertragen werden, dann ist darauf zu achten, dass die Kommunikation über das sichere Protokoll https erfolgt. Dies ist bei den meisten Browsern an einem geschlossenen Schlosssymbol in der rechten unteren Ecke des Browserfensters erkennbar. Weiteres Erkennungsmerkmal für einen sicheren Kommunikationsweg für die Übertragung der Daten ist, daß statt dem üblichen „http://“[3] ein „https://“[4] der Web - Adresse vorangestellt ist.

- Viren, Trojaner, Würmer auf Rechnern im Netzwerk
- Unbefugte erhalten Zugriff auf sensible Daten

5.2.25 Einzelrechner zur Nutzung des Internets

Wenn das Internet für die tägliche Arbeit im Betrieb nicht benötigt wird, wird der Einsatz eines Rechners, der nur für die Kommunikation mit dem Internet zuständig ist, empfohlen. Diese Rechner darf nicht mit dem internen Netz verbunden sein.

- Viren, Trojaner, Würmer auf Rechnern im Netzwerk
- Unbefugte erhalten Zugriff auf sensible Daten

[3] HyperText Transfer Protocol
[4] HyperText Transfer Protocol Secure; sicheres Hypertext - Protokoll

5.2.26 Schutz vor Spammails

Folgende Punkte sollten zum Schutz vor Spammails eingehalten werden:

- Benutzer müssen über die Problematik der Spammails Bescheid wissen.
- Die Firmenemailadresse darf nicht ohne weiteres weitergegeben werden.
- Auf dem Emailserver sollten E-Mail-Filterprogramme eingesetzt werden.
- Für die firmeneigene Webseite ist zu überlegen welche E-Mail-Adressen angegeben werden, da diese für Spammails genutzt werden können.
- Überlastung des Mail-Systems
- Arbeitszeit um Spammails zu löschen

5.2.27 Aktualisierung von E-Mail-Verteilerlisten

E-Mail-Verteilerlisten die entweder zentral auf einem Mailserver liegen, oder sich im Mail-Client des Benutzers befinden, sind laufend zu aktualisieren.

- Mails kommen nicht beim Empfänger an (Mailadresse stimmt nicht mehr)
- Falsche Person erhält die Mails (ist nicht mehr dafür zuständig)

5.2.28 Verwendung von NAT(Network Adress Translation)

Um das interne Netz sicherer zu machen sollte NAT verwendet werden. Die internen IP-Adressen sollten dafür in einem der folgenden Bereiche liegen:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255
- Höheres Sicherheitsrisiko

5.2.29 Nicht benötigte Netzdienste deaktivieren

Dienste die im Netzwerk nicht benötigt werden sind zu deaktivieren.

Einerseits sind die nicht benötigten Dienste auf dem Server zu deaktivieren und andererseits sind die nicht benötigten Ports der Dienste auf dem Router, oder der Firewall zu sperren.

- Eindringen in das Netzwerk durch Unbefugte
- Höheres Sicherheitsrisiko

5.2.30 Personal Firewalls

Zusätzlich zu einer zentralen Firewall ist es sinnvoll ein personal Firewall auf den einzelnen Client-PC's einzusetzen.

Die Personalfirewall muss so konfiguriert werden, dass der Benutzer nicht andauernd Warnmeldungen erhält. Die Filterregeln sollten so eingestellt werden, dass alles verboten ist was grundsätzlich nicht erlaubt ist. Wenn es die Einstelllung erlaubt, sind die Ports 137, 139 und 445 zu sperren. Weiters ist eine Protokollierung der Ereignisse ratsam.

Nach dem Konfigurieren und darauf in regelmäßigen Abständen folgend, ist zu überprüfen ob die Regeln der Firewall auch greifen.

- Schadsoftware auf den Clientrechnern durch das Surfen im Internet oder über E-Mails
- Zentrale Firewall wird nicht entlastet

5.2.31 Wahl der Internet-Anbindung

Bevor die Internet-Anbindung gewählt wird, sollte überlegt werden für welche Zwecke man das Internet benötigt. Je nach Umfang des Surfverhaltens werden von den Internet Service Providern (ISP) verschieden Zugangspakete angeboten.

- Überlastung der Internetverbindung
- Internetverbindung wird nicht ausgelastet (unnötige Kosten)

5.2.32 Richtlinien für die Benutzung von Webmail

Bei der Auswahl des Webmailanbieters sind folgende Punkte zu berücksichtigen:

- Erfolgt die Anmeldung über eine sichere Verbindung?
- Werden meine E-Mails auf Viren geprüft?
- Ist eine Spamfilterung möglich?
- Wie bekomme ich ein neues Passwort, wenn ich mein altes verloren habe?
- Sind die AGBs auf der Seite des Webmailanbieters zu finden?
- Wie wird mit meinen persönlichen Daten umgegangen?

Wenn ein passender Anbieter gefunden wurde, sind bei der Benützung des Webmailaccounts noch folgende Punkte zu beachten:

- Das Passwort für den Zugang zum Webmailaccount muss mindestens 8 Zeichen lang sein und sollte aus alphanumerischen Zeichen bestehen.
- Die Abmeldung muss immer über den Logout-Button erfolgen
- Die E-Mails sollten regelmäßig gelesen und unwichtige Mails gelöscht werden
- Wichtige Mails sind zusätzlich noch lokal zu sichern
- Gefährdung des internen Netzes durch Viren, Würmer und Trojaner

- Spammails
- Gefahr, dass unbefugte an interne sensible Daten gelangen

5.2.33 Sicherer Versand von E-Mails

Wenn sie vertrauenswürdige E-Mails versenden, sollten die E-Mails verschlüsselt und wenn möglich zusätzlich mit einer Signatur versehen werden.

- Gefahr, dass unbefugte an interne Informationen gelangen

5.2.34 Verwaltung von Internet – Domänen

Internet – Domänen müssen bei der entsprechenden Registrierungsstelle angemeldet werden. Falls die Registrierung über einen Internetdienstleister geschieht, ist darauf zu achten, dass die Rechte über die Domain bei der eigenen Organisation bleiben.

- Keine Rechte über eigene Domäne

5.2.35 Sicherung von E-Mails

Wenn im Unternehmen kein E-Mail-Server existiert müssen die E-Mails von jedem Client-PC in regelmäßigen Abständen gesichert werden. Weiters ist zu überprüfen ob anhand der Backups eine Wiederherstellung der E-Mails möglich ist.

- Gelöschte Mails können nicht wiederhergestellt werden.

5.2.36 Sichere Anmeldung bei Internet – Diensten

Bei Anmeldung zu Internet – Diensten solle man sich zweimal überlegen, welche Daten man preisgibt. Die Weitergabe von personenbezogenen Daten sollte nur über eine sichere Verbindung (z.B. SSL) erfolgen. Für verschiedene Internet – Dienste sollte man auch verschiedene Passwörter benutzen (Weitere Details siehe Kapitel 5.1.51).

- Missbrauch von Daten
- Datendiebstahl

5.2.37 Richtlinien für den W – Lan Einsatz

Es sollte festgelegt werden wer für die Installation, Konfigurierung und Administration von W-Lan Komponenten zuständig ist. Der Access – Point sollte so gewählt werden, dass die Funkabdeckung möglichst maximal ist (siehe Kapitel 5.2.38). Bei der Installation aller W – Lan Komponenten sind die Grundkonfiguration und die Standardpasswörter zu ändern. Weiters sollte die vorgenommene Konfiguration gesichert werden. Weiters ist festzulegen welche Daten über das Funk – Netz transportiert werden dürfen und an welche anderen internen oder externen Netze an das W – Lan Netz

gekoppelt werden darf. Wichtig ist, dass das W-Lan nur im Infrastruktur Modus laufen darf, d.H. der Ad – Hoc Modus ist zu deaktivieren. Als Standard sollte 802.11b/g oder höher verwendet werden. Als Kryptoverfahren sollte WPA oder WPA2 gewählt werden. Die kryptografischen Schlüssel müssen auf jeden Fall mindestens aus 20 alphanumerischen Zeichen bestehen und regelmäßig sind die Schlüsselinformation bei allen W – Lan Komponenten auszuwechseln. Bei der Beschaffung von neuen W – Lan Komponenten ist darauf zu achten, dass die neuen Komponenten kompatibel zu den Alten sind. Die Administration des Access – Points sollte nur über ein sicheres Protokoll (z.B. https, SSH) und drahtgebunden erfolgen. Dienste, die nicht benötigt werden (z.B. Telnet, FTP etc.). sind zu deaktivieren. Wenn es die Konfiguration des Access – Points ermöglicht sollte die MAC – Adressfilterung aktiviert werden. Die voreingestellte SSID ist zu ändern und der SSID – Broadcast sollte deaktiviert werden. Wenn möglich sollte der DCHP – Server im Accesspoint deaktiviert werden und statische IP – Adressen vergeben werden.

