JOHANNES KEPLER UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche Fakultät

# Umsetzung von Sicherheitsstandards und dazu konforme Richtlinien für eine geplante IT-Erweiterung in einer Elektronikfirma

MASTERARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Masterstudium

NETZWERKE UND SICHERHEIT

Eingereicht von:
Roland Pachinger

Angefertigt am:
Institut für Informationsverarbeitung und Mikroprozessortechnik

Betreuung und Beurteilung:
o. Univ. Prof. Dr. Jörg R. Mühlbacher

Seewalchen, August 2010

## KURZFASSUNG

Ziel dieser Masterarbeit ist die Umsetzung von Sicherheitsstandards für die IT-Infrastruktur bei einer Elektronikfirma. Nach einer Einführung über die Arbeitsweise werden die verwendeten Sicherheitshandbücher erklärt. Es erfolgt die Ermittlung der existierenden Informationssicherheitsrisiken und die Modellierung der IT-Infrastruktur. Die Informationssicherheitsrisiken werden gewichtet und daraus die notwendigen Sicherheitsmaßnahmen ermittelt. Mit den Maßnahmen werden im Wesentlichen Security-Risiken beseitigt, Risiken oder Mängel bei der Safety (Feuer, Verletzung,…) werden dokumentiert. Weiters ist auch die Ausfallssicherheit (Redundanz, Stromversorgung, …) nicht primäres Ziel, es werden aber einige Aspekte umgesetzt.

Ein wichtiges Werkzeug bei der Einführung des Sicherheitsstandards sind IT-Sicherheitsrichtlinien. Entwurf, Verbreitung und Schulung von IT-Sicherheitsrichtlinien ermöglichen die Einführung einer firmenweiten Sicherheitspolitik und sind ebenfalls in dieser Masterarbeit beschrieben.

Ein weiteres Ziel dieser Diplomarbeit ist die Planung der IT-Erweiterung in dieser Firma und die Ausstattung eines zweiten Serverraumes im neuen Firmenhauptgebäude.

## ABSTRACT

The goal of this master's thesis work is the implementation of network security standards for the IT infrastructure of an electronics company. After an introduction to the approach employed in the thesis work, IT security handbooks are explained. This is followed by a determination of existing information security risks and the modeling of the IT infrastructure. The information security risks are weighted and thereby the necessary security measures are derived. The selected measures largely eliminate the security risks, and risks or shortcomings in terms of safety are documented. While alleviation of safety hazards (fire, injury, etc.) is not a primary goal of this master's thesis, whenever such was possible with simple means, these means were naturally applied. Furthermore, fail-safe realization (redundancy, power supply, etc.) was likewise not a primary goal, but some aspects were realized.

An important tool in the implementation of the security standard is IT security guidelines. Design, dissemination and training regarding IT security guidelines enable the implementation of a company-wide security policy; hence these measures are also described in this master's thesis.

An additional goal of this master's thesis work was to extend the IT infrastructure of the company and to equip a second server room in the firm's new main building.

## DANKSAGUNG

Ich möchte mich an dieser Stelle bei einigen Personen danken, die mich im Studium und im Speziellen bei dieser Masterarbeit unterstützt haben.

An erster Stelle stehen meine Frau und meine nunmehr drei Kinder, ohne deren Unterstützung und Verständnis dieses Studium neben meiner Arbeit nicht möglich gewesen wäre.

Weiters bedanke ich mich bei meinem Betreuer und FIM-Institutsvorstand Prof. Dr. Jörg R. Mühlbacher für seine umsichtige und unterstützende Betreuung bei der Masterarbeit.

Ich bedanke mich bei der Firmenleitung der zu betreuenden Firma für die Möglichkeit, diese Arbeit dort machen zu können und im Besonderen beim zuständigen IT-Leiter der Firma für die Unterstützung und den Umsetzungswillen für die nicht immer einfachen Maßnahmen.

Am Ende bedanke ich mich bei allen Studienkollegen, die mit mir einen Teil des Studiums mitgegangen sind, für die Freundschaft und Zusammenarbeit.

## HINWEIS

Im vorliegenden Text wird aus Gründen der Lesbarkeit z.B. anstatt die Mitarbeiterin und der Mitarbeiter oder die IT-Leiterin und der IT-Leiter häufig nur die männliche Form benutzt. Es ist aber ein Anliegen ausdrücklich zu betonen, dass damit keinerlei geschlechtsspezifische Absicht verbunden ist.

# INHALT

# 1 ALLGEMEINE PROBLEMSTELLUNG

## 1.1 Überlegungen zur IT-Sicherheit

*"Security is a process, not a product"*

Bruce Schneier, Crypto-Gram Newsletter, 15.Mai 2000

Viele Organisationen sind heute von der modernen Informationstechnologie (IT) abhängig. Die IT dient als Basis für zahlreiche Geschäftsprozesse: Vom Einkauf über die Produktion bis zum Verkauf sowie die komplette Verwaltung.

Der Einsatz von Informations- und Kommunikationstechnologien (IKT) ist für Unternehmen besonders wichtig. Im Jänner 2009 nutzten 98% der österreichischen Unternehmen mit mindestens 10 Beschäftigten das Internet. Dies zeigen die Ergebnisse einer Erhebung, die von der STATISTIK AUSTRIA zum neunten Mal durchgeführt wurde. Rund 3.650 Unternehmen mit mindestens 10 Beschäftigten haben an der Befragung teilgenommen. Eine eigene Website stellt für Unternehmen ein wichtiges Informations- und Kommunikationsmedium dar. Bereits 80% aller Unternehmen präsentierten im Jänner 2009 sich und ihre Produkte oder Dienstleistungen über solch eine Website. [STAT09]

Diese prinzipiell positive Entwicklung führt zu einer zunehmenden Abhängigkeit der Organisationen von der Verfügbarkeit der IT, der Integrität (Unversehrtheit) der Daten sowie dem Schutz vor unberechtigtem Zugriff auf Daten. Diese Anforderungen werden unter dem Begriff IT-Sicherheit zusammengefasst. Da eine 100%ige IT-Sicherheit nicht erreichbar ist, müssen die mit dem Einsatz von IT verbundenen Risiken auf ein Niveau gebracht werden, das aus unternehmerischer Sicht vertretbar ist und dauerhaft gehalten werden kann. Um dieses Ziel zu erreichen, ist die Einführung eines IT-Risikomanagements notwendig. Standards spielen im Rahmen des IT-Risikomanagements eine wichtige Rolle. Der Einsatz von IT-Sicherheitsstandards im Unternehmen oder in einzelnen Bereichen macht die sicherheitsrelevanten IT-Prozesse des Unternehmens transparent und damit beherrschbar und reduziert somit das Gesamtrisiko. [BITCOM01], Kapitel 1

Die Sicherheit der Informationstechnologie (IT-Sicherheit) wird heutzutage immer noch zu häufig als eine Anzahl von operationellen Sicherheitsmassnahmen angesehen. Vielmehr gilt es aber neben diesen operationellen Massnahmen auch organisatorische Sicherheitsmassnahmen zu beachten, um die Risiken zu minimieren. Die organisatorischen Massnahmen müssen auf Führungsebene eines Unternehmens entschieden werden. Die IT-Sicherheit ist ein Bestandteil des Qualitätsmanagements. Das Ziel der IT-Sicherheit ist es letzendlich die Vertraulichkeit, Verfügbarkeit und Integrität in den vorgegebenen Rahmenbedingungen (wie Budget, gesetzlichen Regelungen) zu gewährleisten. Die Verantwortung für die Erreichung dieses Zieles obliegt der obersten Instanz. Die Zielvorgaben müssen periodisch überprüft und angepasst werden. Somit ist die IT-Sicherheit als ein Prozess anzusehen, der mittels Regelwerken durchgeführt und unterstützt werden kann, wie ISO-27001 und ISO-27002, BSI-Grundschutz. [UNIFR01]

Im Bereich der IT-Sicherheit geht es nicht um Sicherheit im mathematischen Sinne, sondern eher um eine subjektive und nur sehr schwer messbare Sicherheit. IT-Sicherheit kann nicht umfassend definiert werden, gerade deshalb ist es wichtig, die Grundsätze der IT-Sicherheit zu kennen: [BÖNI08]

- Es gibt keine 100%ige Sicherheit.
- Sicherheit kann nie bewiesen werden, sondern nur Unsicherheit.
- Sicherheit ist nicht das Ziel, sondern der Weg.
- Schutzmaßnahmen sind eine Kosten-/Nutzenrechnung: Vor wem will ich meine Informationen schützen und was sind sie uns / einem Angreifer wert?
- Eine Schutzmaßnahme sollte nicht mehr kosten als das, was ich schützen will, wert ist.
- IT-Sicherheit wird beeinflusst durch Menschen, Prozesse und Technologie.
- IT-Sicherheit wird mittels Risiko-Managements erreicht.

## 1.2 Security und Safety

Bei der Erhebung der Informationssicherheitsrisiken liegt der Focus auf der Security, es werden aber auch die Anforderungen an die „Safety“ überprüft und dokumentiert. Übersetzt in die deutsche Sprache liefern beide Begriffe das Ergebnis „Sicherheit“.

Um den Unterschied zwischen den beiden Begriffen klar zu stellen, folgt ein kurzer Erklärungsversuch:
Die englische Sprache bietet die im Deutschen leider fehlende Unterscheidung zwischen safety und security, die zwei verschiedene Aspekte von Sicherheit näher eingrenzt. Safety bezieht sich auf die Zuverlässigkeit eines Systems, speziell in Bezug auf dessen Ablauf- und Ausfallsicherheit. Security bezeichnet dagegen den Schutz eines Systems vor beabsichtigten Angriffen. Die beiden Begriffe sind nicht völlig unabhängig voneinander: Safety schließt auch Security mit ein, was bedeutet, dass ohne einem gewissen Level an Security keine ausreichenden Safety Eigenschaften erzielt werden können. [STE01]

**Safety** ist der Schutz der Systemumgebung (incl. Menschen) vor nicht ordnungsgemäßem Verhalten des Systems. Das System nimmt demnach keine nicht spezifizierten Zustände ein, daher auch Schutz der Umgebung vor Fehlverhalten des Systems selbst. Im erweiterten Sinn folgt daraus: Safety ist der Schutz gegen zufällig oder unabsichtlich eintretenden Ereignissen. **Security** ist der Schutz (incl. aller Maßnahmen, diesen Schutz zu erreichen) des Systems vor bedrohendem Verhalten seitens der Systemumgebung. Das System nimmt nur solche Systemzustände ein, die zu keiner unauthorisierten Informationsveränderung oder –gewinnung führt. Eine Bedrohung ist eher absichtlich oder geplant. [MÜHL07], Seite13f.

## 1.3 Risiko und Risikoanalyse

Der Begriff Risiko ist in aller Munde, eine einhellige verbale Definition des Begriffes „Risiko“ gibt es nicht. Es folgen nun einige Definitionsversuche des Begriffes selbst:

*“Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequences.”* [SCHBI07], Seite24

*„Ein Risiko ist die Kombination der Wahrscheinlichkeit eines Ereignisses und dessen Konsequenz. Die Konsequenz basiert auf mangelhaften oder fehlerhaften internen Prozessen, Menschen und Systemen oder externen Ereignissen. Die Konsequenz ist sowohl eine positive wie auch eine negative Abweichung von einem erwarteten*

*Ergebnis. Das Ereignis ist unerwünscht und tritt unerwartet auf. Das Ereignis ereignet sich plötzlich und kaum wahrnehmbar.“* [JENZER04]

Das Risiko R einer Bedrohung errechnet sich formal aus der Eintrittswahrscheinlichkeit p (oder relativen Bedrohung) eines Schadensereignisses mal der Höhe des potentiellen Schadens S. [MÜHL07], Seite43

$$R = p \cdot S$$

Die Risikoanalyse dient zur Identifikation und Abschätzung von Risiken. Die folgenden Fragen helfen bei der Risikoanalyse:

- Welche Gefährdungen für das vorliegende IT-System sind denkbar?
- Welche möglichen Ursachen (Schwachstellen) kann es dazu geben?
- Wie hoch ist die Wahrscheinlichkeit des Eintretens?
- Welcher potentielle Schaden entsteht?
- In welchem Verhältnis stehen potentieller Schaden und Kosten zur Vermeidung desselben?

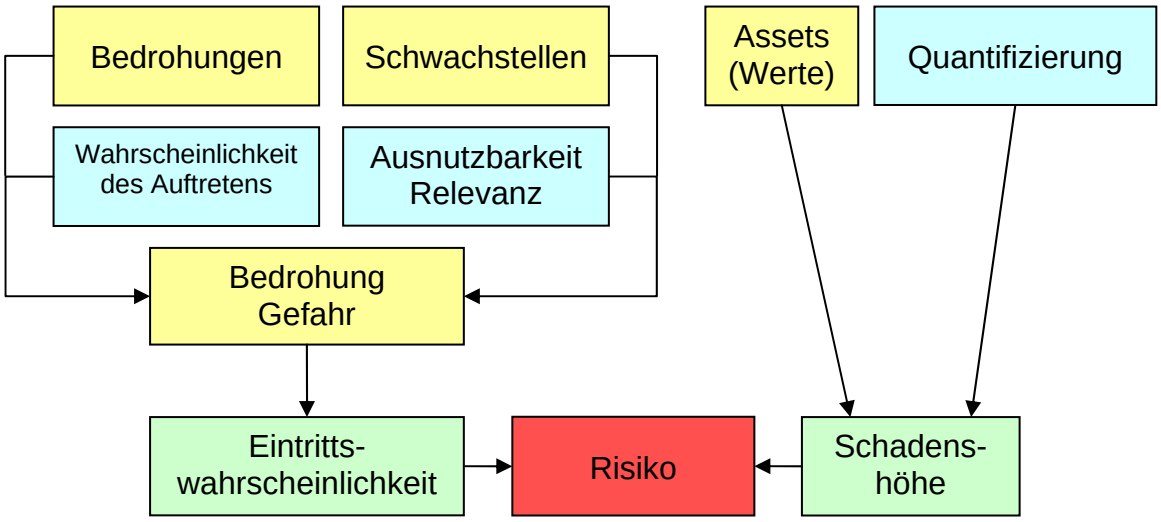



**Abbildung 1: Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe**

Bei der Risikoanalyse geht es letztlich darum, dass alle im jeweiligen Einsatzkontext eines IT-Systems möglichen Risiken und Bedrohungen durch organisatorische und dann folgend durch technische Massnahmen reduziert werden, dass für einen Betreiber eines Systems und die davon Betroffenen ein tragbares Restrisiko verbleibt. Dabei handelt es sich bei der Risikoanalyse sowohl um eine subjektive Einschätzung als auch um quantifizierbare Größen. [MÜHL07], Seite 46ff

Zusätzliche Ausführungen zum Thema Risikoanalyse im Kontext des Österreichischen Sicherheitshandbuches gibt es im Kapitel 2.3.2.4.

## 1.4 IT-Grundschutz

Der IT-Grundschutz ist die Basis für Informationssicherheit. Der IT-Grundschutz geht von einer pauschalierten Gefährdungslage aus. Die Grundidee dahinter ist, dass viele Systeme auch ähnliche Risiken haben. Für den IT-Grundschutz werden typische IT-Komponenten, Geschäftsprozesse und Anwendungen betrachtet. Eine detaillierte Risikoanalyse entfällt dadurch. Pauschalierten Gefährdungen können Sicherheitsmaßnahmen aus vorgegebenen Katalogen entgegen gesetzt werden. Die Vorteile sind die Reduktion des Aufwandes für die Risikoanalyse, die rasche Reduktion des Risikos und ein hoher Schutz gegen die häufigsten Bedrohungen. Ein Nachteil ist, dass der pauschalierte Schutzlevel für einzelne Systeme nicht ausreichend sein kann. In diesem Fall muss bei besonders sicherheitsrelevanten Systemen eine detaillierte Risikoanalyse erfolgen. Die Anforderungen, die der IT-Grundschutz an ein Unternehmen stellt, sind in Sicherheitshandbüchern festgelegt. Die Sicherheitshandbücher sind im Kapitel 2.3 beschrieben.

## 1.5 Verantwortlichkeit der Firmenleitung

IT-Sicherheit und die benötigten Sicherheitsmaßnahmen kosten Zeit und Geld, und Zeit ist wiederum Geld, wenn man an die Kosten der Arbeitszeit denkt. Die Firmenleitung ist angehalten, die notwendigen Sicherheitsmaßnahmen zu finanzieren und auch die Arbeit der IT-Mitarbeiter zu unterstützen. Die organisationsweite Sicherheitspolitik ist eine Managementaufgabe, allein daran ist die grosse Verantwortung der Firmenleitung erkennbar.