- Benutzung des firmeninternen Netzes durch Dritte
- Manipulation, Fälschung und Diebstahl der übertragenen Daten
- W – Lan Komponenten nicht kompatibel untereinander

5.2.38 Montage und Positionierung von Access - Points

Access - Points sollten gut getarnt an einer nicht einsehbaren Stelle in einem Metallgehäuse untergebracht werden. Bei der Positionierung sollte man darauf achten, dass der Abdeckungsbereich der Funkwellen nur die Gebiete erreicht, die per W-Lan versorgt werden sollten. Bei Aufstellung des Access - Points außerhalb eines Gebäudes muss dieser vor Witterungsbedingungen und bei Dachinstallation weiters vor Blitzschlag geschützt werden (Außeninstallation nicht empfehlenswert).

- Manipulation des Access - Points durch Unbefugte
- Zerstörung des Access - Points durch Wassereinbruch bei starkem Regen oder Schneefall
- Eindringen ins interne Funknetz durch Außenstehende (z.B. Firma im Nebenraum)

5.2.39 WLAN an LAN anbinden

Zugriffe aus dem WLAN an das drahtgebundene LAN dürfen nur über Sicherheitsgateways (Firewalls) stattfinden.

Eine laufende Überwachung der WLAN-Infrastruktur und ein

regelmäßiger Sicherheitscheck sollte durchgeführt werden. Weiters sind alle Ereignisse im WLAN zu protokollieren und auszuwerten.

- Gefahr durch Zugriff von Unbefugten auf das Firmennetzwerk

5.2.40 Korrekter Betrieb des Mail-Servers

Es muss gewährleistet sein, dass der Mailserver lokale Mails nur intern weiterleitet und nicht ins öffentliche Netz. Der Mailserver selbst muss gegen Zugriff von unbefugten Personen geschützt werden und sollte daher in einem versperrten Serverraum stehen. Für die Wartung und Konfiguration des Servers sollte ein Administrator zuständig sein. Der Server ist so einzurichten, dass der Benutzer darüber informiert wird, wenn die versendete E-Mail den Empfänger nicht erreicht. Es ist ratsam, dass auf dem Mailserver keine weiteren Dienste laufen um den Server im Notfall auch herunterfahren zu können. Die Benutzer sollten im Normalfall nur Zugriff auf ihr eigenes Postfach haben. Die Ereignisse auf dem Server sind mit zu protokollieren und die Protokolle sollten regelmäßig ausgewertet werden. Auf dem Mail-Server muss ein Antivirenprogramm installiert werden, dass laufend aktualisiert wird. Der Server ist durch eine Firewall zu schützen. Weiters muss der Server davor geschützt werden, dass er missbräuchlich zur Weiterleitung von Spam - Mails verwendet wird (Spam - Relay). Im Netzwerk sollte der E-Mail-Server in einer DMZ des Paketfilters angesiedelt werden. Es sind regelmäßige Kontrollen des freien Speicherplatzes angebracht.

- Interne Mails mit sensiblen Daten werden ins öffentliche Netz versendet
- Die E-Mails kommen beim Empfänger nicht an, Absender erhält keine Nachricht darüber
- Der E-Mail-Server wird sabotiert und kann seine Tätigkeit nicht mehr ordnungsgemäß ausführen
- Benutzer erhält Einsicht in Daten die nicht für ihn bestimmt sind
- Der E-Mail-Server empfängt und versendet die Mails nicht mehr korrekt, dass wird aber von den Benutzern und dem Administrator gar nicht oder erst zu spät bemerkt
- Der Server wird als Spam-Relay verwendet

5.2.41 Konfiguration der E-Mail-Clients

Die folgenden Punkte sollten bei der Konfiguration der Mail-Clients berücksichtigt werden:

- Auf jedem Client ist ein Antivirenprogramm zu installieren, dass regelmäßig mit den neuesten Virendefinition upgedatet wird.
- Als Antwortadresse ist die offizielle Adresse des Benutzers zu wählen.
- Die Abholung der Mails vom Server durch das Clientprogramm sollte nicht öfter als alle 30 Minuten erfolgen.
- Die serverseitigen Postfächer sollten eine Größenbeschränkung haben und der Benutzer ist zu informieren, wenn er die Größe erreicht hat.
- Werden E-Mails von POP3 Postfächern abgeholt, dann sind sie dort zu löschen.
- Es sollten keine HTML-formatierten E-Mails versendet werden können.

- Beim öffnen von HTML-formatierten E-Mails sollten diese als Text geöffnet werden.
- Ausführbare Dateien als Anhänge sollten nicht aus dem Mailprogramm heraus geöffnet werden können.
- Spammails
- Überlastung des Netzes
- Vergeudung von unnötigen Speicherplatz
- Computervirengefahr

5.2.42 Sicherung des Mail-Servers

Der Mail-Server samt Postfächern muss in regelmäßigen Abständen gesichert werden. Weiters ist zu überprüfen, ob mittels der Backups eine komplette Wiederherstellung des Mailservers, wie auch eine Wiederherstellung einzelner Postfächer möglich ist.

- Bei Ausfall des Mailservers ist keine Wiederherstellung möglich
- Gelöschte Mails können nicht wiederhergestellt werden.

5.2.43 Einsatz eines Webservers

Je nach Anforderung kann ein Webserver auf drei Unterschiedliche Arten Betrieben werden.

- Keine Verwendung eines Reverse Proxy
- Verwendung eines Reverse Proxy
- Verwendung eines Reverse Proxy mit zusätzlichem Paketfilter

Keine Verwendung eines Reverse Proxy

Halten sich die Anfragen an den Webserver in Grenzen und bestehen auch keine besonderen Anforderungen an die Sicherheit des Webservers dann sollte sich der Webserver in der DMZ des externen Paketfilters befinden. Es müssen dann entsprechende Paketfilterregeln für den Webserver definiert werden. Weiters ist der Webserver ausschließlich über eine SSH-Verbindung zu konfigurieren und auf dem Webserver ist kein DNS zu verwenden.

Eine Empfehlung für die Filterregeln nach dem GSH [4] lautet wie folgt:

Quelle	Ziel	Entscheidung	Bemerkungen
Allgemein			
Webserver	externes Netz und internes Netz	Nur Pakete erlauben, die zu einer Verbindung gehören, die vom anderen Rechner initiiert wurde	Der Webserver antwortet nur auf Anfragen. Eigene Verbindungen brauchen nicht aufgebaut zu werden
Kommunikation des Webservers mit dem Internet			
Externes Netz	Webserver Port 80	erlauben	Port 80 ist der Standardport
Externes Netz	andere Ports des Webservers	verbieten	
Kommunikation des Webservers mit dem internen Netz			
Internes Netz	Webserver Port 80	erlauben	Nutzung des Webservers auch vom internen Netz aus
Internes Netz (gegebenenfalls Einschränkung auf Administrationsnetz)	Webserver Port 22 (SSH)	erlauben	Administration und Datenübertragung erfolgen per SSH und SCP
Internes Netz	andere Ports des Webservers	verbieten	
Protokollierung			
Webserver	Loghost UDP-Port 514	erlauben	Übertragung der Protokolldaten zum Loghost

Verwendung eines Reverse Proxy

Wenn die Anfragen an den Webserver hoch sind, dann ist es ratsam zur Entlastung des Servers einen Reverse Proxy zu verwenden.

Der Proxy und der Server sollten sich im gleichen DMZ befinden und die Anfragen aus dem Internet dürfen nur über den Proxy erfolgen. Der direkte Zugriff aus dem Internet an den Webserver ist durch den Paketfilter zu unterbinden.

Verwendung eines Reverse Proxy mit zusätzlichem Paketfilter

Sind die Sicherheitsanforderungen an den Webserver höher, dann ist zusätzlich noch ein Paketfilter zwischen dem Webserver und dem Reverse Proxy zu verwenden.