Die ISO27001 (siehe Kapitel 2.2) definiert die Anforderungen an Informations-sicherheitsmanagementsysteme (ISMS). In diesem Regelwerk ist die Verantwortung des Managements unter zwei Gesichtspunkten festgeschrieben: der Verpflichtung und das Engagement des Managements gegenüber dem ISMS und der Bereitsstellung von sachlichen und personellen Ressourcen für das ISMS. Ein weiterer Punkt ist die stete Sensibilisierung der Mitarbeiter für die Wichtigkeit des ISMS. [ITSM08, Seite79ff].

Die Vorteile eines ISMS für die Firmenleitung sind einerseits ein funktionierendes IT-Risikomanagement und andererseits eine rechtliche Absicherung. Nach Angaben

von Gerichtssachverständigen werden zur Bewertung IT-bezogener Delikte gültige Weltstandards wie die ISO27001 für Informationssicherheit herangezogen, da diese international anerkannte Methoden für IT-Risikomanagement umfassen. Unternehmen die Risikomanagement nach ISO27001 betreiben, können damit der Verbandshaftung entgehen. [PRESS07]

Die Implementierung von und das Einhalten der Datensicherheitsmaßnahmen in einem Unternehmen sind zentrale Aufgaben eines verantwortungsvollen Managements. Vorstand und Geschäftsführung eines Unternehmens sind kraft der sie treffenden kaufmännischen Sorgfaltspflicht zu entsprechenden Maßnahmen verpflichtet. Das Datenschutzgesetz 2000 bezieht sich auf direkt oder indirekt personenbezogene Daten und schreibt konkrete Datensicherheitsmaßnahmen vor. Zu schützende Daten wären z.B. Kunden- und Lieferantendaten. Auch dann, wenn es sich nicht um personenbezogene Daten handelt, sind die Leitlinien des Datenschutzgesetzes als Mindestmaßstab analog oder durch vertragliche Vereinbarung in Geschäftsbeziehungen anzuwenden. Aus rechtlicher Sicht ist es daher dringend zu empfehlen, Datensicherheitsmaßnahmen nach dem Stand der Technik im Unternehmen zu ergreifen und die ergriffenen Maßnahmen zu dokumentieren. Eine Verletzung von Datensicherheitsmaßnahmen kann neben Schadenersatzverpflichtungen auch unmittelbare Haftungen der verantwortlichen Unternehmensmitarbeiter (EDV-Abteilungsleiter) und vor allem der Geschäftsführungsorganwalter (Vorstand, Geschäftsführer, Prokuristen) nach sich ziehen. [SICK04]

Unternehmen haften für Schäden, die sie durch Fahrlässigkeit verursachen. Ein Versenden von Viren wegen fehlendem Virenschutz muss nach dem heutigen Stand der Technik als Fahrlässig betrachtet werden. Hierbei ist zu beachten, dass das Unternehmen als ganzes haftet, nicht jedoch der Arbeitnehmer, soweit er nicht grob fahrlässig oder vorsätzlich gehandelt hat. Zusätzlich zu beachten ist die Haftung der Geschäftsführer gegenüber dem eigenen Unternehmen. [SICK04]

# 2 LÖSUNGSANSÄTZE

## 2.1 Vorgehensmodell

Das Vorgehensmodell beschreibt den allgemeinen Ablauf bei der Einführung des IT-Grundschutzes. Als Muster für dieses Modell wurde die Einführung des IT-Grundschutzes des BSI (Kapitel 2.3.1) verwendet. [SCHBI08]

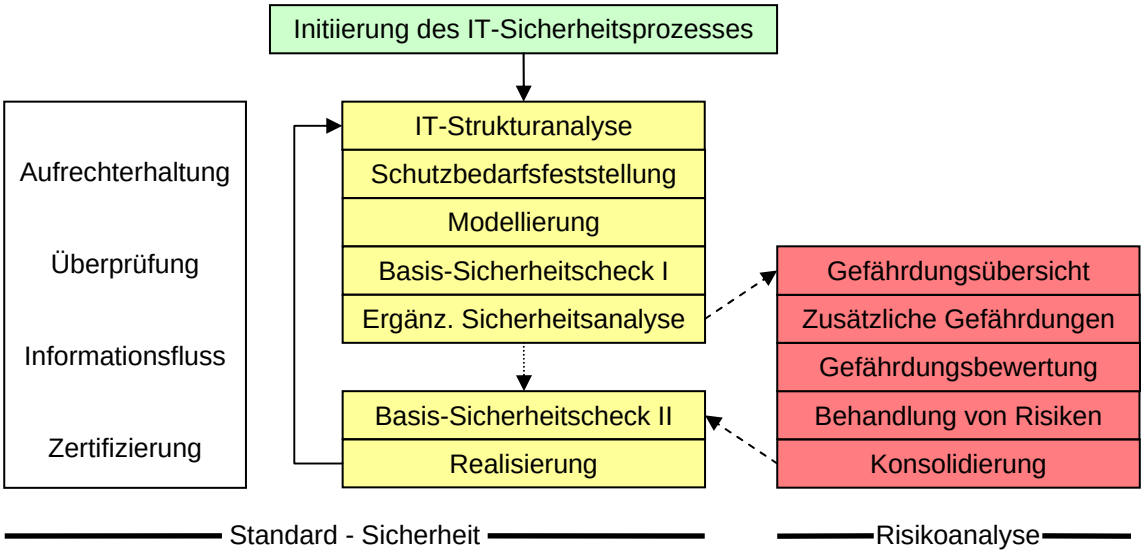



**Abbildung 2: Vorgehensmodell IT-Grundschutz**

### 2.1.1 IT-Strukturanalyse

Die IT-Strukturanalyse definiert die Teile, aus denen das zu untersuchende System besteht und definiert die Abhängigkeiten zwischen den Teilen. Die gemeinsam untersuchten Teile werden als IT-Verbund bezeichnet. Ein IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die bei der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann die gesamte IT einer Institution, einzelne Bereiche (Abteilungsnetz, Personal-Informationssystem) oder Geschäftsprozesse umfassen. Die Aufgaben der IT-Strukturanalyse sind Erstellung bzw. Aktualisierung eines Netzplanes (grafisch), die Erhebung der IT-Systeme (Tabelle), die Erfassung der IT-Anwendungen und der zugehörigen Informationen (Tabelle), die Erhebung der IT-Räume und die Komplexitätsreduktion durch Gruppenbildung.

### 2.1.2 Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung werden die Anforderungen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit festgelegt. Der Schutzbedarf ist in drei Kategorien eingeteilt:

- Normal: Die Schadensauswirkungen sind begrenzt und überschaubar
- Hoch: Die Schadensauswirkungen können beträchtlich sein
- Sehr Hoch: Die Schadensauswirkungen können existenziell bedrohlich sein

Bei einem sehr hohen Schutzbedarf ist eine detaillierte Risikoanalyse notwendig.

### 2.1.3 Modellierung

Bei der Modellierung werden Gefährdungs- und Maßnahmenkataloge gegenüber gestellt und daraus IT-Grundschutz-Bausteine ermittelt. Diese Bausteine geben Maßnahmenempfehlungen vor, die zur Abwendung der Gefährdungen führen.

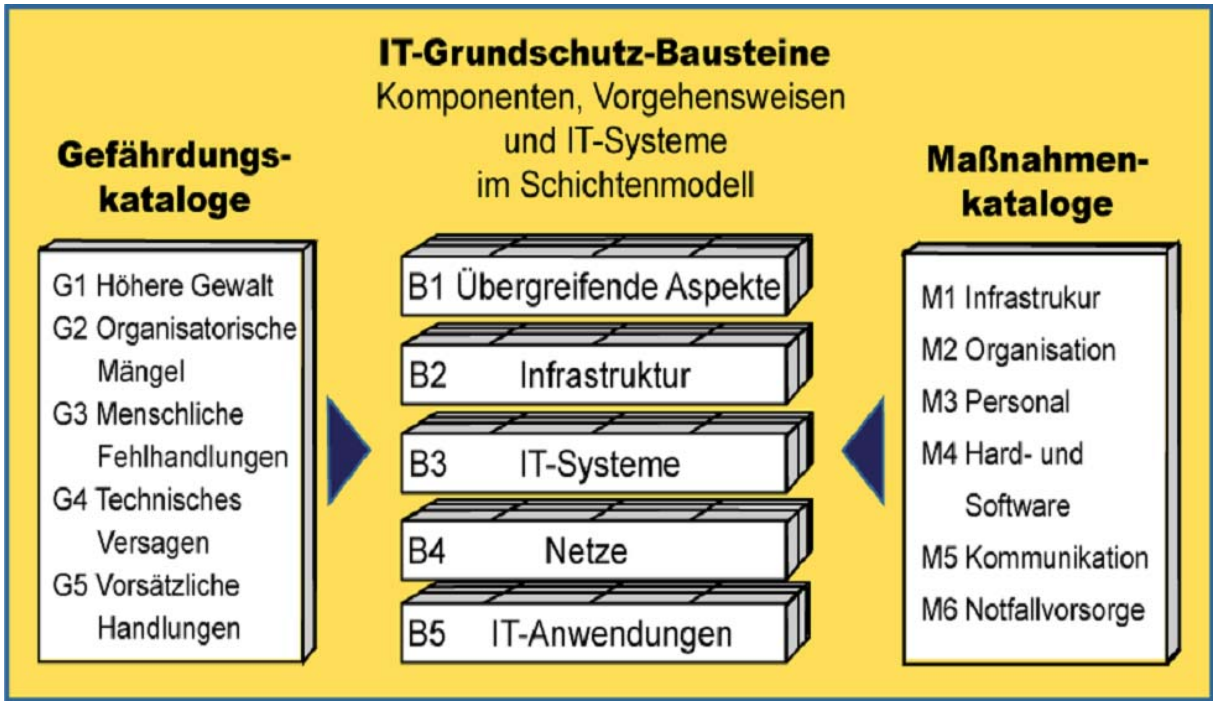



**Abbildung 3: IT-Grundschutz-Kataloge**

### 2.1.4 Basis-Sicherheitscheck

Beim Basis-Sicherheitscheck werden die empfohlenen Maßnahmen aus dem Grundschutz-Modell und die bereits realisierten Maßnahmen aus der IT-Strukturanalyse in einem Soll/Ist-Vergleich gegenüber gestellt. Daraus resultieren die noch umzusetzenden Maßnahmen. Im Idealfall sollen alle diese Maßnahmen umgesetzt werden.

### 2.1.5 Ergänzende Sicherheitsanalyse

Die ergänzende Sicherheitsanalyse entspricht einer detaillierten Risikoanalyse und kommt nur zur Verwendung, wenn ein sehr hoher Schutzbedarf besteht. Es werden hierbei eine Übersicht über die möglichen und zusätzlichen Gefährdungen und eine anschliessende Gefährdungsbewertung durchgeführt. Anhand dieser Bewertung werden die auftretenden Risiken behandelt und konsolidiert, d.h. das akzeptierte Restrisiko festgelegt. Durch einen weiteren Basis-Sicherheitscheck werden die notwendigen Maßnahmen ermittelt.

### 2.1.6 Realisierung

Im letzten Schritt werden die notwendigen Maßnahmen konsolidiert, d.h. eine Umsetzungsstrategie der Maßnahmen geplant und in weiterer Folge auch realisiert. Nach der Einführung des Standards müssen die getroffenen Maßnahmen (personell, organisatorisch, technisch) in den regulären Betrieb übergehen. Hierfür sind Mitarbeiterschulungen, -information sowie ggf. Prozessanpassungen notwendig. Im Rahmen des regulären IT-Betriebs kann die Einhaltung des Standards durch zwei aufeinander aufbauende Verfahren überprüft und gewährleistet werden

### 2.1.7 Aufrechterhaltung im laufenden Betrieb

Nach der Realisierung der umgesetzten Maßnahmen wird das Vorgehensmodell mit einer neuerlichen Strukturanalyse begonnen. Diese Überprüfung macht die Wirkung der gesetzten Maßnahmen sichtbar und messbar und gewährleistet eine Aufrechterhaltung im laufenden Betrieb.

Für das Vorgehensmodell sind die Einhaltung der Sicherheitsmaßnahmen und die Aktualität derselben wichtig. Diese Aspekte sollen durch regelmäßige Audits von internen oder externen Partnern überprüft werden. Dadurch können Unternehmen ihre IT-Sicherheit immer weiter verbessern und sukzessive Sicherheitslücken schließen.

Im Rahmen eines Audits kommt ein externer (zertifizierter) Auditor für einige Tage ins Unternehmen. Anhand der Vorgaben des Standards sowie der Dokumentation des IT-Betriebs wird der Ist-Stand mit dem Soll-Konzept verglichen. Empfehlungen für die Verbesserung der IT-Sicherheit werden ausgesprochen. Diese sollten vom Unternehmen im Nachgang umgesetzt werden. Eine Auditierung kann den gesamten

IT-Betrieb umfassen, sich aber auch nur auf beispielsweise neu eingesetzte Sicherheitskomponenten beschränken (Beispiel: neue Firewall).

### 2.1.8 Zertifizierung

Einige IT-Sicherheitsstandards können als Grundlage für eine Zertifizierung herangezogen werden.
Ein Zertifikat ist eine unabhängige Bestätigung dafür, dass alle (soweit anwendbare) im Standard geforderten Sicherheitsmaßnahmen zum Zeitpunkt der Zertifizierung dokumentiert und tatsächlich umgesetzt sind.
Durch die Ausstellung eines Zertifikates, mit dem die Umsetzung des Standards bestätigt wird, kann diese Dritten transparent gemacht werden. Dritte können hierbei Kunden, Banken, Versicherungen oder auch die Öffentlichkeit sein. Der Aufwand für die Zertifizierung ist abhängig vom Unternehmen und dem Zertifizierungsziel. Hierbei kann jedoch von einem externen Aufwand von einigen Tagen bis einigen Wochen ausgegangen werden. Der interne Aufwand kann deutlich höher sein, je nach Vorbereitungsstand des Unternehmens. Eine generelle Aussage kann nicht getroffen werden. Bei der Auswahl des Zertifizierers ist zu beachten, dass einige Standards einen akkreditierten Zertifizierer fordern.
Bei einer Zertifizierung nach dem IT-Grundschutz wird der IT-Verbund des Antragstellers durch eine zertifizierte Prüfstelle überprüft und ein Prüfbericht erstellt. Dieser Prüfbericht wird wiederum durch eine amtliche Zertifizierungsstelle überprüft. Das Resultat ist ein Grundschutzzertifikat, das dem Antragsteller die korrekte Umsetzung der IT-Grundschutzmaßnahmen bestätigt.

## 2.2 Standards

### 2.2.1 Nutzen von Standards

Der Einsatz von IT in Unternehmen birgt Risiken, die im Rahmen eines IT-Risikomanagements auf ein angemessenes Niveau reduziert werden sollten. Dabei kommt es einerseits darauf an, Risiken umfassend zu ermitteln und andererseits die Schutzmechanismen aus wirtschaftlichen Gründen nicht aufwendiger zu gestalten, als es das zulässige Risiko verlangt.

Die Auswahl und die Anwendung angemessener IT-Sicherheitsstandards sind ein Teil des IT-Sicherheitsmanagements. Die Etablierung eines umfassenden IT-Sicherheitsmanagements ist eine anspruchsvolle Aufgabe. Hierbei können Planungsfehler entstehen, die zu ineffektiven und vor allem ineffizienten Maßnahmen führen können. Firmeneigene Vorgehensweisen sind in der Regel teuer in der Umsetzung und entsprechen erfahrungsgemäß häufig nicht dem Stand der Technik. Daher ist es sinnvoll, auf bewährte Vorgehensweisen zurückzugreifen, die in Standards festgehalten sind. Standards können helfen, die sicherheitsrelevanten IT-Prozesse zum Vorteil des Unternehmens, der Kunden, der eigenen Produkte sowie der Mitarbeiter zu verbessern. Sie bieten Hilfestellung bei der Entwicklung von generischen Maßnahmen auf Management-Ebene bis zu detaillierten technischen Implementierungen, und liefern Methoden für ein leistungsfähiges IT-Sicherheitsmanagement oder definieren die IT-Sicherheit von ausgewiesenen Produkten. Standards können sowohl eigenständig als auch methodisch eingebettet in ein anderes System fortlaufend betrieben werden.

Wesentliche Ziele beim Einsatz von Standards sind in folgender Tabelle zusammengefasst: [BITCOM01, Kapitel2]

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

**Tabelle 1: Ziele beim Einsatz von Standards**

### 2.2.2 Arten von Standards

Die folgenden Standards bieten Richtlinien für einzelne Aspekte des IT-Sicherheits- und Risikomanagements an. Hierzu gehört:

- Festlegen von Sicherheitsstrategien und -leitlinien von Organisationen
- Bewerten von Risiken der IT-Sicherheit
- Ermitteln von Sicherheitszielen und ableiten von Sicherheitsanforderungen
- Auswählen von geeigneten Gegenmaßnahmen (unter anderem auch Grundschutzmaßnahmen) und deren dauerhafte Umsetzung sicherzustellen

Dies alles erfolgt in der Regel im Rahmen des IT-Sicherheits- oder IT-Risikomanagements, welches das systematische Erkennen, Bewerten, Steuern und Überwachen von IT-Sicherheitsrisiken umfasst. [BITCOM01]

#### *2.2.2.1 ISO/IEC 27000er-Familie[1]*

Die ISO/IEC 27001 ist der bedeutendste Standard für ein Informationssicherheits-managementsystem. Weitere Standards aus der ISO/IEC 27000er-Familie ergänzen ISO/IEC 27001. So werden in ISO/IEC 27000 die Terminologie und in ISO/IEC 27002 einzelne Maßnahmen erläutert. Darüber hinaus werden in ISO/IEC 27006 die Anforderungen an Stellen beschrieben, die ein ISMS auditieren oder zertifizieren. Eine Reihe weiterer Standards in der 27000er-Reihe befindet sich zurzeit in der Erstellung. [SCHBI081]

[1] ISO:= International Organisation for Standardization (Internationale Organisation für Normung) ist die internationale Vereinigung von Normungsorganisationen und erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrotechnik und der Elektronik, für die die Internationale elektrotechnische Kommission (IEC) zuständig ist, und mit Ausnahme der Telekommunikation, für die die Internationale Fernmeldeunion (ITU) zuständig ist. Gemeinsam bilden diese drei Organisationen die WSC (World Standards Cooperation). [WIKI-ISO]

IEC:= International Electrotechnical Commission (Internationale Elektrotechnische Kommission) ist ein internationales Normierungsgremium mit Sitz in Genf für Normen im Bereich der Elektrotechnik und Elektronik. Einige Normen werden gemeinsam mit ISO entwickelt. [WIKI-IEC]

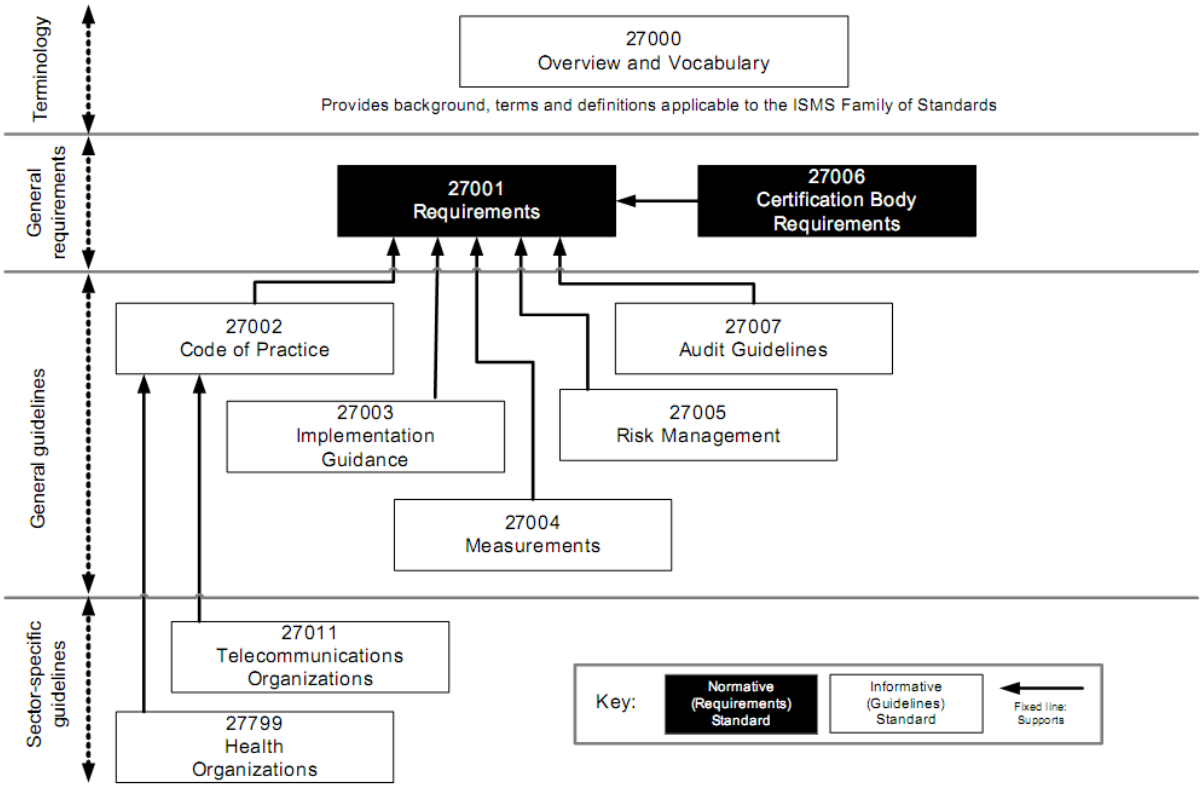



**Abbildung 4: ISO27000-Familie – Quelle [ISOITTF1]**

### *2.2.2.2 ISO/IEC 27001 – ISMS-Anforderungen*

Die ISO/IEC 27001 ist aus dem Teil 2 des britischen Standards BS 7799-2 hervorgegangen. Erklärtes Ziel des Standards ist es, die Anforderungen an ein ISMS im Rahmen eines Prozess-Ansatzes darzustellen.

Das Dokument beinhaltet Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt. Da das Dokument sehr generisch gehalten ist, um auf alle Organisationen unabhängig von Typ, Größe und Geschäftsfeld anwendbar zu sein, haben diese Anforderungen einen geringen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse wohl definiert sind. Aufbauend auf der Norm können nationale Zertifizierungsschemata definiert werden. Als Managementstandard richtet sich das Dokument an die Geschäftsleitung und den IT-Sicherheitsbeauftragten, weniger an die Umsetzungsverantwortlichen, Techniker oder Administratoren. Wegen der engen methodischen Anlehnung an die ISO 9000 (Qualitätsmanagement) und die ISO 14000 (Umweltmanagement) kann die ISO/IEC 27001 als ein Qualitätsstandard für Managementsysteme bezüglich Informationssicherheit angesehen werden. [BITCOM01]

#### *2.2.2.3 ISO/IEC 27002 – Leitfaden zum Informationssicherheitsmanagement*

Die ISO/IEC 27002 ist aus dem Teil 1 des britischen Standards BS 7799-1 hervorgegangen und trägt den Titel *„Code of practice for information security management“*. Dieser wurde zuerst in den internationalen Standard IS 17799:2000 umgewandelt. Aufgrund der Bestrebungen, alle Standards, die ISMS betreffen, als ISO/IEC 27000er-Reihe zusammenzuführen, wurde IS 17799:2000 im Jahr 2007 in ISO/IEC 27002:2005 umbenannt.

Grundsätzlich ist dieser Standard dort anzuwenden, wo ein Schutzbedarf für Informationen besteht. Ziel des Dokuments ist es, Informationssicherheit als Gesamtaufgabe darzustellen. In den Prozess der Informationssicherheit sind alle Bereiche der Organisation einzubeziehen, die alle an der Erhebung, Verarbeitung, Speicherung, Löschung von Informationen beteiligt sind. Der Anwendungsbereich ist somit ohne einen konkreten Bezug zu den Anforderungen in einer Organisation nicht abgrenzbar. Das Dokument richtet sich an IT-Sicherheitsbeauftragte.

Die ISO/IEC 27002 ist in Themenbereiche (control sections) gegliedert, für jeden Bereich gibt es ein oder mehrere Sicherheitsziele (security objectives) und für jedes Sicherheitsziel ein oder mehrere Maßnahmen (security controls).

Die Themenbereiche sind wie folgt:

- Risikoeinschätzung und –behandlung
- Sicherheitsleitlinie
- Organisation der Informationssicherheit
- Management von organisationseigenen Werten
- Personalsicherheit
- Physische und umgebungsbezogene Sicherheit
- Betriebs- und Kommunikationsmanagement
- Zugangskontrolle
- Beschaffung, Entwicklung und Wartung von Informationssystemen
- Umgang mit Informationssicherheitsvorfällen
- Sicherstellung des Geschäftsbetriebs
- Einhaltung von Vorgaben

[SCHBI081]

#### 2.2.2.4 ISO/IEC 27003 – ISMS-Implementierungshilfe

Der Standard ISO/IEC 27003 trägt den Titel *„Information security management system implementation guidance“* und soll Unterstützung in der Implementierung eines Informationssicherheitsmanagements geben. Der Standard wurde im Jahr 2010 veröffentlicht und wird mit ISO/IEC 27003:2010 bezeichnet. [ISO27003]

#### 2.2.2.5 ISO/IEC 27004 – ISMS-Effektivitätsmessung

Der Standard ISO/IEC 27004 trägt den Titel *„Information security management measurement“.* Ziel dieses Standards ist die Messung der Effektivität von ISMS gemäß ISO/IEC 27001 und die Sicherstellung, dass die Kontrollziele der ISO/IEC 27001 auch erreicht werden. Die Kontrolle erfolgt durch Definition von messbaren Zielen und Messung in definierten Zeitabständen, um auch eine Verbesserung oder Verschlechterung der Sicherheit feststellen zu können. Der Standard wurde im Jahr 2009 veröffentlicht und wird mit ISO/IEC 27004:2009 bezeichnet.
[ISO27004] [SCHBI081]

#### 2.2.2.6 ISO/IEC 27005 – Management von Informationssicherheitsrisiken

Die ISO/IEC 27005 ist aus dem Teil 2 des bisherigen ISO/IEC 13335-2 hervorgegangen und trägt den Titel *„Information security risk management“*. Der Standard enthält Leitlinien für ein systematisches und prozessorientiertes Risikomanagement, das gegebenenfalls auch die Einhaltung der Anforderungen an das Risikomanagements nach ISO/IEC 27001 unterstützt.
Ein Informationssicherheitsrisiko wird definiert als Potential, das eine Bedrohung eine Schwachstelle eines Unternehmenswertes ausnutzt und dadurch zu einem Schaden für eine Organisation führt. Zur systematischen Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken wird ein Prozess beschrieben, der als Ergebnis eine priorisierte Liste von Risiken hat, die anschließend kontinuierlich zu verfolgen sind.
Die Anhänge des Standards enthalten unter anderem Einzelheiten und Beispiele zu Bedrohungen, Schwachstellen und Bewertungsansätzen.
Der Standard wurde im Jahr 2008 veröffentlicht und wird mit ISO/IEC 27005:2008 bezeichnet. [BITCOM01]
Die folgende Abbildung zeigt die Vorgangsweise des im Standard beschriebenen Informationssicherheitsrisikomanagementprozesses (IRM-Prozess):

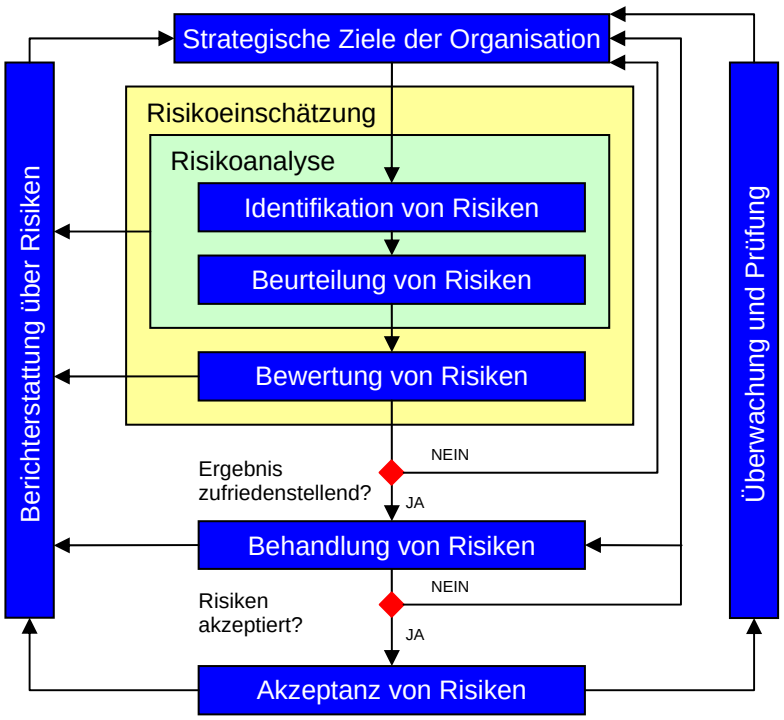



**Abbildung 5: IRM-Prozess [SCHBI081]**

### *(1) Strategische Ziele der Organisation*

Die strategischen Ziele der Organisation werden durch die Firmenleitung festgelegt und sollen:

- ein optimales Gleichgewicht zwischen Wachstums- und Ertragszielen sowie den damit einhergehenden Risiken bringen,
- einen wirtschaftlichen und wirksamen Einsatz von Ressourcen bei der Umsetzung der Organisationsziele ermöglichen,
- die Zuverlässigkeit der Berichterstattung sicherstellen und
- das Einhalten anwendbarer Gesetze und Vorschriften gewährleisten.

### *(2) Risikoeinschätzung*

Die Risikoeinschätzung definiert das gesamte Verfahren von Risikoanalyse und Bewertung von Risiken.

Das Risikoanalyseverfahren unterstützt die wirksame und leistungsfähige Arbeitsweise der Organisation durch Identifikation derjenigen Risiken, mit denen sich das Management beschäftigen sollte. [FERMA]

### *(3) Risikoanalyse*

Die Risikoanalyse umfasst die Identifikation und Beurteilung von Risiken.

### *(4) Identifikation von Risiken*

Die Identifikation von Risiken bildet den ersten Schritt im Rahmen des Risikomanagements. Risikoidentifikation ist die systematische Erhebung aller Risiken, die auf das Unternehmen einwirken.
Aufgrund der sich ständig ändernden Unternehmenssituation ist die Risikoidentifikation eine kontinuierliche Aufgabe, die in die geschäftsüblichen Arbeitsabläufe integriert werden muss. Dies fördert bei den betroffenen Mitarbeitern die Akzeptanz und vermindert den Aufwand.
In der Praxis werden vor allem folgende Methoden der Risikoidentifikation angewandt:

- *Besichtigungsanalyse:* Besichtigung des realen Geschehens, z.B. bei Elementarrisiken wie Brandrisiko.
- *Dokumentenanalyse:* Risiken aus Verträgen, Behördenbescheiden oder Planungsunterlagen sowie dem betrieblichen Rechnungswesen.
- *Organisationsanalyse:* Risiken aus einer unzureichenden Aufbau- und Ablauforganisation.
- *Mitarbeiterbefragung:* Die Mitarbeiter können viele Aspekte aus der täglichen Erfahrung am besten einschätzen. Durch Befragungen kann man sie zu Beteiligten des Risikomanagementprozesses machen. Auf der anderen Seite besteht die Gefahr der Verfälschung durch psychologische Aspekte.
- *Prüflisten:* Systematische Erhebung von Risikoinformationen per Checklisten.
- *Beobachtung der externen Faktoren:* Markt- und Technologierecherchen oder die Entwicklung der Rechtssprechung.