- Überlastung des Webservers
- Einbruch ins Firmeninterne Netz

5.2.44 Sicherheitsstrategien für Einsatz eines Web - Servers

Wenn WWW – Dienste im Internet, als auch im Intranet angeboten werden, sind zwei getrennte Systeme dafür einzusetzen (Internet – Webserver und Intranet – Webserver). Bei Verbindung des Internet – Webservers mit dem internen Netz ist der Übergang mit einer Firewall zu schützen. Es ist darauf zu achten, wer welche Information bereitstellen darf und wer für die Aktualisierung und Korrektheit der Daten zuständig ist. Ebenfalls zu regeln ist, wer auf welche Information und Dateien auf dem Server zugreifen darf. Bei Bereitstellung von Daten ist darauf zu achten, dass die Datenschutzrichtlinien einzuhalten sind. Die Daten auf dem Web – Server sind laufend auf ihre Aktualität zu überprüfen. Am Web – Server sollte nur die Programme, die für den korrekten Betrieb des Servers notwendig, installiert sein. Zugriffe auf Dateien am Web – Server müssen geschützt sein. Weiters sollte der Zugriff aus dem Internet durch einen Paketfilter beschränkt werden. Die Administration des Web – Servers darf nur über eine sichere, verschlüsselte Verbindung erfolgen. Es soll unterbunden werden, dass Dateien oder Verzeichnisse mit symbolischen Links bzw. Verknüpfungen in den WWW – Dateienbaum eingeblendet werden. Sollte der DNS Dienst nicht benötigt werden, ist dieser zu deaktivieren.

- Zugriff auf interne Daten und Programme durch Dritte
- Virenbefall
- Download von nicht aktuellen bzw. nicht autorisierten Daten
- Manipulation und Fälschung von Daten

5.2.45 Notfallplan für den Webserver

Es sollte ein Notfallplan für den Ausfall des Webservers erstellt werden, dabei sind folgende Aspekte zu berücksichtigen: [4]

- Die Notfallplanung für den Webserver muss in den existierenden Notfallplan integriert werden.

- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für den Webserver zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte. Hierin sollte nicht nur der Webserver selbst, sondern auch das Gesamtsystem, innerhalb dessen der Webserver eingesetzt wird, berücksichtigt werden. Dazu gehören unter Umständen Datenbanken, Applikationsserver oder Proxy-Installationen zur Lastverteilung.
- Bestehen besondere Anforderungen an die Verfügbarkeit des Webservers, so sollten benötigte Komponenten redundant ausgelegt werden. Beispielsweise kann der Webserver selbst in manchen Anwendungen durch die Verwendung eines gemeinsamen, externen Speichersystems redundant ausgelegt werden.
- Zum Betrieb des Webservers im Internet ist eine funktionierende Internet-Anbindung Voraussetzung. Bei bestimmten Konfigurationen ist auch ein korrekt funktionierender DNS-Server nötig. Ein Ausfall dieser Komponenten muss daher ebenfalls in Betracht gezogen werden.
- Wird SSL auf dem Webserver eingesetzt, so muss beim Wiederanlauf des Systems auch der private Schlüssel des SSL-Zertifikates zugreifbar sein. Da dieser durch ein Passwort geschützt sein sollte, muss dieses sicher hinterlegt sein, damit es für den Wiederanlauf verfügbar ist.
- Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.

- Bei Ausfall des Webservers kann dieser nicht wieder in Betrieb genommen werden.
- Es kann zu Datenverlust kommen.
- Die Konfiguration des Webservers kann nicht wieder hergestellt werden.
- Die Verfügbarkeit des Webservers ist nicht gegeben.
- Das SSL-Zertifikat kann nicht erstellt werden.

5.2.46 Einsatz eines Datenbankserver

Wird ein Datenbankserver verwendet, dann sollte der Zugriff auf die Daten des Datenbankservers über ein Web-Frontend erfolgen.

Dabei sollte der Webserver und der Datenbankserver in unterschiedlichen DMZ stehen.

- Zugriff durch unbefugte auf sensible Firmendaten

5.2.47 Richtlinien zur Datenbankverwaltung

Bei Speicherung von Daten in einer verteilten Datenbank ist darauf zu achten, dass die Daten stets konsistent sind. Nicht benötigte Datenbank – Accounts sind zu löschen. Es ist ein regelmäßiger Sicherheitscheck (haben manche Benutzer zu leichtes bzw. gar kein Passwort, gibt es Benutzer mit zu viel Rechten, wer hat Zugriff auf den SQL – Editor, etc.) durchzuführen. Weiters ist die Datenbank regelmäßig auf Füllgrad und Auslastung zu überprüfen, sowie Datenbank zu defragmentieren. Bei Speicherung von sensiblen Daten ist eine Datenbankverschlüsselung zu empfehlen (Online-, Offlineverschlüsselung).

- Manipulation, Fälschung und Diebstahl von Daten
- Ausfall der Datenbank
- Überlastung der Daten
- Inkonsistenz der Datenbestände

5.2.48 Richtlininen zur Datenbanksicherung

Es ist eine Komplettsicherung (Offline) der Datenbank in regelmäßigen Abständen durchzuführen. Eine Sicherung im laufenden Betrieb (Online) sollte nur zusätzlich zur Offline-Sicherung erfolgen. Weiters sollte eine Dokumentation zur Wiederherstellung der Datenbank erstellt werden.

- Bei Ausfall der Datenbank kann sie nicht wiederhergestellt werden
- Es ist keine vollständige Wiederherstellung der Datenbank möglich

5.2.49 Richtlinien zur elektronischen Archivierung

Vor der Einführung eines elektronischen Archivierungssystems ist festzulegen, welche Daten (Buchhaltungsdaten, Kundendaten etc.) aus welchen Bereichen archiviert werden sollen, welches Sicherheitsniveau erreicht werden soll und wer die Verantwortung für die Archivierung dieser Daten trägt.

Die für die elektronische Archivierung maßgeblichen technischen Einflussfaktoren sind unter anderem [4]

- das zu erwartende Datenaufkommen,

- die Dateiformate der zu archivierenden Dokumente,
- das Änderungsvolumen und Versionierung,
- die Aufbewahrungsdauer der Dokumente,
- die Zahl und Art der Zugriffe,
- die vorhandene IT-Einsatzumgebung sowie
- zu beachtende Normen und Standards.

Weiters ist auf die Mindestaufbewahrungszeit aus steuerlichen Gründen und Höchstaufbewahrungszeit aus Datenschutzgründen zu achten. Es müssen auch die Zugriffsrechte für Externe, wie Finanzamt, berücksichtigt werden. Es sind regelmäßige Kontrollen durchzuführen, ob auf den Sicherungsmedien für die Archivierung genügend Speicher vorhanden sind. Weites sind die gesicherten Daten einer regelmäßigen Prüfung auf Vollständigkeit zu unterziehen. Da Hardware – Komponenten einen technischen Verschleiß unterliegen, sollten diese regelmäßig gewartet werden und bei Bedarf sind diese auszutauschen. Überhaupt ist das Archivierungssystem im Laufe der Zeit dem momentanen technologischen Standard anzupassen.

Das Archivsystem hat eine Versionierung, Erweiterbarkeit und eine Protokollierung zu unterstützen und die archivierten Daten sollten einem Zugriffsschutz unterliegen.

Bei der Wahl der Archivmedien sollte man sich an den aktuellen Stand der Technik orientieren. Auf jeden Fall sind bei Wahl des richtigen Mediums folgende Punkte wichtig:

1. Datenvolumen
2. Mittlere Zugriffszeit
3. Haltbarkeit
4. Anzahl der gleichzeitigen Zugriffe
5. Revisionssicherheit

Bei der Wahl des Datenformates zur Speicherung im Archiv, ist darauf zu achten, dass das Datenformat von langfristiger Relevanz ist (empfehlenswert z.B. pdf, xml).

Das Archivsystem ist regelmäßig mit aktuellen Daten zu versorgen, ebenfalls ist das Archivsystem zu sichern. In gewissen Abständen ist eine Kontrolle durchzuführen, ob die Daten des Archivsystems noch lesbar bzw. wiederverwendbar sind. Die Zugriffe auf das System sind mit zu protokollieren.

- Verlust von wichtigen Daten
- Keine strategische Planung möglich
- Rechtliche Konsequenzen
- Daten nicht mehr lesbar in paar Jahren
- Keine Wiederverwendbarkeit der Daten

5.2.50 Richtlinien zum Einsatz des Proxy – Servers

Für Clients mit hohem Schutzbedarf ist der aktive Inhalt von http - Seiten herauszufiltern. Weiters sind alle Cookies zu sperren und die Browsererkennung zu filtern. Je nach Bedarf sind URLs mit bedenklichen zu sperren. Die Dienste Telnet und FTP, wenn nicht unbedingt erforderlich, sind zu sperren. Empfehlenswert ist die Filterung der Dateien mit folgenden Endungen .bat, .vbx, .com, .hta, .inf, .js, .jse, .wsa, .vbs., .vbe.