Diese Informationen sollten in einem dauerhaften Prozess gewonnen werden. Deshalb ist die Verantwortung für die Risikoidentifikation eindeutig zu definieren. [TEIA1]

### *(5) Beurteilung von Risiken*

Die Beurteilung von Risiken wird hinsichtlich der Eintrittswahrscheinlichkeit und der möglichen Schadensausprägung des Risikos durchgeführt. Der Erwartungswert eines Risikos ergibt sich als (vgl. dazu Kapitel 1.3):

$$R = p \cdot S$$

Die jeweilige Schadenshöhe sowie Eintrittswahrscheinlichkeit eines identifizierten Risikos ist zu bestimmen. Wenn möglich, sollte dies auf der Basis objektiver Daten, z.B. Zeitreihen, erfolgen. Ist dies nicht möglich werden qualitative Bewertungen vorgenommen, z.B.:

*"sehr wahrscheinlich"/ "wahrscheinlich" / "möglich" / "unwahrscheinlich" / "unmöglich"*

oder

*"existenzbedrohend" / "schwerwiegend" / "mittel" / "gering" / "unbedeutend"*

Wird die Eintrittswahrscheinlichkeit in ein Koordinatensystem übertragen, ergibt sich z.B. folgendes Bild:

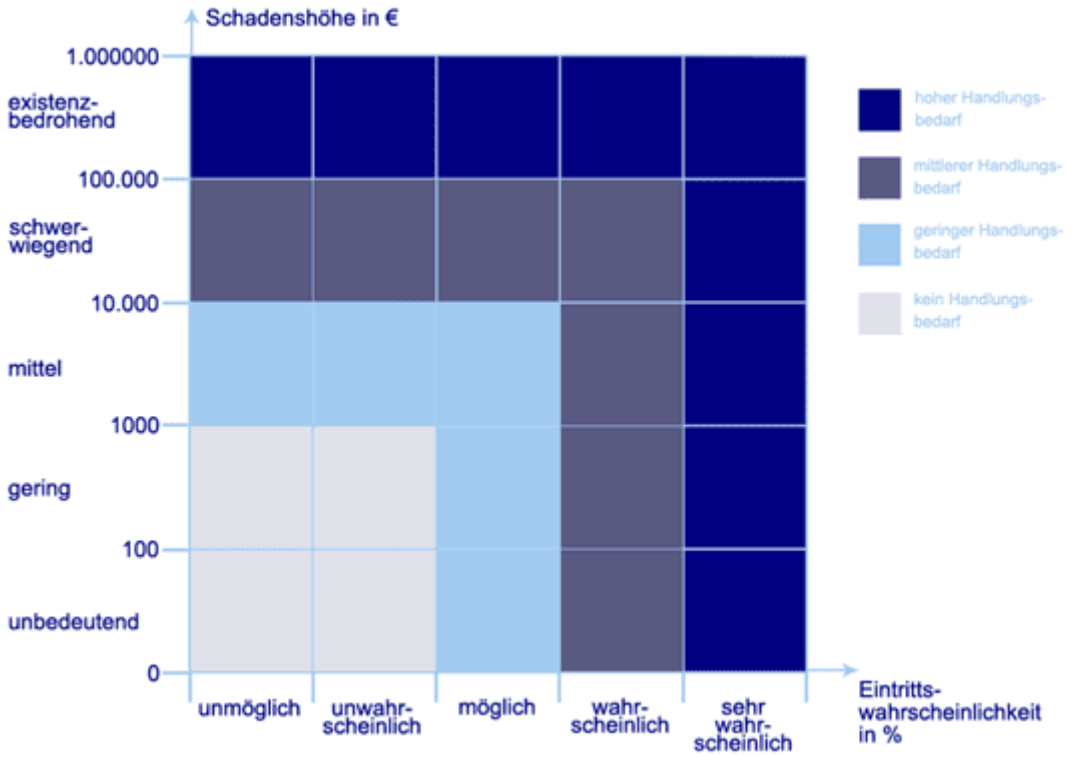



**Abbildung 6: Beurteilung von Risiken**

Aus dieser Bewertung heraus ergibt sich der Handlungsbedarf, der wiederum in Klassen eingeteilt werden kann. [TEIA2]

### *(6) Bewertung von Risiken*

Nach Abschluss des Risikoanalyseverfahrens sind die beurteilten Risiken mit den von der Organisation ausgearbeiteten Risikokriterien zu vergleichen. Zu den Risikokriterien gehören möglicherweise anfallende Kosten und Leistungen und rechtliche Auflagen. Daher dient die Risikobewertung zur Entscheidung über Risikosignifikanz für die Organisation und Akzeptanz oder Behandlung jedes spezifischen Risikos. [FERMA]

### *(7) Behandlung von Risiken*

Die Behandlung von Risiken ist der Prozess der Auswahl und Durchführung von Maßnahmen zur Risikoveränderung. Zu den Hauptelementen der Risikobehandlung gehören Risikokontrolle und Risikoeindämmung, wobei aber beispielsweise Risikovermeidung, Risikotransfer, Risikofinanzierung usw. ebenfalls umfasst sind.

Jedes Risikobehandlungssystem sollte mindestens Folgendes enthalten:

- wirksame und leistungsfähige Arbeitsweise der Organisation
- wirksame interne Kontrollen
- Einhalten von Gesetzen und Vorschriften

### *(8) Akzeptanz von Risiken*

Unter diesem Punkt werden sog. Restrisiken akzeptiert. Hierbei handelt es sich um Risiken, die verbleiben, wenn alle möglichen Maßnahmen getroffen wurden, die Risiken zu minimieren oder ihre Eintrittswahrscheinlichkeit und Tragweite gegen Null laufen zu lassen. Risiken sind allerdings dabei niemals völlig auszuschliessen. Treten Restrisiken auf, ist es Aufgabe des Projektmanagements Szenaria und Alternativpläne (Plan B) bereit zu halten, um möglichst frühzeitig die Auswirkungen einzuschränken. Hierzu ist eine vom Projektmanagement gesteuerte Risikoüberwachung gefragt. Die Restrisiken werden kontinuierlich hinsichtlich ihrer aktuellen Eintrittswahrscheinlichkeit und Folgen überwacht.

### *(9) Berichterstattung über Risiken*

Die verschiedenen Organisationsniveaus benötigen unterschiedliche Informationen aus dem Risikomanagementverfahren. [FERMA]

*Der Vorstand sollte:*

- die bedeutsamsten Risiken für die Organisation kennen
- für angemessene Sensibilisierung in der gesamten Organisation sorgen
- wissen, wie die Organisation eine Krise bewältigen wird
- wissen, wie wichtig das Vertrauen der Akteure in die Organisation ist
- überzeugt sein, dass der Risikomanagementprozess wirksam funktioniert
- eine klare Risikomanagementpolitik einschließlich Philosophie und Verantwortungen im Bereich Risikomanagement veröffentlichen

*Die Unternehmenseinheiten sollten:*

- sich der in ihren Verantwortungsbereich fallenden Risiken, ihrer etwaigen Auswirkungen auf andere Bereiche und der möglichen Auswirkungen anderer Bereiche auf sich selbst bewusst sein
- über Leistungsindikatoren verfügen, mit Hilfe derer sie die wichtigsten geschäftlichen und finanziellen Tätigkeiten überwachen, die Zielverwirklichung verfolgen und Entwicklungen identifizieren können, die ein Eingreifen erfordern (z. B. Prognosen und Haushalte)
- Systeme haben, die prognostische und budgetäre Abweichungen mit angemessener Häufigkeit melden, um ein Eingreifen zu ermöglichen
- die oberste Unternehmensleitung systematisch und umgehend über alle wahrgenommenen neuen Risiken oder Fehler der bestehenden Kontrollmaßnahmen unterrichten

*Einzelpersonen sollten:*

- ihre Rechenschaftspflicht für Einzelrisiken kennen
- verstehen, wie sie zu einer ständigen Verbesserung des Risikomanagementverhaltens beitragen können
- wissen, dass Risikomanagement Kernstück der Organisationskultur sind
- die oberste Unternehmensleitung systematisch und umgehend über alle wahrgenommenen neuen Risiken oder Fehler der bestehenden Kontrollmaßnahmen unterrichten

[FERMA]

#### *(10) Überwachung und Prüfung*

Zum wirksamen Risikomanagement gehört eine Berichts- und Revisionsstruktur zur Gewährleistung einer wirksamen Risikoidentifikation und -einschätzung und des Bestehens angemessener Kontrollen und Reaktionen. Um Verbesserungsmöglichkeiten zu identifizieren, sollte eine regelmäßige Überprüfung der Einhaltung von Politik und Normen und der Standardleistung erfolgen. Dabei ist nicht zu vergessen, dass Organisationen dynamisch sind und in dynamischen Umfeldern agieren. Veränderungen in der Organisation und ihrem Arbeitsumfeld müssen identifiziert und die Systeme in angemessener Weise abgeändert werden. Der Überwachungsprozess sollte dafür sorgen, dass für die Tätigkeiten der Organisation geeignete Kontrollen bestehen und dass die Verfahren verstanden und eingehalten werden. Veränderungen in der Organisation und ihrem Arbeitsumfeld müssen identifiziert und die Systeme in angemessener Weise abgeändert werden. [FERMA]

### *2.2.2.7 ISO/IEC27006 – Zertifizierung*

Die ISO/IEC 27006 ist aus dem Leitfaden EA-7/03 der European Accreditation Foundation hervorgegangen und trägt den Titel *„Requirements for bodies providing audit and certification of information security management systems“*. Sie basiert auf der DIN EN ISO/IEC 17021 („Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren“) und ergänzt diese um die ISMS-spezifischen Anforderungen.

Grundsätzlich ist dieser Standard dort anzuwenden, wo die Anforderungen an Zertifizierungs- und Auditierungsstellen von ISMS gemäß DIN ISO/IEC 27001 definiert werden. Primär dient er somit der Akkreditierung von Zertifizierungsstellen, kann aber auch im Rahmen von „peer assessments“ oder zur Etablierung von Auditprozessen herangezogen werden.

Ziel des Dokuments ist es, harmonisierte Anforderungen an alle Zertifizierungsstellen zu formulieren und diesen einen Leitfaden zur Umsetzung bereitzustellen, beispielsweise für Aspekte wie die Dauer von Audits.

Der Standard wurde im Jahr 2007 veröffentlicht und wird mit ISO/IEC 27006:2007 bezeichnet. [BITCOM01]

### *2.2.2.8 ISO/IEC 15408 - Common Criteria (CC)*

Die Norm ISO/IEC 15408 trägt den Titel *„Evaluationskriterien für IT-Sicherheit“* und definiert ein Kriterienwerk für die Sicherheitsevaluierung von IT-Produkten und IT-Systemen. Die Norm ist auch unter dem Namen *„Common Criteria“* bekannt. Die Common Criteria (CC) sind aus den europäischen ITSEC, den amerikanischen Federal Criteria (FC) und den kanadischen CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) entstanden und wurden von ISO/IEC JTC 1/SC 27 international standardisiert. Neben einem Katalog vordefinierter Funktionalitäten legen die CC Anforderungen an die Vertrauenswürdigkeit gemäß einer Vertrauenswürdigkeitsstufe fest. Die CC bieten die Möglichkeit, Sicherheitsanforderungen in vorevaluierten Schutzprofilen zusammenzufassen.
Der Standard besteht aus folgenden drei zusammengehörigen Teilen:

- Teil 1: Einführung und allgemeines Modell
- Teil 2: Funktionale Sicherheitsanforderungen
- Teil 3: Anforderungen an die Vertrauenswürdigkeit

Teil 1 stellt das allgemeine Konzept der Evaluationskriterien vor. Grundlegende Begriffe wie Sicherheitsanforderungen, Sicherheitsziele, Schutzprofile und Evaluationsgegenstand (Target of Evaluation, TOE) werden eingeführt.
Teil 2 enthält einen Katalog vordefinierter Funktionalitäten. Die Sicherheitsanforderungen an die Funktionalität sind nach Klassen strukturiert und innerhalb einer Klasse weiter in Familien aufgeteilt. Jede Familie besitzt zumindest eine Komponente, in der die Sicherheitsanforderungen an die konkrete Funktionalität beschrieben werden. Darüber hinaus können eigene Sicherheitsvorgaben als Grundlage für die Evaluierung/Zertifizierung definiert werden.
Teil 3 spezifiziert Kriterien für die Evaluierung von Schutzprofilen und Sicherheitsvorgaben. Die Sicherheitsvorgaben werden vor Beginn der eigentlichen Evaluierung eines TOE separat evaluiert. Auch Schutzprofile können vorevaluiert werden. Die Sicherheitsanforderungen an die Vertrauenswürdigkeit sind wie in Teil 2 des Standards mittels Klassen, Familien und Komponenten strukturiert. Sie werden für jede Komponente in einem festgelegten Aufbau formuliert, der sich aus Anforderungen an den Entwickler, Anforderungen an Inhalt und Form der Prüfnachweise, sowie Anforderungen an den Evaluator zusammensetzt.

Die Nutzung der Common Criteria erfolgt im Wesentlichen durch namhafte Hersteller etwa von Chipkarten und Chipkartenhardware oder von hochsicheren Spezialprodukten. Kleinere Hersteller von preiswerten Sicherheitslösungen scheuen oft die Kosten einer Evaluierung nach den Kriterien. Staatliche Stellen gehen zunehmend dazu über, die CC zur Grundlage für die Akzeptanz sicherer Systeme zu machen. In Deutschland wird die CC vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen und benutzt. Das BSI war auch an der Entwicklung der CC maßgeblich beteiligt. Eines der Ziele des BSI ist, die Anwendung der CC auch für kleine Hersteller attraktiv zu machen. [BSICC], [BITCOM01]

#### *2.2.2.9 BSI-Standards*

BSI-Standards enthalten Empfehlungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Das BSI greift dabei Themenbereiche auf, die von grundsätzlicher Bedeutung für die Informationssicherheit in Behörden oder Unternehmen sind und für die sich national oder international sinnvolle und zweckmäßige Herangehensweisen etabliert haben. Der BSI-Standard teilt sich in vier Standards auf, die im Folgenden kurz beschrieben sind:

##### *(1) BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*

Der vorliegende BSI-Standard definiert allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der anderen ISO-Standards der ISO 2700x-Familie wie beispielsweise ISO 27002. Er bietet eine leicht verständliche und systematische Einführung und Anleitung, unabhängig davon, mit welcher Methode man die Anforderungen umsetzen möchte.
Das BSI stellt den Inhalt dieser ISO-Standards in einem eigenen BSI-Standard dar, um einige Themen ausführlicher zu beschreiben und so eine didaktische Darstellung der Inhalte zu ermöglichen. Zudem ist die Gliederung so gestaltet, dass sie zur IT-Grundschutz-Vorgehensweise kompatibel ist. Durch die einheitlichen Überschriften in beiden Dokumenten ist eine einfache Orientierung möglich. [BSI-ITGS]
Der Standard kann unter [BSI100-1] herunter geladen werden.

### *(2) BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise*

Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Sicherheitsmanagements und der Aufbau von Organisationsstrukturen für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrecht erhalten und verbessert werden kann, wird beantwortet.

IT-Grundschutz-Vorgehensweise interpretiert damit die sehr allgemein gehaltenen Anforderungen der ISO-Standards der 2700x-Reihe und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrundinformationen und Beispielen. Im Zusammenspiel mit den IT-Grundschutz-Katalogen wird in der IT-Grundschutz-Vorgehensweise nicht nur erklärt, was gemacht werden sollte, sondern es werden auch konkrete Hinweise gegeben, wie eine Umsetzung (auch auf technischer Ebene) aussehen kann. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen der oben genannten ISO-Standards nachzukommen. [BSI-ITGS]

Der Standard kann unter [BSI100-2] herunter geladen werden.

### *(3) BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz*

Der vorliegende Standard bietet eine Vorgehensweise, wenn Unternehmen oder Behörden bereits erfolgreich mit den IT-Grundschutz-Maßnahmen arbeiten und möglichst nahtlos eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten.

Hierfür kann es verschiedene Gründe geben:

- Die Sicherheitsanforderungen des Unternehmens gehen teilweise deutlich über das normale Maß hinaus (hoher oder sehr hoher Schutzbedarf).
- Die Institution betreibt wichtige Anwendungen oder Komponenten, die (noch) nicht in den IT-Grundschutz-Katalogen des BSI behandelt werden.
- Die Zielobjekte werden in Einsatzszenarien (Umgebung, Anwendung) betrieben, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Die Vorgehensweise richtet sich sowohl an Anwender der Informationstechnik als auch an Berater und Experten. [BSI-ITGS]
Der Standard kann unter [BSI100-3] herunter geladen werden.

### *(4) BSI-Standard 100-4 Notfallmanagement:*

Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen.
Aufgaben eines Notfallmanagements sind daher, die Ausfallsicherheit zu erhöhen und die Institution auf Notfälle und Krisen adäquat vorzubereiten, damit die wichtigsten Geschäftsprozesse bei Ausfall schnell wieder aufgenommen werden können. Es gilt, Schäden durch Notfälle oder Krisen zu minimieren und die Existenz der Behörde oder des Unternehmens auch bei einem größeren Schadensereignis zu sichern. [BSI-ITGS]
Der Standard kann unter [BSI100-4] herunter geladen werden.

## 2.3 Sicherheitshandbücher

### 2.3.1 BSI IT-Grundschutzhandbuch (IT-Grundschutz-Kataloge)

#### *2.3.1.1 Verfasser*

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der zentrale IT-Sicherheitsdienstleister von Deutschland und ist für IT-Sicherheit in Deutschland verantwortlich. Das BSI gehört zum Geschäftsbereich des Innenministeriums und wurde 1991 gegründet und hat sich zur Aufgabe gemacht, dass Sicherheitsaspekte schon bei der Entwicklung von IT-Systemen und IT-Anwendungen berücksichtigt werden.
Die Arbeitsschwerpunkte des BSI sind:

- Internetsicherheit
- Sensibilisierungskampagne IT-Sicherheit
- sicheres E-Government
- Zertifizierung und Zulassung (incl. CC)
- Kryptographie, Biometrie
- Abhörsicherheit
- Schutz kritischer Infrastrukturen
- nationale / internationale Kooperationen
- **IT-Grundschutz**

[SCHBI08]

#### *2.3.1.2 Aufgabenbereich IT-Grundschutz*

Das BSI stellt das IT-Grundschutzhandbuch als wesentliches Werkzeug zur Erreichung des IT-Grundschutzes zur Verfügung. Das *"IT-Grundschutzhandbuch"* heißt seit der Version 2005 *"IT-Grundschutz-Kataloge"*.
Die IT-Grundschutz-Kataloge beinhalten die Baustein-, Maßnahmen- und Gefährdungskataloge. Eine genaue Beschreibung der Kataloge ist auf der Webseite des BSI zum Thema Grundschutz-Kataloge nachzulesen. Auf eine genauere Beschreibung der Kataloge wird verzichtet, weil sie nicht für diese Masterarbeit verwendet wurden. [BSI-ITGS]

Die Vorgehensweise nach IT-Grundschutz, Ausführungen zum Informationssicherheitsmanagement und zur Risikoanalyse findet man unter den BSI-Standards (Kapitel 2.2.2.9).