- Virenbefall
- Hackangriffe

5.3 Sicherheitsmassnahmen für mobile IT - Systeme

5.3.1 Tragbare IT - Systeme in Einsatz (mobil/stationär)

Das tragbare IT - System (z.B. Laptop, PDA...) sollte man nie unbeaufsichtigt lassen, nie im Auto offen liegen lassen und in Hotels das IT - System verschließen. Bei Einsatz in fremden Büros ist es ratsam bei kurzzeitigem Verlassen das Gerät entweder mitzunehmen oder zu verschließen. Bei längerer Nichtbenützung des Gerätes ist dieses ausschalten oder eine Zugriffssperre zu aktivieren. Bei Transport ist das IT - System vor Umwelteinflüssen zu schützen und auch schon bei kürzeren Transportwegen dieses stoßgeschützt befördern. Bei Betrieb des tragbaren IT - Systems in den Büroräumlichkeiten ist es darauf zu achten, dass es außerhalb der Arbeitszeiten weggeschlossen wird. Werden im Betrieb mehrere tragbare IT - Systeme verwendet besteht die Option einer Sammelaufbewahrung in einem speziell gesicherten Raum. Bei der Benutzung des mobilen IT - Systems sollte man darauf achten, dass eine ausreichende Stromversorgung vorhanden ist und ob der Einsatz überhaupt erlaubt ist (z.B. Flugzeug). Weiters sollte man die Einsatzumgebung so wählen, dass keine Einsichtmöglichkeiten auf den Bildschirm bestehen und, dass die Umgebung den Einsatz nicht beeinträchtigt (z.B. schlechte Witterungsverhältnisse).

- Gelegenheitsdiebstahl im Hotel, wenn IT - System nicht weggesperrt
- Raub des Gerätes aus Auto
- Datendiebstahl bei Einsatz im betriebsfremden Büro
- Zerstörung des Gerätes durch Witterung

5.3.2 Energieversorgung von mobilen Geräten

Die Energiewarnanzeige des mobilen Gerätes darf nicht ignoriert werden, bei Anzeige des Warnsignals sollte das mobile Gerät entweder an eine Steckdose angesteckt werden, oder der Reserve-Akku sollte verwendet werden. Ist das nicht möglich, sind alle offenen Dateien zu speichern und die Programme zu schließen. Es ist ratsam immer einen aufgeladenen Reserve-Akku und das Ladenetzteil mitzuführen.

- Alle nichtgespeicherten Daten gehen verloren

5.3.3 Zweckmäßige Aufstellung von IT - Systemen am häuslichen Arbeitsplatz

Ein separater Arbeitsraum wäre empfehlenswert oder mindestens ein vom Wohnraum temporär, räumlich getrennter Arbeitsplatz.

Beim häuslichen Arbeitsplatz ist auf folgende Punkte zu achten: [4]

- ausreichend Platz für Möbel und Bildschirmarbeitsplatz,
- regelbare Raumtemperatur und ausreichende Lüftungsmöglichkeiten,
- Abschirmung gegenüber Lärmquellen,
- Tageslicht sowie ausreichend künstliche Beleuchtung,
- Sichtschutz des Monitors, falls er durch ein Fenster beobachtet werden könnte,
- Vermeidung von störenden Blendungen, Reflexen oder Spiegelungen am Arbeitsplatz und
- Anschlüsse für Telefon und Strom.

Das vom Betrieb zur Verfügung gestellte IT - System darf nur zu Betriebszwecken genutzt werden.

- Keine ausreichende Motivation bei Arbeit
- Keine ausreichender Gesundheitsschutz bei Arbeit
- Keine ausreichende Sicherheit
- Betriebsfremde Familienmitglieder benutzen das IT - Gerät für private Zwecke

5.3.4 Übergabe und Rücknahme von tragbaren IT - Systemen

Bei der Übergabe muss der Übernehmende darauf hingewiesen werden, dass er das Passwort sofort ändert. Weiters muss die Übergabe dokumentiert werden. Bei der Rücknahme ist das Gerät auf Vollständigkeit (Maus, Stromkabel, Akku etc.) und auf Viren zu überprüfen. Weiters hat der Benutzer die Daten, die er noch benötigt auf einen Datenträger zu überspielen und diese dann dauerhaft vom mobilen IT - System

zu löschen. Eventuell können die Festplatten des IT - Systems formatiert werden und die Grundkonfiguration kann durch eine Neu - Installation wieder hergestellt werden.

- Fremde haben Zugriff auf sensible Daten
- Virenverseuchung
- Verlust des IT - Systems

5.3.5 Einsatz von Laptops

Direkte Verbindung mit dem Internet

Wird der Laptop Unterwegs direkt mit dem Internet verbunden, ist eine Personal Firewall unbedingt erforderlich. Die Firewall sollte so konfiguriert werden, das alles was nicht erlaubt ist grundsätzlich verboten ist. Die Software auf dem Laptop sollte sich immer auf dem neuesten Stand befinden, Sicherheitsupdates sollten laufend eingespielt werden. Wenn es die Funktion automatisches Update gibt, sollte diese aktiviert werden. Der E-Mail-Client und der WWW-Browser auf dem mobilen Gerät, sollten sicher betrieben werden. (siehe 5.2.41, 5.2.24)

Weiters sollten auf dem Laptop zwei Profile eingerichtet werden. Ein Profil für das Firmennetzwerk und das zweite Profil für den direkten Internetzugriff , welches nur mit minimalen Benutzerrechten ausgestattet ist.

Der Benutzer darf keine Berechtigung besitzen, Änderungen der Sicherheitseinstellungen des Laptops vorzunehmen.

Anbindung an das interne Firmennetzwerk

Bevor Laptops die mobil verwendet werden an das interne Firmennetzwerk angebunden werden, ist ein vollständiger Virenscann mit einer aktualisierten Antivirensoftware auf dem Gerät durchzuführen.

Wenn der mobile Rechner lokal an das Firmennetzwerk angebunden wird, ist eine Zugriffssbeschränkung erforderlich. Bei Verwendung eines DHCP-Servers sind IP-Adressen nur an zugelassene MAC-Adressen zu vergeben.

Bei einem Remotezugang zum Firmennetz ist der Punkt „Mobiler Zugriff auf das interne LAN“ (5.3.8) zu beachten.

- Gefährdung des Internen Netzes durch Viren, Würmer und Trojaner
- Gefahr, dass unbefugte an interne sensible Daten gelangen

5.3.6 Datensicherung von Laptops

Datensicherungen von Laptops sollten entweder auf externen Datenträgern oder, wenn möglich, über das Firmennetzwerk durchgeführt werden. Bei der Sicherung ist darauf zu achten, dass alle relevanten Daten gesichert werden und, dass die Sicherung größtmöglich automatisiert erfolgt.

- Gelöschte Daten können nicht wieder hergestellt werden
- Bei Ausfall der Festplatte sind die gespeicherten Daten verloren

5.3.7 Laptop Benutzerwechsel

Wenn der Benutzer eines Laptops wechselt, dann sind alle sensiblen Daten des Vorbesitzers zu löschen. Weiters ist der Laptop einer vollständigen Virenprüfung zu unterziehen.

- Virenbefall
- Zugriff auf sensible Daten durch unbefugte Dritte

5.3.8 Mobiler Zugriff auf das interne LAN

Wenn von einem mobilen Gerät wie einem Laptop oder einem PDA auf das interne Netzwerk zugegriffen wird, sind folgende Sicherheitsanforderungen zu beachten [4]:

- *Sicherstellung der Vertraulichkeit der übertragenen Daten*: es muss durch eine ausreichend sichere Verschlüsselung der Datenübertragung erreicht werden, dass auch durch Abhören der Kommunikation kein Rückschluss auf den Inhalt der Daten möglich ist. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- *Sicherstellung der Integrität der übertragenen Daten*: Die eingesetzten Übertragungsprotokolle müssen die Möglichkeit bieten, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.
- *Sicherstellung der Authentizität der Daten*: bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, so dass eine Maskerade oder ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck muss eine gegenseitige Authentisierung der

Kommunikationspartner (beispielsweise über digitale Zertifikate) erfolgen.

- *Sicherstellung der Nachvollziehbarkeit der Datenübertragung*: um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann an wen übertragen wurden.

- Einsicht in interne Daten durch unbefugte Dritte
- Übertragene Daten werden verfälscht
- Welche Daten wann übertragen wurden, ist nicht mehr nachvollziehbar

5.3.9 Richtlinien zum Einsatz in einem fremden Netz

Man sollte sich genau überlegen welche Daten man über das Netz überträgt und welche Aktionen man über das Fremde Netz tätigt (z.B. Internetbanking nicht empfehlenswert). Überhaupt sollte man versuchen keine sensiblen Daten über dieses Netz zu verschicken. Nach Beendigung der Sitzung sind alle temporären Dateien von der eigenen Festplatte zu löschen. Beim Browser ist die Funktion „Auto-Vervollständigung“ abzuschalten.

- Datendiebstahl
- Einschleusung von Viren

5.3.10 Umsetzung von Sicherheitsrichtlinien bei Mobiltelefonen

Bei Benutzung von Mobiltelefonen sollten folgende Punkte beachtet werden:

- *Gefahr des Missbrauchs der SIM – Karte*
  Das Mobiltelefon mit SIM – Karte sollte nie unbeaufsichtigt gelassen werden. Der PIN – Code der SIM – Karte darf nicht weitergegeben werden. Bei firmeninterner Weitergabe der SIM – Karte ist der PIN – Code zu ändern. Weitere Informationen zum PIN – Code siehe Kapitel 5.1.51.

- *Einzelverbindungsnachweis*
  Vom Mobilfunk – Provider ist für jede SIM – Karte ein Einzelverbindungsnachweis anzufordern.

- Sicheres Telefonieren
  Telefongespräche sollten nicht in der Öffentlichkeit geführt werden und vertrauliche Gespräche, wenn möglich, sollten nicht über eine Telefonverbindung stattfinden.

- Nutzungsverbot von Mobiltelefonen
  In Räumen mit viel IT – Infrastruktur (z.B. Serverräumen) ist die Nutzung von Mobiltelefonen zu verbieten.

- Verbot von Mobiltelefonen mit Kamerafunktion
  In Bereichen mit Zugang zu sensiblen Daten bzw. Infrastruktur sollte die Nutzung von Mobiltelefonen mit Kamerafunktion verboten werden.
- Energieversorgung
  Die Warnanzeigen, die den Spannungsabfall anzeigen sollten nicht ignoriert werden. Sollte ein langfristiger Einsatz geplant werden, ist ein Reserve - Akku oder das Ladegerät mitzunehmen.

Bei Verlust des Mobiltelefons bzw. SIM – Karte ist der Mobilfunk – Anbieter zu informieren und die SIM – Karte sofort zu sperren.

- Benutzung des Mobiltelefons durch Dritte
- Abhören von geheimen Informationen
- Störung der bestehenden IT – Infrastruktur
- Fotografieren von geheimen Daten

5.3.11 Sicherung und Ausfallvorsorge von Mobiltelefonen

Alle wichtigen Daten (Kontakte, Nachrichten, usw.) die auf dem Mobiltelefon gespeichert sind müssen regelmäßig gesichert werden. Es sollte auch eine Liste der Handy-Reparaturfachbetriebe erstellt werden. Wenn man ständig erreichbar sein muss, sollte ein Ersatzhandy oder zumindest ein Ersatzakku mitgeführt werden.

Weiters sollten alle wichtigen Konfigurationen des Handys dokumentiert werden.

- Bei Ausfall des Handys gehen wichtige Daten verloren.
- Die ständige Erreichbarkeit ist nicht mehr gegeben.
- Die Konfiguration des Handys ist nur schwer wiederherstellbar.

5.3.12 Richtlinien für Einsatz von PDAs

Es sollte eine zentrale Verwaltung für die PDAs eingerichtet werden. Bei Nutzung im Betrieb, sollte die Übertragung über das Mobilfunknetz ausgeschaltet werden. Es sollte vermieden werden sensible Daten dauerhaft auf dem PDA zu speichern. Die private Nutzung des PDA sollte, soweit wie möglich, eingeschränkt werden. Zum Diebstahlschutz sollten PDAs nie unbeaufsichtigt gelassen werden und sind mit sicheren PIN – Code bzw. Passwort abzusichern. (siehe Kapitel 5.1.51).

Auch bei PDAs ist eine regelmäßige Datensicherung durchzuführen und eine Synchronisierung mit dem PC ist empfehlenswert. Überhaupt ist es notwendig den PDA auch an das Sicherheitslevel des Unternehmens anzupassen. In hoch schutzbedürftige Bereiche des Unternehmens ist das Mitnehmen von PDAs zu verbieten. Für PDAs gelten die gleichen Installationsrichtlinien und Virenschutzrichtlinien, wie für PCs (siehe Kapitel 5.1.60). An sich ist für PDAs, wie für Mobiltelefone, empfehlenswert erweiterte

Sicherheitsfunktionen, wie Verschlüsselung der Speicherkarteninhalte oder eine verbesserte Authentisierungs - Methode (z.B. Fingerprint – Scanner), zu benutzen.

- Unverschlüsselte Übertragung über das Mobilfunknetz
- Datendiebstahl
- Diebstahl des PDAs
- Verlust von Daten
- Dateninkonsistenz
- Fotografieren von geheimer IT – Infrastruktur
- Mitschneiden von Gesprächen

5.4 Erhöhte Sicherheitsmaßnahmen

5.4.1 Einbruchhemmende Türen und Fenster

Einbau von Sicherheitstüren ist empfehlenswert, ebenso der Einbau von einbruchhemmenden Fenstern im Fassadenbereich des Gebäudes.

- Leichter Einbruch in das Gebäude

5.4.2 Alarmanlage

Eine Installation einer Alarmanlage, die aus einer Vielzahl von lokalen Meldern besteht ist empfehlenswert. Die lokalen Melder können bei Gefahren, wie Einbruch, Wasser, Gas oder Brand Alarm schlagen. Als Einbruchschutz können z.B. Bewegungsmelder, Videokameras oder Glasbruchsensoren dienen. Entscheidend für das Funktionieren des Alarmsystems ist die Weiterleitung des Alarmzustandes an eine ständig besetzte Stelle, wie Wachdienst oder Feuerwehr. Bei kleineren Unternehmen sind selbstständig agierende Gefahrenmelder in Betracht zu ziehen. Es ist zu überlegen, welche Räume am schützendwertesten sind (wie Serverraum, Archiv, Chefbüro, etc.) und Melder besonders auf diese Räume zu konzentrieren. Des Weiteren besteht die Möglichkeit einer Fernanzeige von Störungen. In jedem Fall ist es wichtig die Anlage regelmäßig zu warten, damit diese im Ernstfall einwandfrei funktioniert.

- Keine rechtzeitige Reaktion auf Alarmzustand
- Keine Reaktion auf Einbruch oder Brand
- Keine Weiterleitung des Alarmzustandes an übergeordnete Stelle

5.4.3 Videoüberwachung

Die Installation eines Video - Überwachungssystems ist empfehlenswert, dabei ist die Videoüberwachung in das Gesamtkonzept des Einbruchschutzes (siehe 5.4.2) mit einzubeziehen Es ist auch auf regelmäßige Wartung zu achten.

- Einbruch
- Videoüberwachung werkt autonom, ohne Zusammenarbeit mit Alarmsystem, daher bei entdeckten Einbruch durch Videoüberwachung erfolgt kein Alarmzustand
- Eingeschränkte bzw. keine Funktionalität wegen fehlender Wartung

5.4.4 Kontrollgänge

Es sollten regelmäßig Kontrollgänge durchgeführt. Diese dienen, dazu eventuelle Nachlässigkeiten zu entdecken und zur Kontrolle der Umsetzung von Sicherheitsmaßnahmen. Die Mitarbeiter sollten bei den Kontrollgängen nicht bevormundet werden!

- Keine Entdeckung von Nachlässigkeiten
- Keine Kontrolle der Umsetzung von Sicherheitsvorschriften
- Keine Entdeckung von gewaltsamer Öffnung an Verteilern

5.4.5 Kontrolle an bestehenden Verbindungen

Ein Teil der Kontrollgänge sollte auch sein, dass man eine stichprobenartige Sichtprüfung an den bestehenden Verbindungen vornimmt (vor allem Verteiler).

In größeren, regelmäßigen Abständen sollten an Leitungen, die häufig schützenswerte Informationen transportieren, eine Funktionskontrolle durchgeführt werden.

- Keine rechtzeitige Erkennung von Datendiebstahl
- Fremde Unternehmen zapfen ständig Verbindungen an
- Unzulässige Einbauten. bzw. Veränderungen
- Versorgungspläne der Leitungen nicht am aktuellsten Stand (siehe Kapitel 5.1.7)

5.4.6 Sicherheitscheck des Netzes

Das Netzwerk sollte in regelmäßigen Abständen kontrolliert und die Auswertung dokumentiert werden.