#### *2.3.1.3 Grundschutz Tool*

Mit dem *„GSTOOL“* stellt das BSI seit 1998 eine regelmäßig aktualisierte, innovative und ergonomisch handhabbare Software bereit, die den Anwender bei Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten entsprechend dem IT-Grundschutz effizient unterstützt. Die Software ist kostenpflichtig und kostet als Einzelplatzversion bereits ca. € 900. [GSTOOL]

Als Alternative kann auch das kostenlose OpenSource Grundschutz-Tool *„verinice“* verwendet werden. Dies ist ein ISMS-Tool für das Management von Informationssicherheit. Die Software wird unter der Lizenz LGPLv3 zum freien Download als OpenSource-Software kostenfrei bereit gestellt. *„verinice“* läuft auf den Betriebssystemen Windows, Linux und MacOS und hat die Grundschutzkataloge des BSI lizenziert. [VERINICE]

### 2.3.2 Das österreichische Informationssicherheitshandbuch (ÖSHB)

#### *2.3.2.1 Verfasser*

Verfasser des ÖSHB ist A-SIT (Zentrum für sichere Informationstechnologie-Austria) und wurde im Mai 1999 als gemeinnütziger Verein durch das Bundesministerium für Finanzen, der österreichischen Nationalbank und der technischen Universität Graz gegründet. Der Verein, dessen Tätigkeit nicht auf Gewinn ausgerichtet ist, bezweckt die kompetente Zusammenführung und Weiterentwicklung fachlicher Inhalte aus dem Bereich der technischen Informationssicherheit. [ASIT01]

#### *2.3.2.2 Entstehung*

Ausgehend von seiner ersten Version SIHA 1998 („IT-Sicherheitshandbuch für die öffentliche Verwaltung“), die sich am Sicherheitsbedürfnis öffentlicher Einrichtungen orientiert hat, wurde beim *„Österreichischen IT-Sicherheitshandbuch“* dem steigenden Interesse aus der Wirtschaft Rechnung getragen, um in der vorliegenden Version *„Österreichisches Informationssicherheitshandbuch“* vom April 2007 auf die umfassende Bedeutung von Information - unabhängig von ihrer Gestalt – einzugehen.
Es besteht ein Kooperationsübereinkommen zwischen A-SIT und BSI. Das ÖSHB ist eng mit dem IT-Grundschutz des BSI und der ISO/IEC 27001 verknüpft und nimmt Rücksicht auf die österreichischen Gesetze und Normen.

#### *2.3.2.3 Zielsetzung*

Mit dem ÖSHB soll Unterstützung geboten werden, um:

- relevante Sicherheitsziele und -strategien zu ermitteln
- eine organisationsspezifischen Informationssicherheitspolitik zu erstellen
- spezifisch geeignete Sicherheitsmaßnahmen auszuwählen und zu realisieren
- Informationssicherheit im laufenden Betrieb zu gewährleisten
- Kenntnis international üblicher Best-Practices im Bereich der IS zu erlangen.

Generell soll der Prozess des Informationssicherheitsmanagements (ISM) vereinheitlicht werden. Weiters bietet das ÖSHB eine Sammlung von Standardsicherheitsmaßnahmen für den mittleren Schutzbedarf.
Als Zielgruppen gelten die öffentliche Verwaltung, die Privatwirtschaft und mittlere bis größere Organisationen. Laut einem Ministeratsbeschluss im Juli 2007 wird es für die

Anwendung in der öffentlichen Verwaltung zur Sicherung einer gemeinsamen Informationssicherheitspolitik empfohlen. [SCHBI07]

#### 2.3.2.4 Aufbau

Das ÖSHB besteht aus zwei Teilen:

##### *(1) 1.Teil: Informationssicherheitsmanagement*

Der erste Teil beschreibt den grundlegenden Vorgang, Informationssicherheit in einer Behörde, Organisation bzw. einem Unternehmen zu etablieren und bietet eine konkrete Anleitung, den umfassenden und kontinuierlichen Sicherheitsprozess zu entwickeln. Dieser Vorgang wird Informationssicherheitsmanagement Prozess (ISM-Prozess) genannt. Weiterführende Informationen dazu im Kapitel 2.3.2.5.

##### *(2) 2.Teil: Informationssicherheitsmaßnahmen*

Der zweite Teil beschreibt die konkreten Einzelmaßnahmen auf organisatorischer, personeller, infrastruktureller und technischer Ebene, sodass den spezifischen Bedrohungen angemessene Standardsicherheitsmaßnahmen für IT-Systeme und Informationen entgegengesetzt werden können. Dabei wird besonders auf die spezifisch österreichischen Anforderungen, Regelungen und Rahmenbedingungen, aber auch auf die durchgängige Einbeziehung des gesamten Lebenszyklus der jeweiligen Systeme, von der Entwicklung bis zur Beendigung des Betriebs, eingegangen [ASIT02].
Weiterführende Informationen zu diesen Maßnahmen findet man im Kapitel 2.3.2.6.

#### 2.3.2.5 Der Informationssicherheitsmanagement Prozess (ISM-Prozess)

Zentrale Aktivitäten im Rahmen des ISM-Prozesses sind:

- Entwicklung
    - Entwicklung einer organisationsweiten Informationssicherheitspolitik
    - Risikoanalyse
    - Erstellung eines Sicherheitskonzeptes
- Realisierung
    - Umsetzung des Informationssicherheitsplans
- Betrieb
    - Informationssicherheit im laufenden Betrieb

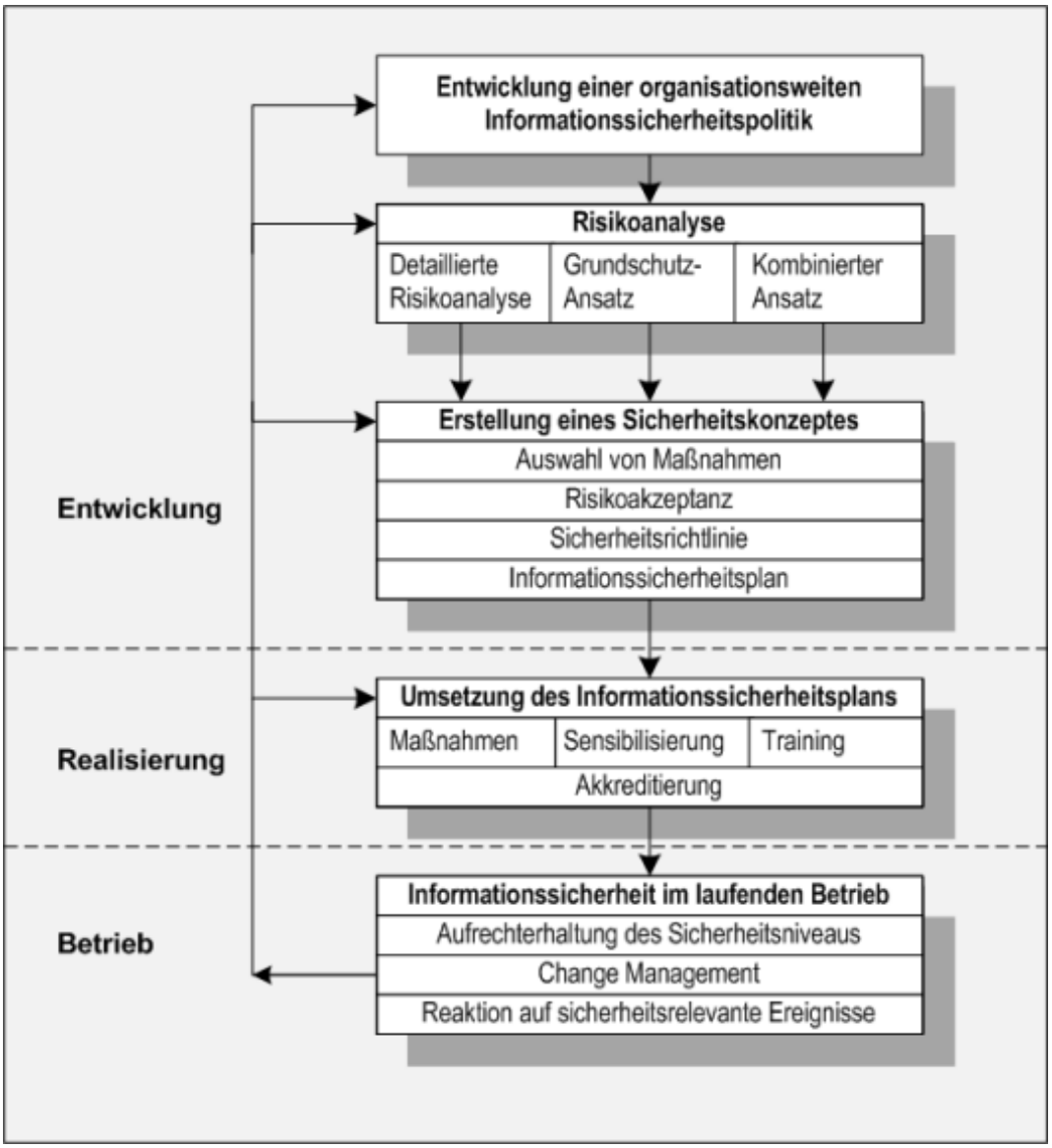



**Abbildung 7: Der Informationssicherheitsmanagementprozess [ASIT03]**

**(vgl. dazu auch Abbildung 5: IRM-Prozess [SCHBI081])**

Es folgt nun ein kurzer Überblick über die Punkte des ISM-Prozesses. Der ISM-Prozess wird auch im ÖSHB beschrieben. [ASIT03, Seite 133ff]

### *(1) Entwicklung einer organisationsweiten Informationssicherheitspolitik*

Die IS-Politik ist ein Grundlagendokument, das die sicherheitsbezogenen Ziele, Strategien, Verantwortlichkeiten und Methoden langfristig verbindlich festlegt. Es ist ein schriftliches Dokument, das als Grundlage des IS-Managements Leitlinien, aber keine Implementierung enthält. Es wird offiziell verabschiedet und in Kraft gesetzt und durch alle Mitarbeiter zur Kenntnis genommen. Die wesentlichen Inhalte sind nachfolgend angeführt. [SCHBI07]

| | |
|---|---|
| *Ziele und Strategien* | *Was soll erreicht werden?*<br>*Wie können die festgelegten Ziele erreicht werden?* |
| *Organisation & Verantwortlichkeiten* | *Definition von Rollen*<br>*Verantwortlichkeiten, Rechte/Pflichten*<br>*Berichtswesen* |
| *RA-Strategie* | *Erkennen und Bewerten von Risiken*<br>*Reduktion des Risikos*<br>*akzeptierbares Restrisiko* |
| *Klassifizierung von Daten* | *Vertraulichkeit*<br>*Datenschutz*<br>*Integrität* |
| *Klassifizierung von Applikationen und Systemen* | *Verfügbarkeit*<br>*Business Continuity Planung* |
| *Nachfolgeaktivitäten* | *Security Compliance Che*<br>*Incident Handling*<br>*Schulung, Awareness* |

**Tabelle 2: Inhalte der Informationssicherheitpolitik**

### *(2) Risikoanalyse*

Zur Begriffsdefinition von Risiko und Risikoanalyse sei auf Kapitel 1.3 verwiesen. Man unterscheidet bei der Risikoanalyse (RA) drei verschiedene Ansätze:

- *Detaillierte RA:* Jedes Risiko wird einzeln identifiziert und bewertet. Es erfolgt nun die Entscheidung, ob eine Behandlung des Risikos mit geeigneten Maßnahmen durchgeführt wird oder das Restrisiko akzeptiert wird. Diese Entscheidung soll vom Management getragen werden.
- *Grundschutzansatz:* Dieser Ansatz geht von einer pauschalierten Gefährungslage aus (siehe Kapitel 1.4). Es werden Sicherheitsmaßnahmen aus vorgegebenen Katalogen umgesetzt, um einen guten Schutz gegen die häufigsten Bedrohungen zu erhalten. Dieser Schutz kann für einzelne Systeme aber nicht ausreichend sein.
- *Kombinierter Ansatz:* Dieser Ansatz vereint beide vorangegangenen Methoden und wird empfohlen: Bei Risiken mit niedrigem bis mittlerem Schutzbedarf wird der Grundschutzansatz angewendet, bei einem hohen Schutzbedarf wird eine detaillierte Risikoanalyse durchgeführt.

[SCHBI07]

### *(3) Erstellung eines Sicherheitskonzeptes*

Das Sicherheitskonzept wird in den folgenden vier Schritten erstellt:

- *Auswahl von Maßnahmen:* Das ÖSHB bietet Sicherheitsmaßnahmen in technischer, organisatorischer, baulicher und personeller Hinsicht. Es können auch Maßnahmen aus dem IT-Grundschutzkatalogen oder der ISO/IEC 27002 verwendet werden.
- *Risikoakzeptanz:* Die verbleibenden Restrisiken werden quantifiziert und bewertet.
- *Sicherheitsrichtlinien:* Sie enthalten Details zu den gewählten Sicherheitsmaßnahmen und begründen deren Auswahl.
- *Informationssicherheitsplan:* Hier werden Umsetzungspläne der Maßnahmen, Verantwortlichkeiten, Zeitpläne, Schulungsmaßnahmen, Prioritäten dokumentiert.

[SCHBI07]

### *(4) Umsetzung des Informationssicherheitsplans*

Bei der Umsetzung ist zu beachten, dass:

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

Gleichzeitig mit der Implementierung der Sicherheitsmaßnahmen sollten auch entsprechende Trainings- und Sensibilisierungsmaßnahmen gesetzt werden, um die optimale Einhaltung und Akzeptanz der Maßnahmen bei den Anwendern/innen zu erreichen.

Als letzter Schritt der Umsetzung des Informationssicherheitsplanes sind die implementierten Maßnahmen in ihrer tatsächlichen Einsatzumgebung auf ihre Auswirkungen zu testen und abzunehmen (Akkreditierung). [SCHBI07]

### *(5) Informationssicherheitspolitik im laufenden Betrieb*

Das nach der Umsetzung des Informationssicherheitsplanes erreichte Sicherheitsniveau lässt sich nur dann aufrechterhalten, wenn

- Wartung und administrativer Support der Sicherheitseinrichtungen gewährleistet sind,
- die realisierten Maßnahmen regelmäßig auf ihre Übereinstimmung mit der Informationssicherheitspolitik geprüft ( Security Compliance Checking ) und
- die IT-Systeme fortlaufend überwacht werden ( Monitoring ).

Change Management hat die Aufgabe, neue Sicherheitsanforderungen infolge von Systemänderungen zu erkennen, angemessen auf alle sicherheitsrelevanten Änderungen zu reagieren und die schriftliche Dokumentation aller Änderungen und Entscheidungsgrundlagen zu gewährleisten. Eine Änderung des IT-System kann eventuell eine neuerliche RA erforderlich machen.
Unter sicherheitsrelevanten Ereignissen sind alle Vorkommnisse zu verstehen, die Sicherheitsprobleme aufdecken oder nach sich ziehen. Auch bei Vorhandensein wirksamer Sicherheitsmaßnahmen und eines hohen Sicherheitsniveaus ist das Auftreten solcher Ereignisse nicht gänzlich zu verhindern. Daher sind alle Mitarbeiter/innen über ihre Verantwortung bei Eintreten sicherheitsrelevanter Ereignisse, die vorgesehenen Meldewege und zu setzenden Aktionen zu unterrichten.
Zur Sicherstellung einer angemessenen Behandlung von sicherheitsrelevanten Ereignissen ist es empfehlenswert, detaillierte Vorgaben in Form eines *“Incident Handling Planes”* (IHP) auszuarbeiten und allen Mitarbeitern/innen bekannt zu machen.
Der IHP legt in schriftlicher Form und verbindlich fest:

- wie auf sicherheitsrelevante Ereignisse zu reagieren ist,
- die Verantwortlichkeiten für die Meldung sicherheitsrelevanter Vorfälle,
- die einzuhaltenden Meldewege,
- die Protokollierung und Dokumentation sicherheitsrelevanter Vorfälle sowie
- die Ausbildung von Personen, die sicherheitsrelevante Vorfälle behandeln bzw. Gegenmaßnahmen treffen müssen.