Bei dieser Kontrolle sollten folgende Punkte überprüft werden([4]):

- Gibt es Benutzer ohne Passwort?
- Gibt es Benutzer, die längere Zeit das Netz nicht mehr benutzt haben?
- Gibt es Benutzer, deren Passwort nicht die erforderlichen Bedingungen einhält?

- Welche Benutzer besitzen die gleichen Rechte wie der Administrator?
- Sind Systemprogramme und Systemkonfiguration unverändert und konsistent?
- Entsprechen die Berechtigungen von
  - Systemprogrammen und Systemkonfiguration
  - Anwendungsprogrammen und -daten
  - Benutzerverzeichnissen und -daten
- den Vorgaben der Sicherheitsrichtlinie?
- Welche Netzdienste laufen auf den einzelnen Systemen? Sind sie den Vorgaben der Sicherheitsrichtlinie entsprechend konfiguriert?

- Inkonsistenz des Netzwerks
- Angriffe auf das Netzwerk

5.4.7 Richtlinien für Sicherheitsgateway - Protokollierung

Für den Einsatz der Protokollierung am Sicherheitsgateway sollten die folgenden Punkte beachtet werden: [4]

- Es muss möglich sein, die Protokolldaten (beispielsweise IP-Adressen) eindeutig einzelnen Rechnern (oder Personen) zuzuordnen. Dabei müssen jedoch die jeweils zutreffenden gesetzlichen Regelungen zum Datenschutz beachtet werden.
- Die Protokolldaten sollten nicht nur auf den einzelnen Komponenten des Sicherheitsgateways, sondern zusätzlich auch auf einem zentralen Protokollierungsserver (Loghost) gespeichert werden, so dass die Gefahr des Datenverlustes durch einen Hacker-Angriff oder durch einen Systemausfall verringert wird.
- Die Übertragung der Protokollinformationen von den Komponenten zum Loghost muss über eine gesicherte Verbindung erfolgen, damit die Protokollinformationen vor ihrer endgültigen Speicherung nicht verändert werden können.
- Wenn bei der Übertragung zum Loghost nicht-vertrauenswürdige Netze passiert werden müssen, so müssen die Daten verschlüsselt werden.
- Die Größe des freien Speicherplatzes auf dem verwendeten Medium sollte regelmäßig kontrolliert werden.
- Bei einem Ausfall der Protokollierung (z. B. aufgrund fehlenden Speicherplatzes auf der Festplatte) sollten alle Funktionen, die Proto-

kolldaten generieren, gesperrt werden. Idealerweise sollte das Sicherheitsgateway jeglichen Verkehr blockieren und eine entsprechende Meldung an den Administrator weitergeben.

- Die Protokolldaten sollten auf einem WORM-Medium („Write Once, Read Many“) gespeichert werden.
- Art und Umfang der Protokollierung sollten sich an der Sensibilität der zu verarbeitenden Daten sowie am Verwendungszweck orientieren.
- Spezielle, einstellbare Ereignisse, wie z. B. wiederholte fehlerhafte Passworteingaben für eine Benutzer-Kennung oder unzulässige Verbindungsversuche, müssen bei der Protokollierung hervorgehoben werden und sollten zu einer unverzüglichen Warnung des Firewall-Administrators führen.
- Die einzelnen Komponenten sollten eine Zeitsynchronisation durchführen, um eine Korrelation der Daten zu ermöglichen.

Die mit protokollierten Daten sind mit speziellen Tools auszuwerten.

5.4.8 Richtlinien für den Netzzugang in Besprechungsräumen

Wenn es nicht unbedingt erforderlich ist, sollte in Besprechungs- und Schulungsräumen kein Zugang zum internen Netzwerk (Intranet) vorhanden sein.

Falls es unumgänglich ist, sollten folgende Punkte berücksichtigt werden:

- Nur eigene sichere Geräte dürfen an das Netzwerk angebunden werden (MAC-Adressprüfung).
- Schulungs- und Besprechungsräume sind durch einen restriktiv konfigurierten Paketfilter vom LAN zu trennen.
- Entweder wird kein DHCP für die Zugänge in den Schulungs- und Besprechungsräume verwendet, oder die IP-Adresse wird nur an bestimmte MAC-Adressen vergeben(statisches DHCP).
- Der Datenverkehr von Mitarbeitern in den Schulungs- und Besprechungsräumen darf von Dritten nicht mitgelesen werden (z.B: Verschlüsselung).
- Zugriff durch unbefugte auf sensible Firmendaten
- Gefährdung des Internen Netzes durch Viren, Würmer und Trojaner

5.4.9 Richtlinien für Schulungs- und Konferenzräume

Die Lage des Schulungsraumes sollte so gewählt, dass Fremde nicht unnötig sicherheitsrelevante Bereiche durchqueren müssen. Es darf im Schulungsraum keine Möglichkeit geben über W-Lan oder Ethernet in das firmeninterne Netz zu gelangen. Empfehlenswert ist ein eigener Zugang zum Internet. Es ist zu regeln unter welchen Bedingungen Schulungsteilnehmer mobile IT – Systeme mitnehmen und verwenden dürfen. IT – Komponenten im Schulungsraum sollten gegen Diebstahl abgesichert werden.

- Diebstahl von IT – Komponenten
- Fälschung, Manipulation und Diebstahl von Daten
- Zugang zu sensiblen Bereichen durch unbefugte Dritte

5.4.10 Einsatz kryptographischer Verfahren

Vor dem Einsatz kryptographischer Verfahren ist zu klären, mit welchen Angriffen zu rechnen ist, welches Sicherheitsniveau gilt es zu erreichen und welche kryptografischen Funktionen sind dafür notwendig.

Es müssen des Weiteren folgende personelle und organisatorische Aspekte in Betracht gezogen werden:

- Benutzerfreundlichkeit: Benötigen die Benutzer für die Bedienung kryptographische Grundkenntnisse? Behindert der Einsatz eines Kryptoprodukts die Arbeit?
- Zumutbarkeit: Wie viel Belastung durch zusätzliche Arbeit ist dem Anwender zumutbar (Arbeitszeit, Wartezeit)?
- Zuverlässigkeit: Wie zuverlässig werden die Benutzer mit der Kryptotechnik umgehen?
- Schulungsbedarf: Inwieweit müssen die Benutzer geschult werden?
- Personalbedarf: Ist zusätzliches Personal erforderlich, z. B. für Installation, Betrieb, Schlüsselmanagement?
- Verfügbarkeit: Kann durch den Einsatz eines Kryptoprodukts die Verfügbarkeit reduziert werden?

Auf jeden Fall ist regelmäßig zu prüfen, ob das eingesetzte kryptographische Verfahren am momentanen Stand der Technik ist.

- Überteuerter Einsatz von Kryptographie
- Unnötiger Einsatz von Kryptographie
- Eingesetzte Verfahren veraltet

5.4.11 Verschlüsselungsprogramme für mobile IT-Systeme

Tragbare IT-Systeme (Laptop, PDA) sollten mit einem Verschlüsselungsprogramm ausgestattet sein. Je nach Bedarf sind einzelne sensible Dateien, Teile der Festplatte oder die komplette Festplatte zu verschlüsseln. Das Verschlüsselungsprogramm ist so zu konfigurieren, dass die verschlüsselnden Dateien nicht ohne ein entsprechendes Passwort im Klartext angezeigt werden. Die Wahl des richtigen Passwortes wird in dem Kapitel 5.1.51 beschrieben.

- Zugriff auf sensible Daten durch unbefugte Dritte
- Manipulation sensibler Daten durch unbefugte Dritte

5.4.12 Verwendung der Standardsicherheitsfunktionen in Anwendungsprogrammen

Wenn möglich, sollten die in vielen Anwendungsprogrammen angebotenen Sicherheitsfunktionen wie zum Beispiel: Automatische Speicherung von Zwischenergebnissen, Deaktivierung der Anzeige von Makros und Verschlüsselung von Dateien verwendet werden.

- Bei Absturz des Systems gehen die zuletzt und nicht gespeicherten Daten verloren
- Virenbefall
- Zugriff auf sensible Daten durch unbefugte Dritte

5.4.13 Abschalten des Rechnermikrofons

Bei vertraulichen Konferenzen bzw. Gesprächen sind Rechner mit integrierten Mikrofon, die geeignet zur Aufnahme sind, aus dem Raum zu entfernen.

- Mitschneiden von vertraulichen Gesprächen

5.4.14 Einsatz der BIOS – Sicherheitsmaßnahmen

Es ist empfehlenswert im BIOS den Passwortschutz zu aktivieren. Die Boot – Reihenfolge sollte man so einstellen, dass immer zuerst von der Festplatte gebootet wird. Weiters ist das Booten von externen Medien zu unterbinden.

- Zugriff auf den Rechner durch unbefugte Dritte
- Virenbefall

5.4.15 Regelmäßige Integritätsprüfung

Das Dateisystem ist regelmäßig auf unerwartete Veränderungen zu überprüfen. Weiters sollte ein Tool verwendet werden um wichtige Elemente der Systemkonfiguration (z.B. Registry) auf Integrität zu überprüfen.

- Angriffe auf System
- Systemausfall
- Virenbefall

5.4.16 Schutz gegen nachträgliche Veränderungen von Informationen

Falls ein Dokument, dass weitergegeben werden soll, nicht verändert werden soll, sind folgende Verfahren empfehlenswert

- Schutz durch digitale Signatur zur Erkennung von unbemerkten Änderung.
- Verwendung von Dateiformaten, die eine spätere Änderung unterbinden (z.B. pdf, ps,..).
- Änderung des Dokumentes und daraus folgender Missbrauch
- Nachträgliche Änderung von Daten

5.4.17 Restriktive Vergabe von Zugriffsrechten auf Systemdateien

Auf Systemdateien und Systemverzeichnissen dürfen nur Administratoren Zugriff haben. Weiters sind Anwendungsdaten getrennt von Systemdateien zu speichern (z.B. Keine Anwendungsdaten in Systemordner speichern). Der Zugriff auf Systemdateien sollte mit protokolliert werden.

- Instabilität des Systems bis Systemabsturz
- Unabsichtliches Löschen von Systemdateien

5.4.18 Richtlinien zur Nutzung von USB – Speichermedien

Falls möglich ist ein mechanisches USB – Schloss zu verwenden. Ansonsten ist mit Hilfstools zu arbeiten, die das Hinzufügen von USB – Speichermedien unterbinden bzw. eine Nachricht an den Admin schicken. Zum Beispiel ist es unter Windows XP ab Service Pack 2 möglich das Schreiben auf USB – Speichermedien durch einen Eintrag in Registry zu verhindern. [18]

- Unbefugtes Kopieren von Daten
- Virenbefall

5.5 Maßnahmen zur Erhöhung der Verfügbarkeit

5.5.1 Redundante Leitungen

Leitungen die für den IT-Betrieb von Wichtigkeit sind, sollten doppelt verlegt werden.

Die Backupleitungen sind in regelmäßigen Abständen auf Funktion zu überprüfen und sind über eine andere Trasse zu verlegen.

- Bei Ausfall von Leitungen gibt es keinen Ersatz und der IT-Betrieb steht still

5.5.2 Verwendung redundanter Netzkomponenten

Netzkomponenten die für die Aufrechterhaltung des lokalen Netzes notwendig sind (Switch, Router) sollten in zweifacher Ausführung existieren um sie entweder doppelt ins Netzwerk einzubinden, oder bei Ausfall sofort austauschen zu können.

- Teil oder Komplettausfall des lokalen Netzes.
- Verzögerung der Wiederaufnahme des lokalen Netzes.

5.5.3 Erhöhung der Verfügbarkeit bei Servern

Zur Erhöhung der Verfügbarkeit sind folgende Maßnahmen empfehlenswert.

- Cold – Standby
  Neben dem aktiven Server wird ein baugleiches, nicht aktives Ersatzsystem bereitgehalten. Dieses Ersatzsystem muss bei Ausfall des aktiven Systems manuell hochgefahren werden.
- Hot – Standby
  Neben dem aktiven Server ist ein baugleiches System parallel im Einsatz. Bei Ausfall des aktiven Servers wird automatisch bzw. manuell auf das zweite System gewechselt.
- Cluster (Zusammenschluss von 2 oder mehreren Servern, die parallel betrieben werden).
  - Load – Balanced Cluster
    Die Auslastung wird auf mehrere Server verteilt, die im Verbund agieren.
  - Failover Cluster
    Bei Ausfall eines, des im Verbund befindlichen, Servers übernimmt automatisch ein anderer Server dessen Dienste.
- Dienstunterbrechung des Servers
- Verringerung der Verfügbarkeit

5.5.4 Extern bezogene Personal – Resourcen

Um im Notfall die Verfügbarkeit aufrecht zu halten, sind externe Personen (z.B.: Zeitarbeitsfirma) einzuschulen. Diese Mitarbeiter sollen Gelegenheit erhalten das IT-Umfeld im Normalbetrieb kennenzulernen.

- Teilweiser bzw. kompletter Stilstand des Betriebes

5.5.5 Extern bezogene Hardware – Resourcen

Es sind externe Hardware – Kapazitäten (z.B. in einem externen Rechenzentrum) anzumieten. Auf diese Kapazitäten kann man im Notfall zurückgreifen. Im Normalbetrieb sind regelmäßige Testlaufe vorzunehmen, ob mit den externen Hardware – Resourcen der Betrieb aufrecht erhalten werden kann.

- Teilweiser bzw. kompletter Stilstand des Betriebes

Generell sollte für alle IT – Bereiche gelten „Was nicht ausdrücklich erlaubt ist, ist verboten!“

Abschlussbemerkung:
Die Arbeit wurde in Zusammenarbeit mit Nebojsa Babic verfasst. Die Arbeitsaufteilung der Kapitel erfolgte unter folgenden Gesichtspunkten:

1. Einleitung, Aufgabenstellung, Fragenkatalog und Grundlagen wurden gemeinsam abgefasst.
2. Gernot Deischler : 5.1.1 – 5.1.21 und 5.1.62 – 5.1.81
   Nebojsa Babic : 5.1.22 – 5.1.61
3. Nebojsa Babic : 5.2.1 – 5.2.25
   Gernot Deischler : 5.2.26 – 5.2.50
4. Gernot Deischler : 5.3.1 – 5.3.6
   Nebojsa Babic : 5.3.7 – 5.3.12
5. Nebojsa Babic : 5.4.1 – 5.4.9
   Gernot Deischler : 5.4.10 – 5.4.18
6. Kapitel 5.5 und Glossar wurden gemeinsam verfasst.

6 Glossar

Access Points

Dienen als Schnittstelle zwischen einem Funknetz und einem kabelgebundenen Rechnernetz. Zu Access Points stellen mobile Endgeräte eine Funkverbindung her.

ActiveX, Java, JavaScript

ActiveX, Java und JavaScript stellen aktive Inhalte dar, die bei Einsatz in Webbrowsern keine eigenen Sicherheitsfunktionen besitzen.

Administrator

Ein Administrator ist für die Konfiguration und für den korrekten Betrieb von Systemen, wie Netzwerke, Webseiten, Betriebssysteme, verantwortlich.

Authentizität

Gibt Auskunft darüber, ob die Glaubwürdigkeit und Echtheit einer Person oder

eines Dienstes nachweisbar ist.

Backup

Ist eine Sicherung von Daten auf Speichermedien.

BIOS

Das „Basic Input Output System“ wird nach jedem PC – Start aufgerufen und leitet den Aufruf des Betriebssystems ein.

Client

Der Client ist ein Programm, das Dienste des Servers anfordert.

Cluster

Der Cluster ist ein Zusammenschluss von zwei oder mehreren Servern, die parallel betrieben werden.

Cookies

Der Cookie ist ein Eintrag im Dateiverzeichnis, der zum Austausch von Informationen über das Internet dient.

DFÜ – Versorgung

DFÜ ist die Abkürzung für die Datenfernübertragung, darunter versteht man die Übermittlung von Daten zwischen zwei oder mehreren Computern. Für die Übertragung wird ein Medium, wie zum Beispiel die Telefonleitung, benutzt. [5]

DMZ

Die „Demilitarized Zone“ bezeichnet eine Pufferzone zwischen eigenem Netzwerk und dem Internet. [6]

DNS – Server

Der Domain-Name-Server wandelt den Domainnamen des angeforderten Webservers in eine IP-Adresse um, über die auf den jeweiligen Webserver zugegriffen wird.

Firewall

Eine Firewall trennt die Teile eines verteilten Systems von der Außenwelt. Alle ausgehenden, aber insbesondere alle ankommenden Pakete werden genauer inspiziert, bevor diese weitergegeben werden. Nicht erlaubter Verkehr wird verworfen. [16]

FTP

FTP stellt sowohl ein Protokoll als auch ein Programm für die Übertragung von Dateien zwischen Server und Client dar.