[SCHBI07]

### *2.3.2.6 Informationssicherheitsmaßnahmen*

Ausgangspunkt für die vorgeschlagenen Maßnahmen sind die IT-Grundschutzkataloge des BSI, wobei aber im ÖSHB keine produktspezifischen Maßnahmen enthalten sind. Das ÖSHB ist zwar eine „abgespeckte" Variante, dafür sind die Maßnahmen aber österreichspezifisch.
Die Anforderungen an den Maßnahmenkatalog sind:

- Kompatibilität mit Vorgehensweise lt. Teil 1
- österreichische Gesetze und Normen
- generische Maßnahmen, keine systemspezifischen Details
- gesamter System-Lifecycle [SCHBI07]

Der zweite Teil ist in sieben Kapitel aufgeteilt und mit Maßnahmen bestückt. Jede Maßnahme trägt eine Referenznummer, je nachdem, zu welchem Kapitel die Maßnahme gehört. Zur besseren Veranschaulichung ein Beispiel aus dem Kapitel 5 „Systemsicherheit" in gekürzter Form (Referenznummer SYS 4.9):

| ***SYS 4.9*** | ***Verhaltensregeln bei Auftreten eines Virus*** |
|---|---|
| ***Relevanz:*** *Umsetzung/Wartung; Anwender/innen;* | |
| *Gibt es Anzeichen, dass ein Rechner von einem Virus befallen ist (z.B. Programmdateien werden länger, unerklärliches Systemverhalten, nicht auffindbare Dateien, veränderte Dateiinhalte, ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde), so sind zur Feststellung des Virus und zur anschließenden Beseitigung folgende Schritte durchzuführen.* | |
| ***Grundregel:*** *Falls möglich, sollten fachkundige Betreuer/innen (Administrator, Bereichs-IT, Sicherheitsverantwortliche/r, Helpdesk) zu Hilfe geholt werden.* | |
| *Falls dies nicht möglich ist, sollten folgende Schritte durchgeführt werden:*<br>• *Beenden der laufenden Programme und Abschalten des Rechners*<br>• *Einlegen einer einwandfreien, schreibgeschützten System-Diskette in Laufwerk A:*<br>• *Booten des Rechners von dieser Diskette*<br>• *Überprüfen des Rechners mit einem aktuellen Virenschutzprogramm*<br>• *Entfernen des Virus abhängig vom jeweiligen Virustyp*<br>• *usw...* | |
| *Sollte der Virus Daten gelöscht oder verändert haben, so muss versucht werden, die Daten aus den Datensicherungen und die Programme aus den Sicherungskopien der Programme zu rekonstruieren.*<br>*→ vgl. BCP 1.6 „Sicherungskopie der eingesetzten Software"* | |

**Tabelle 3: Verhaltensregeln bei Auftreten eines Virus**

Im Folgenden werden die einzelnen Kapitel des ÖSHB mit den Unterkapiteln mit der jeweiligen Referenznummer angeführt, wobei das „x“ immer als Platzhalter für die durchnummerierten Einzelmaßnahmen steht:

*(1) Kapitel 1: Bauliche und infrastrukturelle Maßnahmen (INF):*

- Bauliche Maßnahmen (INF 1.x)
- Brandschutz (INF 2.x)
- Stromversorgung, Maßn. gegen elektr. und elektromagnet. Risiken (INF 3.x)
- Leitungsführung (INF 4.x)
- Geeignete Aufstellung und Aufbewahrung (INF 5.x)
- Weitere Schutzmaßnahmen (INF 6.x)

*(2) Kapitel 2: Personelle Maßnahmen (PER)*

- Regelungen für Mitarbeiter/innen (PER 1.x)
- Regelungen für den Einsatz von Fremdpersonal (PER 2.x)
- Sicherheitssensibilisierung und –schulung (PER 3.x)

*(3) Kapitel 3: IT-Sicherheitsmanagement (SMG)*

- IT-Sicherheitsmanagement (SMG 1.x)

*(4) Kapitel 4: Sicherheit in der Systementwicklung (ENT)*

- Sicherheit im gesamten Lebenszyklus eines IT-Systems (ENT 1.x)
- Dokumentation (ENT 2.x)
- Evaluierung und Zertifizierung (ENT 3.x)

*(5) Kapitel 5: Systemsicherheit (SYS)*

- Berechtigungssysteme, Schlüssel- und Passwortverwaltung (SYS 1.x)
- Betriebsmittel und Datenträger (SYS 2.x)
- Einsatz von Software (SYS 3.x)
- Virenschutz (SYS 4.x)
- Arbeitsplatz-IT-Systeme (SYS 5.x)
- System-/Netzwerkadministration (SYS 6.x)
- Remote Access (SYS 7.x)
- Gesicherte Anbindung an Fremdnetze (Internet-Sicherheit) (SYS 8.x)

- Telearbeit (SYS 9.x)
- Protokollierung (SYS 10.x)
- Kryptographische Maßnahmen (SYS 11.x)

*(6) Kapitel 6: Aufrechterhaltung der Sicherheit im laufenden Betrieb (BET)*

- Wartung (BET 1.x)
- Security Compliance Checking und Monitoring (BET 2.x)
- Change Management (BET 3.x)
- Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling) (BET 4.x)

*(7) Kapitel 7: Disaster Recovery und Business Continuity Planung (BCP)*

- Datensicherung (BCP 1.x)
- Strategie und Planung (BCP 2.x)
- Umsetzung und Test (BCP 3.x)

Als Anhänge sind wichtige Normen, Referenzdokumente, Muster für Verträge, Verpflichtungserklärungen und wichtige Adressen angefügt:

*(8) Anhang A: Wichtige Normen*

- A1 Brandschutz
- A2 Sicherheitstüren und einbruchhemmende Türen
- A3 Wertbehältnisse
- A4 Vernichtung von Akten und Daten
- A5 Informationssicherheit und IT-Sicherheit

*(9) Anhang B: Referenzdokumente*

*(10) Anhang C: Muster für Verträge und Verpflichtungserklärungen*

*(11) Anhang D: Wichtige Adressen*

*(12) Anhang E: Referenzierte IKT-Board Beschlüsse und Gesetze*

Das aktuelle ÖSHB kann unter [ASIT03] herunter geladen werden.

### 2.3.3 IT-Sicherheitsempfehlungen der WKO

#### *2.3.3.1 IT-Sicherheitshandbuch der WKO*

Das ÖSHB ist sehr umfangreich und gibt einen detaillierten Einblick in die Entwicklung einer unternehmensweiten Informationssicherheitspolitik. Für eine Ist-Analyse eines Unternehmens und die rasche Aufdeckung von IT-Sicherheitsmängeln ist das IT-Sicherheitshandbuch der Wirtschaftskammer Österreich (WKO) ein guter Leitfaden. Verfasser dieses Handbuches ist die Bundessparte Information und Consulting (BSIC) in der WKO Die BSIC ist Branchenvertretung für über 100.000 Dienstleistungsunternehmen aus verschiedenen Branchen.
Die Themenbereiche beschreiben einen IT-Grundstandard (Sollzustand), nach dessen Umsetzung ein guter IT-Grundschutz gewährleistet wird, der für die meisten kleinen und mittleren Unternehmen (KMUs) als Basisschutz reicht. Durch Vergleich des Ist-Zustandes mit diesem Standard werden Defizite aufgedeckt, die durch geeignete Maßnahmen aus dem Handbuch bzw. aus dem Maßnahmenkatalog des ÖSHB behoben oder abgemildert werden können. [ITS01]

Im Folgenden werden die behandelten Kapitel durch Schlagworte kurz beschrieben:

*(1) Risikomanagement*

Erhebung und Klassifizierung der Unternehmenswerte, Erhebung der Bedrohungen und Schwachstellen, Planung und Umsetzung von Sicherheitsmaßnahmen

*(2) Datensicherung und Notfallwiederherstellung*

Datensicherung, Datensicherungskonzept und –planung, Geeignete Aufbewahrung der Backup-Datenträger, Schriftliche Aufzeichnungen der Konfigurationsdaten, Datensicherung bei mobilen IT-Systemen (Notebooks, PDAs etc.), Notfallvorsorge und –wiederherstellung, Erhebung der wichtigsten Anwendungen, Notfallvorsorge und eingeschränkter Ersatzbetrieb, Notfallwiederherstellung

*(3) Sicherheit des Internetzugangs*

Firewalls, Personal Firewalls, Wireless LAN (WLAN), Festlegung einer WWW-Sicherheitsstrategie, Gefahren beim WWW-Zugriff, Sicherheit von Internet-Browsern

### *(4) Virenschutz*

Technische Virenschutzmaßnahmen, Vermeidung bzw. Erkennung von Viren durch den Benutzer, Notfallmaßnahmen im Fall von Vireninfektionen

### *(5) Computersicherheit*

Auswahl von Passwörtern, Rechtestruktur auf Arbeitsplatzrechnern, Gefahrenquelle Wechselmedien, Einsatz eines Verschlüsselungsproduktes für Arbeitsplatzsysteme, Regelmäßige Software-Updates, Nutzungsverbot nicht-betrieblicher Software

### *(6) Personelle Maßnahmen*

Regelungen für Mitarbeiter, Verfahren beim Ausscheiden von Mitarbeitern, Regelungen für den Einsatz von Fremdpersonal, Sicherheitssensibilisierung und –schulung, Abwehr von Social Engineering-Angriffen, Clear Desk/Clear Screen-Policy, Entsorgung von Datenträgern und Papierdokumenten, Nutzung und Aufbewahrung mobiler IT-Geräte, Telearbeit

### *(7) Bauliche und infrastrukturelle Maßnahmen*

Baulich-organisatorische Maßnahmen, schützenswerte Gebäudeteile, Zutrittskontrolle, Schlüsselverwaltung, Empfang, geeignete Aufstellung und Aufbewahrung von Servern und anderen besonders schützenswerten IT-Komponenten, Brandschutz, Handfeuerlöscher, Stromversorgung, Maßnahmen gegen elektrische Risiken, angepasste Aufteilung der Stromkreise, lokale unterbrechungsfreie Stromversorgung (USV), Klimatisierung

### *(8) Einhaltung rechtlicher Vorgaben*

Bestimmungen zur Geschäftsführerhaftung (UGB, GesmbH-Gesetz), das österreichische Datenschutzgesetz (DSG 2000), das Verbandsverantwortlichkeitsgesetz (VbVG), Bestimmungen zu Aufbewahrungsfristen (DSG, BAO), Bestimmungen im Arbeitsrecht

Das Handbuch bietet zu jedem Themenbereich Punkte an, die auf jeden Fall umgesetzt werden sollen oder über die man sich Gedanken machen muss. Dabei werden praktische Tipps zur mehr oder weniger einfachen Umsetzung gemacht. Es ist auf jeden Fall ein erster guter Ratgeber in Richtung IT-Grundschutz.

#### 2.3.3.2 IT-Mitarbeiterhandbuch der WKO

Als zusätzliches Service der Bundessparte Information und Consulting der WKO gibt es auch ein IT-Mitarbeiterhandbuch. Der Inhalt des Handbuchs befasst sich mit jenen Bereichen, die Mitarbeiter selbst beeinflussen und steuern können. [ITS02]

Im Folgenden werden die behandelten Kapitel durch Schlagworte kurz beschrieben:

*(1) Sicherer Umgang mit Computern und Informationen*

Sicherer Umgang mit personenbezogenen Daten, Datenträger und Papierdokumente richtig entsorgen, sicherer Umgang mit mobilen IT-Geräten, Wechselmedien richtig verwenden, Clear Desk Policy, Social Engineering

*(2) Passwörter – richtig auswählen und verwalten*

Die richtige Auswahl, der richtige Umgang, Passwort-Manager verwenden

*(3) Sicher unterwegs im World Wide Web*

Vorsichtsmaßnahmen, Verschlüsselte Datenübertragung

*(4) E-Mails und Spam*

Umgang mit unerwünschten Mails, Phishing-Mails, gefälschte Absenderadressen, sparsamer Einsatz der eigenen Mail-Adresse im Internet

*(5) Gefährliche Schadprogramme*

Wie können Sie erkennen, dass Ihr PC infiziert ist? Maßnahmen richtig setzen, Vireninfektion: Was tun?

Dieses Handbuch ist ein wertvolles Hilfsmittel, den Benutzer in Bezug auf IT-Sicherheit zu sensibilisieren und kann als Unterlage für Mitarbeiterschulungen verwendet werden.

# 3 FALLBEISPIEL

Diese Masterarbeit soll ein Leitfaden sein, wie man in einem Elektronikunternehmen Sicherheitsstandards einführen kann. Diese beschriebene Vorgangsweise basiert auf der tatsächlichen Analyse und Umsetzung in einer Elektronikforma. Diese Firma wird aber in dieser Arbeit anonymisiert und die Vorgangsweise verallgemeinert, um keine Rückschlüsse auf die betroffene Firma ziehen zu können (obwohl sie nach dieser Masterarbeit durch einen guten IT-Grundschutz abgesichert ist). Wichtig für diese Masterarbeit ist der praktische Bezug, um die tatsächlich auftretenden Mängel zu finden und die Beseitigung in einem realen Umfeld zu zeigen.

## 3.1 Profil der Firma

Damit man sich einen Überblick über die Rahmenbedingungen und die Größenordnung der Firma machen kann, werden die relevanten Eckdaten der Firma bekannt gegeben:

Die Firma entwickelt kundenspezifische Elektroniklösungen in verschiedenen Bereichen. Dies ist durch eine eigene Produktion und ein 20-köpfiges Entwicklerteam möglich. Lösungen basieren stark auf dem Firmenwissen, d.h. dem Know-How der Mitarbeiter. Viele dieser Lösungen sind durch Patente geschützt. Es ist daher wichtig, diese Informationen für den Wettbewerb zu schützen, jedoch auch immer griffbereit zu haben.

Die Firma ist auf 2 Standorte verteilt und verfügt über 190 Mitarbeiter und Mitarbeiterinnen. Der Hauptstandort wurde durch ein neues Gebäude erweitert und umfasst nun eine „Netzwerklandschaft“ von 500 Netzwerkanschlüssen, 12 Server (Windows, Linux). Die drei Gebäude des Hauptstandortes sind mit Glasfaserkabeln miteinander vernetzt. Es existiert derzeit nur ein ausgestatteter Serverraum. Der Anbau des Firmengebäudes ist abgeschlossen, ein zweiter Serverraum ist bereits eingeplant.

Ein besonderes Merkmal ist das stetige Wachstum der Firma hinsichtlich Mitarbeiterzahl und Umsatz. Im gleichen Maße ist auch die IT-Infrastruktur ständig gewachsen und mit ihr auch die Anzahl an IT-Verantwortlichen. Begann die IT-Betreuung anfangs nebenbei durch einen einzigen Mitarbeiter, so umfasst die derzeitige IT-Abteilung vier vollbeschäftige IT-Mitarbeiter.

## 3.2 Wahl des Vorgehensmodells und der Ziele

Das verwendete Vorgehensmodell hält sich an das Vorgehensmodell der Einführung des IT-Grundschutzes des BSI wie unter Kapitel 2.1 beschrieben. Am Beginn folgt eine IT-Strukturanalyse (Ist-Analyse). Zur Definition der IT-Strukturanalyse sei auf Kapitel 2.1.1 verwiesen. Um eine Übersicht über die bestehende IT-Infrastruktur zu bekommen, werden die bestehenden Serverräume, die Netzwerkkomponenten, die Verkabelung und die PC-Systeme erhoben.

Die Ist-Analyse ist der erste Schritt im Vorgehensmodell, der Übersicht wegen ist diese aber erst im Kapitel 4.2 beschrieben, weil die Ist-Analyse auch für die Erweiterung der bestehenden IT-Infrastruktur notwendig ist und diese im Kapitel 4 durchgeführt wird.

Anhand der erhobenen IT-Infrastruktur können die Basis-Sicherheitschecks gemacht werden. Als Referenzhandbuch für die wichtigsten Sicherheitsthemen wird das IT-Sicherheitshandbuch der WKO verwendet. Das Handbuch setzt sich in übersichtlicher und leicht lesbarer Form mit den wesentlichen Sicherheitsproblemen eines KMUs auseinander und bietet Maßnahmen an, nach deren Umsetzung ein guter IT-Grundschutz im Unternehmen gewährleistet wird. Das Handbuch und die behandelten Themenbereiche sind im Kapitel 2.3.3 beschrieben. Die Erhebung der Informationssicherheitsrisiken erfolgt durch einen Vergleich mit den vorgeschlagenen Maßnahmen aus dem Handbuch und dem erhobenen Ist-Zustand im Unternehmen, woraus die Mängel resultieren. Die ermittelten Mängel werden je nach Schutzbedarf (Kapitel 2.1.2) einer Risikoeinschätzung unterzogen. Es wird dabei das Prinzip der Risikoanalyse nach dem kombinierten Ansatz gewählt (Kapitel 2.3.2.5). Aus dieser Risikoeinschätzung folgt ein notwendiger Maßnahmenkatalog.

Als Grundlage für den entstehenden Maßnahmenkatalog dienen einerseits die Vorschläge aus dem IT-SHB der WKO und die vorgeschlagenen Grundschutzmassnahmen aus dem ÖSHB.

Als abschliessender Punkt steht die Überführung der notwendigen Maßnahmen in den regulären Betrieb. Zur Realisierung der gewählten Maßnahmen ist die Erstellung von IT-Sicherheitsrichtlinien und Notfallplänen wichtig (Kapitel 3.8).

Ziel soll es sein, durch die eingeführten Maßnahmen einen guten Grundschutz im Unternehmen zu etablieren. Eine abschliessende Zertifizierung ist derzeit nicht vorgesehen und auch nicht Teil dieser Masterarbeit.

## 3.3 Ist-Analyse: Erhebung der Sicherheitsmängel

### 3.3.1 Vorgangsweise

Am Beginn jedes Kapitels stehen Fragen, die im IT-Sicherheitshandbuch der WKO im Zusammenhang mit diesem Kapitel gestellt werden. Sie sind Grundlage für die Erhebung. Die Mängel werden in einzelnen Hauptkapiteln aufgelistet.
Sicherheitsmängel zu den einzelnen Kapiteln wurden hauptsächlich durch Einzelgespräche mit dem IT-Leiter der betroffenen Firma und den Mitarbeitern der IT-Abteilung erhoben.
Sicherheitsmängel im Bereich der personellen Sicherheit wurden auch durch Einzelgespräche mit Mitarbeiterinnen und Mitarbeitern der Verwaltung erhoben. Die Mitarbeiter waren durchwegs sehr hilfsbereit und beantworteten alle gestellten Fragen nach bestem Wissen.

Der Text in den Kapiteln ist wie folgt strukturiert:

< *Frage(n) aus dem IT-SHB der WKO* >

< Antwort bzw. Beobachtung >

### 3.3.2 Datensicherung und Notfallwiederherstellung

Datensicherung und Notfallswiederherstellungsmaßnahmen helfen bei der Schadensbegrenzung nach Systemausfällen, dem Verlust einzelner Dateien oder im schlimmsten Fall der Zerstörung der gesamten IT-Infrastruktur.
Die regelmässige und geplante Datensicherung gehört daher zu den wichtigsten IT-Tätigkeiten in einem Unternehmen.

#### *3.3.2.1 Datensicherung*

*„Haben Sie einen präzisen Überblick über die Art Ihrer Daten, deren Speicherort sowie die Art, Häufigkeit und den Ort ihrer Sicherung? Haben Sie eine sinnvolle Auslagerungsstrategie für die Sicherungsdatenträger? Haben Sie ein schriftliches Datensicherungskonzept?“* [ITS01] Seite 21.
Die „eigenen Dateien“ jedes einzelnen Mitarbeiters werden auf den Datenserver umgeleitet. Jede Abteilung (Entwicklung, Produktion, Verwaltung,…) hat ein gemeinsames Arbeitsverzeichnis auf dem Datenserver. Der Emailverkehr wird durch eine Datenbank verwaltet, die am Mailserver gespeichert ist. Fotos und Filme, die für eine größere Benutzergruppe zur Verfügung stehen, sind am Medienserver

gespeichert. Die Dateien des Intranets (Webseite für interne Informationen, Vorstellung neuer Mitarbeiter, Essensbestellung,…) befinden sich am Intranet-Server.
Gesichert werden:

- Verzeichnisse der „eigenen Dateien“
- Abteilungsverzeichnisse
- Email-Datenbank
- Verzeichnisse am Medienserver
- Intranet-Dateien

Die angeführten Daten werden täglich gesichert. Jeden Arbeitstag wird ein eigenes Speicherband verwendet (Mo, Di, Mi, Do, Fr). Die Sicherung am Freitag ist zugleich die Wochensicherung. Die Tagesbänder (Mo – Do) werden 14 Tage aufbewahrt und dann wieder überschrieben. Die Wochensicherung wird 4 Wochen aufbewahrt. Weiters werden Monats- und Jahressicherungen der angeführten Daten gemacht. Die Tagessicherungen werden für 14 Tage im Serverraum, die Wochensicherungen im Haussafe und die Monats- und Jahressicherungen im Banktresor aufbewahrt.
Das Problem ist hier, dass Sicherungsbänder nie im gleichen Raum wie der Server selbst aufbewahrt werden dürfen, da ein Brandfall im Serverraum die Serverfestplatten und auch die Sicherungslaufwerke zerstören würde. Komplettsicherungen können wegen der Menge an zu sichernden Daten meist nur einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wiedereingespielt werden.
Es gibt kein schriftliches Dokument, das den Vorgang der Sicherung und den Umfang der Daten, sowie die personelle Zuständigkeit für die Sicherung regelt. Eine Überprüfung der Sicherungsbänder ist nicht vorgesehen.

#### *3.3.2.2 Notfallwiederherstellung*

*„Haben Sie ein schriftliches Notfallkonzept, das festlegt, wer im Notfall informiert werden muss, wie und innerhalb welcher Zeiträume die Datenwiederherstellung abläuft und wer welche Verantwortung trägt? Wird das Notfallkonzept inklusive der Datenwiederherstellung in regelmäßigen Abständen (mindestens einmal jährlich) einem Test unterzogen?“* [ITS01] Seite 21.

Es gibt keine Notfallrichtlinie, die ein geregeltes Wiederherstellen der Daten dokumentiert. Eine Rücksicherung wird nur fallweise (halbjährlich) getestet. Das Haltbarkeitsdatum der Bänder wird mit 30 Jahren angenommen. Ein Ausfall eines

Bandlaufwerkes und dessen Folgen werden nicht in Betracht gezogen. Eine eventuelle Kompatibilität der Dateien auf den Sicherungsbändern wird nicht abgesichert, d.h. es wird nicht bedacht, ob ein Dateiformat nach 10 Jahren noch gelesen werden kann, bzw. es noch Programme gibt, die das gespeicherte Format richtig interpretieren.

### 3.3.3 Computer- und Datensicherheit

#### *3.3.3.1 Firewalls*

*„Haben Sie ein fachmännisch installiertes und laufend gewartetes Firewallsystem im Einsatz, dessen Protokolle (Logfiles) regelmäßig überprüft und ausgewertet werden?“* [ITS01] Seite 31.

Als Firewall wird eine zentrale Checkpoint-Firewall von SecureGuard mit Fremdwartung verwendet. Im Fehlerfall ist eine Reaktionszeit von 4h vereinbart. Eine Contentwall von Ikarus scannt eingehende E-Mails und filtert als gefährliche geltende Dateianhänge aus dem E-Mails heraus. Diese Vorgangsweise wird *„Blacklist-Filterung“* genannt, bei der in einer „schwarzen Liste“ die als gefährlich eingestuften E-Mail-Anhänge (exe, bat, vbs,…) eingetragen sind und von der Contentwall ausgefiltert werden. Ausgehende E-Mails werden nicht in dieser Form überprüft. Der interne und ausgehende Email-Verkehr ist frei (Größenbeschränkung 5,5MB).

Eine Personal-Firewall ist auf Laptops installiert, wenn diese sich nicht im Firmennetz befinden. Die Logfiles der Firewall werden fallweise (wöchentlich) überprüft.

#### *3.3.3.2 Virenschutz*

*„Haben Sie auf allen Ihren Computern Virenschutzprogramme und werden diese laufend aktualisiert? Werden Ihre Mitarbeiter regelmäßig über die Gefahren von Viren und deren Vermeidung geschult? Haben Sie ein schriftliches Notfallkonzept, das bei akutem Virenbefall eine Ansprechperson, ein Programm an Erstmaßnahmen sowie Wiederherstellungsstrategien unter Berücksichtigung Ihres Datensicherungskonzepts vorsieht?“* [ITS01] Seite 37.

Als Virenscanner wird ein zentraler Virenschutz der Firma Kaspersky mit automatischen Updates der Clients verwendet. Das Virenprotokoll wird wöchentlich manuell geprüft. Ein Virenbefall wird sofort gemeldet, es gibt aber keine Richtlinie und Notfallmaßnahmen bei einem Virenbefall. Es fehlt auch eine geeignete Schulung der Mitarbeiter, wie bei einem Virenbefall vorgegangen werden muss und wie Viren generell vermieden werden können.

#### 3.3.3.3 Wireless LAN (WLAN)

*„Wenn Sie ein Wireless Lan (WLAN) betreiben, sind Sie sicher, dass es fachmännisch installiert wurde und dass es mittels WPA oder WPA2 verschlüsselt ist?“* [ITS01] Seite 31.

Es gibt zwei WLAN-Access-Points in der Produktion, die in das Firmennetz integriert sind. Sie werden für den Betrieb von Handscannern benötigt. Die Verschlüsselung ist mittels WPA realisiert, da der Handscanner keine andere Verschlüsselungstechnik unterstützt.

#### 3.3.3.4 Auswahl der Passwörter

*„Wurden Ihre Mitarbeiter über die fachgerechte Auswahl und den richtigen Umgang mit Passwörtern geschult?“* [ITS01] Seite 43.

Passwörter werden beim ersten Mal durch die IT-Abteilung vergeben. Passwort-Änderungen werden halbjährlich oder im Anlassfall durchgeführt und von der IT-Abteilung angeregt. Passwörter werden durch die IT-Abteilung verifiziert (durch mündliche oder schriftliche Bekanntgabe) und in einer passwortgeschützten Datei im Excel-Format am Server gespeichert. Passwortänderungen sind nur über die IT-Abteilung möglich. Das Passwort für die Excel-Datei ist nur dem IT-Leiter bekannt, dieses Passwort ist auch nirgendwo dokumentiert.

Das Domänenadministrator-Passwort ist allen IT-Mitarbeitern bekannt.

Die Passwortliste wird benutzt, um sich mit dem Login eines Benutzers anzumelden. Dies wird als nötig angesehen, um einen PC auf die Bedürfnisse eines Benutzers abstimmen zu können (z.B. Microsoft Outlook Postfach einrichten, Eigene Dateien auf den Server umleiten, Email-Signaturen einrichten, Telefon-Software,…).

#### 3.3.3.5 Rechtestruktur auf Arbeitsplatzrechnern

*„Haben Sie ein schriftliches Nutzungskonzeptverbot für nicht-betriebliche Software und ist in Ihrem Unternehmen durch ein angemessenes Berechtigungssystem sichergestellt, dass die Installation von Programmen nur von fachkundigen Administratoren vorgenommen werden kann?“* [ITS01] Seite 43.

Auf den Arbeitsplatzrechnern haben alle Benutzer Hauptbenutzerrechte. Eine Programminstallation durch den Benutzer ist nicht vorgesehen. Eine Ausnahme bilden die Mitarbeiter der Entwicklungsabteilung, die über Administrationsrechte verfügen. Dies ist erforderlich, da sie selbst regelmäßig Programmupdates (Compiler,…) durchführen müssen. Diese Updates sind mit der IT-Abteilung abgesprochen.

Die „eigenen Dateien“ sind auf ein Serverlaufwerk umgeleitet und werden dadurch bei der Sicherung berücksichtigt. Es dürfen keine firmenrelevanten Daten lokal auf dem Arbeitsplatzrechner gespeichert werden, da sie sonst nicht gesichert werden. Diese Vorgabe wird aber nicht überprüft und verhindert.

#### *3.3.3.6 Wechselmedien*

*„Ist die Benutzung von Wechselmedien wie z.B. USB-Sticks in Ihrem Unternehmen reguliert und wurden die Vorschriften den Mitarbeitern zur Kenntnis gebracht?“* [ITS01] Seite 43.

Für den Einsatz von Wechselmedien gibt es keine schriftliche Vereinbarung, es ist aber die Verwendung von USB-Sticks laut Firmenphilosophie untersagt. Die USB-Ports der Laptops und PCs sind nicht gesperrt, es fehlt auch ein Logging über benutzte Wechselmedien. Es fehlt eine schriftliche IT-Richtlinie zu diesem Thema.

#### *3.3.3.7 Verschlüsselung*

*„Werden Daten auf Ihren Firmennotebooks verschlüsselt und werden die Verschlüsselungspasswörter an zentraler, gesicherter Stelle hinterlegt?“* [ITS01] Seite 43.

Firmennotebooks werden derzeit nicht verschlüsselt, obwohl Firmenlaptops mit relevanten Firmendaten auch im Ausland „unterwegs“ sind. Es wird generell keine Verschlüsselung im Unternehmen eingesetzt.

### 3.3.4 Datenaustausch und Benutzerverwaltung

#### *3.3.4.1 Active Directory Struktur (AD-Struktur)*

Die Verwaltung der Benutzer und der Gruppenzugehörigkeit erfolgt durch zwei Domänencontroller mit installiertem Active Directory.

Durch das starke Wachstum der Mitglieder und der Umstrukturierung der Firma sind die Gruppenzuteilungen teilweise redundant. Gruppenzuteilungen überschneiden sich, Rechte werden immer neu vergeben, aber selten wieder genommen. Die Benutzer sind im AD nur in der „BuiltIn User Group“, keine Organisationseinheiten sind angelegt, die Übersichtlichkeit leidet dadurch stark.

Der Domaincontroller ist auch Exchange-Mailserver.

#### *3.3.4.2 Berechtigungen auf Serverlaufwerke*

Auf dem Datenserver sind verschiedene Verzeichnisse freigegeben. Jeder Mitarbeiter verfügt über ein exklusives Verzeichnis für die „eigenen Dateien“. Die Mitarbeiter einer Abteilung haben Zugriff auf ein Abteilungsverzeichnis (Entwicklung,

Produktion, Verwaltung,…). Diese Verzeichnisse werden durch ein Anmeldeskript automatisch einem Laufwerksbuchstaben zugewiesen. Man spricht von sog. Serverlaufwerken. Zusätzlich können von der IT-Abteilung Verzeichnisse für einzelne Projektgruppen angelegt werden.

Der Zugriff auf diese Verzeichnisse und darin gespeicherte Dateien ist durch NTFS-Berechtigungen und das Active-Directory-Gruppensystem, wie auf einem Datenserver üblich, festgelegt.

Eine Besonderheit ist die ungewollte Tatsache, dass die Verzeichnisrechte durch Benutzer so manipuliert werden können, dass der Benutzer Vollzugriff auf das Verzeichnis erhalten kann:

Diese Eigenheit soll nun durch Screenshots veranschaulicht werden. Zuerst legen wir unseren Blick auf das Hauptverzeichnis \\daten01\verwaltung\pachinger. Die Sicherheitseinstellungen gewähren uns Änderungsrechte, eine Änderung auf diesem Ordner ist aber aufgrund der Vererbung nicht möglich.

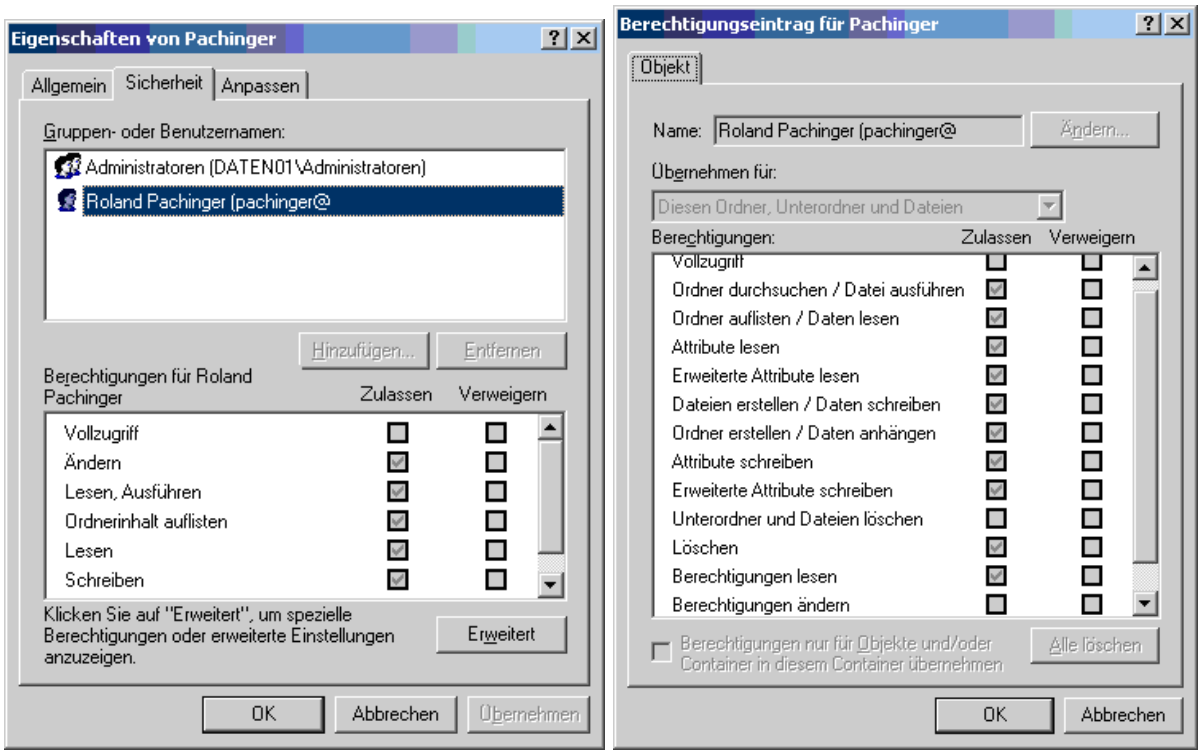



**Abbildung 8: Berechtigung auf Serverlaufwerke – Eigenschaften von „Pachinger“**

Erstellt man nun in diesem Benutzerordner ein Verzeichnis (hier „Geheim“), wird der aktuelle Benutzer als Besitzer für dieses Verzeichnis eingetragen!