Gateway

Gateways sind Rechner, die die Verbindung bzw. den Datentransfer zwischen unterschiedlichen Netzen ermöglichen. [16]

HTTPS (HyperText Transfer Protocol Secure)

HTTPS ist ein Protokoll, das auf HTTP aufbaut und bei dem die Informationen verschlüsselt übertragen werden. Als Verschlüsselungsmethode wird SSL verwendet. [7]

Integrität

Gibt Auskunft darüber, ob Daten unbemerkt verändert wurden bzw. ob

alle Änderungen nachvollziehbar sind.

IP – Adresse

Eine IP – Adresse dient zur eindeutigen Adressierung von Rechnern in einem IP – Netzwerk.

ISP (Internet Service Provider)

Der Provider bietet technische Dienstleistungen an, die zum Betrieb des Internet notwendig sind.

KMU

KMU ist eine Abkürzung für Klein- und Mittelbetriebe.

Kryptographie

Die Kryptographie dient zur Verschlüsselung von Inhalten.

LAN

Steht für Local Area Networks. Die Ausbreitung eines LAN's beschränkt sich meist auf ein Gebäude. [11]

MAC – Adresse

Die MAC (Media Access Control) Adresse dient zur eindeutigen Identifizierung von Netzwerkadaptern im Netz.

Mail – Server

Der Mail – Server ist ein Server, der für den Empfang, die Weiterleitung, das Versenden und das Speichern von Mails verantwortlich ist.

Man in the Middle – Angriff

Bei einer Kommunikation von zwei Partnern, wird von einem unbekannten Dritten eine

falsche Identität vorgetäuscht, nämlich die Identität des jeweiligen Anderen.

Mithilfe dieses Angriffs kann man zum Beispiel eine gesicherte Online-Banking Verbindung belauschen. [9]

NAT (Network Address Translation)

Hier werden von einem Internet-Router die lokalen IP – Adressen in den ausgehenden Datenpaketen, durch die IP-Adresse des Routers ersetzt. [13]

Outsourcing

Beim Outsourcing wird ein Teil der Unternehmensaufgaben an Drittunternehmen übergeben. Zum Beispiel können die Aufgaben der EDV-Abteilung an ein externes Rechenzentrum übergeben werden.

PDA (Personal Digital Assistent)

Unter einem PDA versteht man einen kleinen tragbaren Computer mit dem man unter anderem seine Adress,- Kalender- und Aufgabenverwaltung erledigen kann.

POP3 (Post Office Protocol Version 3)

POP3 ist ein Übertragungsprotokoll mit dem E-Mail-Clients E-Mails von Mail-Servern abholen können.

Proxyserver

Ein Proxyserver ist ein Server, der häufig angeforderte Daten von Clients zwischenspeichert, um sie schneller liefern zu können und um das Datenvolumen des Datenverkehrs ins Internet einzuschränken. [14]

Remote – Administration

Unter Remote – Administration versteht man, wenn ein IT-System nicht lokal, sondern aus der Ferne, zum Beispiel über SSH, administriert wird

Reverse Proxy

Der Reverse Proxy wird vor einer Gruppe von Webservern geschaltet, um die Zugriffe auf diese zu verteilen und um unberechtigte Zugriffe zu verhindern. [14]

Router

Router sind IT-Komponenten, mit denen man mehrere Rechnernetzte miteinander verbinden kann.

Server

Ein Server ist ein Rechner, der einen oder mehrere Dienste zur Verfügung stellt und die von Client-Rechnern angefordert werden können.

SMTP (Simple Mail Transfer Protocol)

SMTP ist ein Übertragungsprotokoll mit dem E-Mails in Computernetze versendet werden können.

Spam

Unter Spammails versteht man unerwünschte Werbemails, die als Massen - Aussendung an mehrere Empfänger versendet werden.

Spyware

Als Spyware wird eine Software bezeichnet, die ohne ihr Wissen und ohne ihr Einverständnis Aktionen, wie zum Beispiel Anzeigen von Werbung, auf ihrem Computer ausführt. [15]

SQL (Structured Query Language)

SQL ist eine Datenbanksprache und dient zur Abfrage und Manipulation von Daten in relationalen Datenbanken.

SSH (Secure Shell)

SSH ist ein Protokoll, dass eine gesicherte Kommunikation über unsichere Netze ermöglicht. [17]

SSID (Service Set Identifier)

Der Service Set Identifier ist die eindeutige Bezeichnung eines Wireless Lokal Area Networks (WLAN).

SSL (Secure Socket Layer)

SSL ist ein Protokoll, das die sichere Übertragung von Daten gewährleistet und die Identität von Internetseiten sicherstellt.

Telnet (Telecommunication Network)

Telnet ist ein im Internet verbreitetes Netzwerkprotokoll, mit diesem man über die Konsole auf entfernte Rechner zugreifen kann. Dieses ist heutzutage aufgrund der fehlenden Verschlüsselung nicht mehr sonderlich relevant.

Twisted – Pair Kabel

Twisted – Pair Kabel kommen vorzugsweise in Netzwerken und der Telefonie zum Einsatz. Man unterscheidet zwischen ungeschirmten und geschirmten Kabeln.

VPN (Virtual Private Networks)

Mittels VPN soll gewährleistet werden, das sensible Daten vertrauenswürdig über verschiedene Netzt übertragen werden.

Webserver

Ein Webserver ist ein Server, über den der Internetauftritt des jeweiligen Unternehmens bewerkstelligt wird. Er überträgt Dokumente an die Webbrowser der Clients.

WLAN (Wireless Lokal Area Network)

Unter WLAN versteht man ein drahtloses Netz in dem mehrere Endgeräte per Funk miteinander verbunden sind.

WPA, WPA2 (Wi-Fi Protected Access/ Wi-Fi Protected Access2)

WPA bzw. WPA2 sind Verschlüsselungsmethoden für ein WLAN.

Literatur

[1] AGENTUR, AUSTRIAN PRESSE: *Aufholbedarf für IT-Sicherheit in Österreich*. http://www.wirtschaftsblatt.at/home/boerse/bwien/321133/index.do.

[2] BUNDESKANZLERAMT, BEREICH IKT-STRATEGIE DES BUNDES: *Österreichisches IT - Sicherheitshandbuch*. http://www.cio.gv.at/securenetworks/sihb/.

[3] INFORMATIONSTECHNIK, BUNDESAMT FÜR SICHERHEIT IN DER: *Grundschutzhandbuch*. http://www.bsi.bund.de/gshb/index.htm.

[4] INFORMATIONSTECHNIK BUNDESAMT FUER SICHERHEIT IN DER: *IT - Grundschutzhandbuch*. http://www.bsi.bund.de/gshb/deutsch/m/m01.htm.

[5] JANSSEN, WILHELM: *Netzwerk-Fachbegriffe, DFÜ*. http://www.at-mix.de/dfue.htm.

[6] JANSSEN, WILHELM: *Netzwerk-Fachbegriffe, DMZ*. http://www.at-mix.de/dmz.htm.

[7] KIRK, ALEXANDER: *Computer Lexikon, HTTPS*. http://www.computerlexikon.com/definition-https.

[8] MÜLLER, KLAUS-RAINER: *It - Sicherheit mit System*. Verlag Vieweg, 2008.

[9] ONLINE HEISE: *Man-in-the-Middle-Angriff (MITM)*. http://www.heise.de/glossar/entry/e4477cb0a876144c.

[10] PILLER, DR. DI. ERNST: *Security, Folien für die universitätere Vorlesung an der TU WIen*.

[11] SCHILDT, HELGE: *Einführung in die Technische Informatik*. Springer, 2005.

[12] SCHMIDTMANN, ACHIM: *IT - Sicherheit*. http://www.sicherheitsthemen.de/it-sicherheit.php.

[13] SCHNABEL, PATRICK: *Elektronik - Kompendium, NAT*. http://www.elektronik-kompendium.de/sites/net/0812111.htm.

[14] SCHNABEL, PATRICK: *Elektronik - Kompendium, Proxy*. http://www.elektronik-kompendium.de/sites/net/1101221.htm.

[15] SCHUBERT, MICHAEL: *Spyware*. http://www.masterscripts.de/lexikon/s/spyware.html.

[16] TANNENBAUM, ANDREW: *Verteilte Systeme, Grundlagen und Paradigmen*. Pearson Studium, 2007.

[17] TRAPP, HOLGER: *Secure Shell (SSH), Gesicherte Kommunikation über unsichere Netze*. http://www-user.tu-chemnitz.de/ hot/ssh, 11 2006.

[18] WINTOTAL, REDAKTION: *Schreibschutz fuer USB Storage Device*. http://www.wintotal.de/Tipps/Eintrag.php?TID=986.

[19] WITT, BERNHARD C.: *IT - Sicherheit kompakt und verständlich*. Verlag Vieweg, 2006.