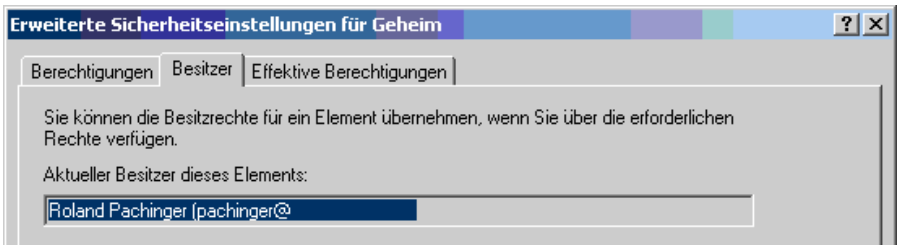



**Abbildung 9: Berechtigung auf Serverlaufwerke – Besitzübernahme**

Nun ist es aber möglich, sich Vollzugriff auf dieses Verzeichnis zu geben!

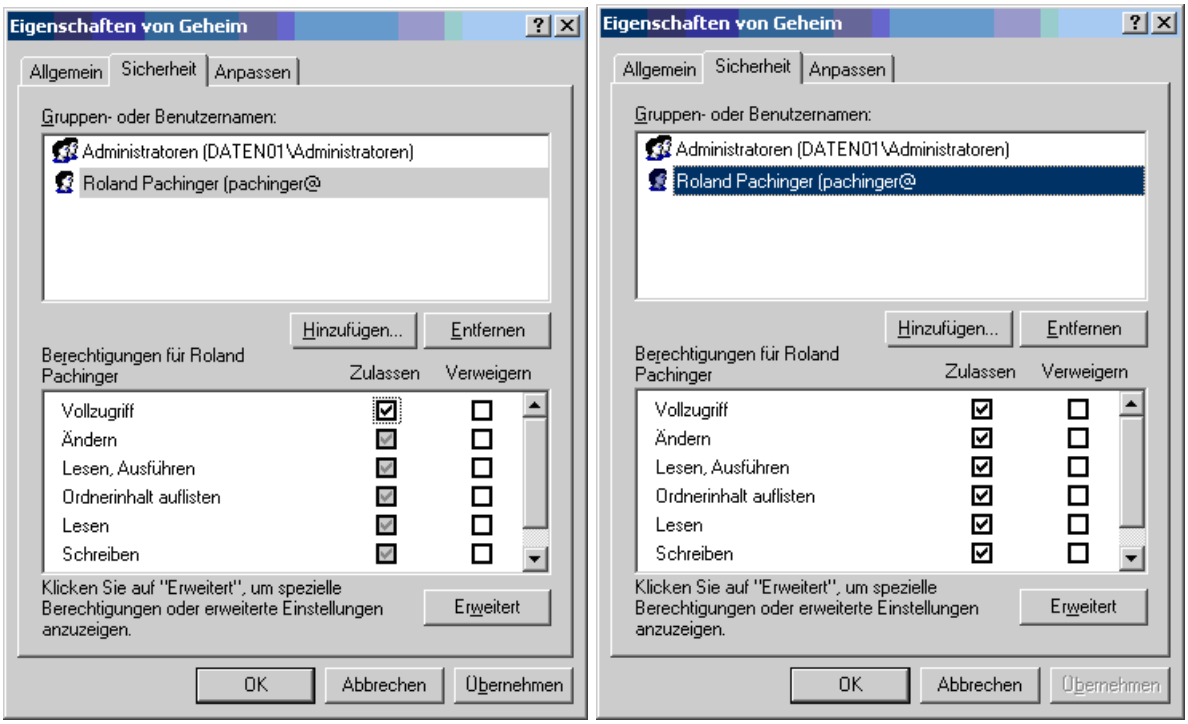



**Abbildung 10: Berechtigung auf Serverlaufwerke – Eigenschaften von „Geheim“**

Man kann sogar einen anderen Domänenbenutzer hinzufügen und diesem Vollzugriff geben. Das Verzeichnis selbst kann aber nicht freigegeben werden. Ein Zugriff ist aber über den UNC-Pfad \\Daten01\Verwaltung\Pachinger\Geheim möglich, obwohl dieser Benutzer keinen Zugriff auf den Pfad \\Daten01\Verwaltung\Pachinger hat.

Dieser Benutzer kann nun ein Verzeichnis erstellen und ist für dieses Verzeichnis wiederum der Besitzer. Er hat damit uneingeschränkten Zugriff auf dieses Verzeichnis.

Durch diese Vorgangsweise ist ein nicht kontrollierbarer Datenaustausch zwischen dem Besitzer des Verzeichnisses (Pachinger) und dem neu hinzugefügten Benutzer möglich.

Ein zusätzliches Problem, das dadurch entsteht, ist das *„Confinement Problem“*.
Es wird mit nachfolgender Darstellung erläutert:

- User1 habe Leserechte auf Datei_A und Schreibrechte auf Datei_B
- User2 habe nur Leserechte auf Datei_B
- User1 könnte Auszüge von Datei_A auf Datei_B schreiben und diese Daten somit User2 zugänglich machen

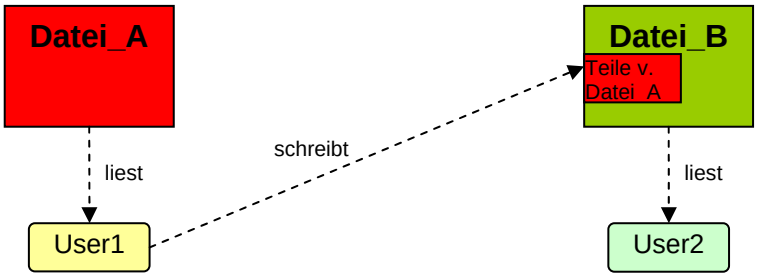



**Abbildung 11: Confinement Problem [ECKE08]**

Dieses Problem besteht bei reinen Serverlaufwerken, wenn die Berechtigungen wie oben dargestellt sind.

#### *3.3.4.3 Netztransfer*

Auf jeder Arbeitsstation im Firmennetzwerk gibt es ein Verzeichnis mit dem Namen „Netztransfer“. Dieses Verzeichnis ist für jeden Benutzer freigegeben und erlaubt Änderungsrechte, d.h. es kann jeder Benutzer im Firmennetzwerk auf jeder Arbeitsstation in dieses Verzeichnis Daten schreiben und Daten daraus lesen. Dieses Verzeichnis ist historisch gewachsen und daher noch immer in Verwendung. Wird z.B. ein E-Mail-Anhang versehentlich von der Firewall gesperrt, weil das Dateiformat nicht der erlaubten Spezifikation entspricht, kontaktiert der betroffene Empfänger des E-Mails die IT-Abteilung. Ein IT-Mitarbeiter löst darauf den benötigten Anhang vom E-Mail und kopiert diesen auf das Netztransfer-Verzeichnis des jeweiligen Mitarbeiters. Der Mitarbeiter wird dann telefonisch von der Transaktion verständigt.

### 3.3.5 Personelle Mängel

#### *3.3.5.1 Regelungen für Mitarbeiter*

*„Haben alle Mitarbeiter PC-Benutzungsregeln und eine Verpflichtungserklärung auf das Datengeheimnis unterzeichnet? Werden neue Mitarbeiter mit den Sicherheitsbestimmungen im Unternehmen vertraut gemacht?“* [ITS01] Seite 51.

Bei einem Neueintritt in die Firma muss man eine Geheimhaltungsvereinbarung unterschreiben. Darin sind die wesentlichen Punkte der Geheimhaltung verankert.

Es gibt jedoch kein schriftliches Regelwerk (Richtlinie) für Mitarbeiter, worin der Umgang mit PCs, Wechseldatenträger, E-Mail dokumentiert ist. Bei einer Neueinstellung werden die Mitarbeiter durch die Abteilung geführt, in der sie arbeiten (Verwaltung, Produktion, Entwicklung), eine Einführung in die Sicherheitsbestimmungen erfolgt nur punktuell und mündlich.

#### *3.3.5.2 Regelungen für Fremdpersonal*

*„Wurden Regeln über die Verpflichtungen von Fremdpersonal und den Umgang der Mitarbeiter mit diesen Personen festgelegt und kommuniziert?“* [ITS01] Seite 51.

Für Fremdpersonal gibt es keine dokumentierten Richtlinien. Es gibt auch keine Richtlinie, die den Umgang mit diesen Personen regelt.

#### *3.3.5.3 Ausscheiden von Mitarbeitern*

*„Ist ein dokumentiertes Verfahren beim Ausscheiden von Mitarbeitern hinsichtlich sicherheitsrelevanter Maßnahmen, wie etwa dem Löschen von Zugangsberechtigungen und Zugriffsrechten vorgesehen?“* [ITS01] Seite 51.

Für das Ausscheiden von Mitarbeitern gibt es keine dokumentierten Richtlinien. Es gibt auch keine Richtlinie, die den Umgang mit diesen Personen regelt.

#### *3.3.5.4 Social Engineering*

*„Werden Mitarbeiter über Social-Engineering Attacken und die Sensibilität der von Ihnen bearbeiteten Daten geschult? Gibt es eine schriftliche Festlegung der vertraulich zu behandelnden Datenarten und kennt jeder Mitarbeiter eine Ansprechperson für Rückfragen im Zweifelsfall?“* [ITS01] Seite 51.

Das Thema „Social Engineering“ ist Teil der Regelungen für Mitarbeiter, wird aber in einem eigenen Kapitel angeführt, damit es auch bewertet werden kann.

Als Ansprechpartner gilt immer der jeweilige Vorgesetzte. Für alle IT-Belange ist die IT-Abteilung zuständig. Es fehlt aber an einer konkreten Schulung der Mitarbeiter. In einem konkreten Fall konnte sogar durch eine gezielte Anfrage an einen Mitarbeiter

an einem PC-Arbeitsplatz das Passwort erfragt werden. Dies gelang auch deshalb, weil der IT-Verantwortliche über eine Passwortdatei aller Mitarbeiter verfügt und daher eine Weitergabe des Passwortes an IT-Mitarbeiter nicht weiter ungewöhnlich ist.

### 3.3.6 Bauliche und infrastrukturelle Mängel

#### *3.3.6.1 Schützenswerte Gebäudeteile*

*„Haben Sie beim Aufstellen Ihres Servers oder für Ihre Datenträgerarchive bauliche Risiken (z.B. Wassereinbruch, Brandgefahr, Diebstahlgefahr) berücksichtigt? Ist der Zutritt zu kritischen IT-Komponenten gesichert und geregelt?“* [ITS01] Seite 59.

Die Gebäudeteile bestehen bereits, daher ist eine Reaktion in dieser Richtung nicht einfach möglich. Der erste Serverraum ist im 1.Stock, der zweite Serverraum wird gerade im 2.Stock des neuen Gebäudetraktes fertiggestellt. Die beiden Serverräume sind zentral angeordnet, sodass ein Wassereinbruch sowie schädliche Umwelteinflüsse weitgehend vermieden werden können.

Serverräume und Räume mit Netzwerkkomponenten sind zwar extra versperrt, ein Schlüsselplan fehlt aber.

#### *3.3.6.2 Zutrittskontrolle und Schlüsselverwaltung*

*„Haben Sie ein schriftliches Zutrittskontrollkonzept und eine entsprechende Schlüsselverwaltung? Wenn Sie einen Empfangsdienst haben, wurden die dort tätigen Mitarbeiter über ihre Kontrollfunktion geschult und gibt es definierte Verfahren zum Umgang mit Besuchern?“* [ITS01] Seite 59.

Das Firmengebäude am Hauptsitz verfügt über einen Haupteingang mit Empfang und 3 Nebeneingangstüren. Alle, bis auf eine Tür, können zusätzlich mit einem Schlüsselschalter geöffnet werden. Eine Nebeneingangstür ist mit einem Transponder versehen. Jeder Mitarbeiter hat einen Transponder, die Mitarbeiter der Verwaltung und der Entwicklung, sowie einige Produktionsmitarbeiter haben auch einen Schlüssel. Es gibt verschiedene Schlüsselsysteme (Produktion, Entwicklung, Verwaltung), Firmenleitung, Putzfrau und Hausmeister haben einen Zentralschlüssel. Der Hausmeister schließt zwischen 20 und 22Uhr alle Türen ab. Serverräume haben einen extra Schlüssel, den nur IT-Mitarbeiter und „???“ besitzen. Die drei Fragezeichen stehen für „unbekannt“, denn es konnte kurzfristig nicht geklärt werden, wer noch Zugang zu den Serverräumen hat, da eben ein Schlüsselplan fehlt.

In Folge der starken Bautätigkeit ist ein Zutritt zum Gebäude einfach durch den Zubau möglich. Es sind keine Kameras am Gebäude montiert, der Zugang ist tagsüber problemlos möglich. Eine elektrische Schiebetür im Untergeschoß, die durch einen Transponder zu öffnen ist, kann auch durch leichten Druck auf die Türblätter geöffnet werden.
Beim selbstbewussten Eintreten mit einem freundlichen Gruß kommt man ohne weitere Formalitäten am Empfang vorbei. Eine Richtlinie und Schulung der Mitarbeiter am Empfang fehlt, auch der Umgang mit Firmenfremden ist nicht schriftlich geregelt.

#### *3.3.6.3 Brandschutz*

*„Haben Sie angemessene Brandschutzmaßnahmen wie etwa Brandmelder und Handfeuerlöscher für systemkritische Räume vorgesehen? Gibt es ein Verbot des Hantierens mit leicht brennbaren Materialien in kritischen Räumen und wird es auch kontrolliert?“* [ITS01] Seite 59.

Der Brandschutz und die notwendigen Maßnahmen werden durch einen Brandschutzbeauftragten verwaltet. Dies ist eine Einzelperson, die regelmässig die notwendigen Wartungsarbeiten durchführt. Im Brandfall wird durch eine Meldeanlage die Feuerwehr verständigt. Brandabschnitte sind nur sehr eingeschränkt vorhanden (Produktion-Entwicklung). Es gibt ein generelles Rauchverbot und ein Raucherkammerl im Keller.

#### *3.3.6.4 Stromversorgung*

*„Ist die Stromversorgung Ihrer IT-Komponenten angemessen und betreiben Sie gegebenenfalls eine Anlage zur unterbrechungsfreien Stromversorgung?“* [ITS01] Seite 59.

Die Stromversorgung der Serverräume wird durch zwei unabhängige Stromkreise gewährleistet. Es existiert eine Notstromversorgung als lokale unterbrechungsfreie Stromversorgung (USV) für Server und die Switches im alten Serverraum, der derzeit auch alle Server beinhaltet (der 2. Serverraum ist in Errichtung).
Fällt die Stromversorgung aus, werden nach 8 Minuten die Server herunter gefahren, wobei die beiden Domaincontroller nach 10 Minuten herunter gefahren werden. Der automatische Neustart der Server nach einem Stromausfall ist nicht aktiv, da die Reihenfolge der Server wichtig ist (Domaincontroller zuerst). Derzeit wird der Neustart manuell initiiert. Weiters ist aufgefallen, dass während der Bautätigkeit mehrmals der Strom ausgefallen ist. Die USV musste nachher 1 Stunde wieder aufgeladen werden, bevor die Server wieder gestartet werden konnten. Es wäre

sonst in dieser Zeit keine USV-Versorgung möglich gewesen. Eine echte Notstromversorgung, um über eine längere Zeit den Betrieb aufrecht zu erhalten, ist nicht vorgesehen.

#### *3.3.6.5 Klimatechnik*

*„Ist die ausreichende Klimatisierung des Serverraums sichergestellt?“* [ITS01] Seite 59.

Die Temperaturregelung der beiden Serverräume wird durch jeweils eine zweistufige Klimaanlage, die von zwei Stromkreisen versorgt wird, gewährleistet. Die Klimaanlage funktioniert vollautomatisch, ist aber bei einem Stromausfall nicht aktiv. Ein Ausfall der Klimaanlage wird nicht automatisch gemeldet.

## 3.4 Bewertung und Risikoeinschätzung der aufgezeigten Sicherheitsmängel

### 3.4.1 Vorgangsweise

In den folgenden Kapiteln werden die aufgezeigten Sicherheitsmängel bewertet und das Sicherheitsrisiko bzw. der Handlungsbedarf eingeschätzt. Die Kapitel sind gleich wie im vorigen Kapitel 3.3, *"Ist-Analyse: Erhebung der Sicherheitsmängel"* angeordnet, um die Kapitel einfacher vergleichbar zu machen und das Dokument übersichtlich zu halten.

Die Beurteilung[2] von Risiken wird hinsichtlich der Eintrittswahrscheinlichkeit p und der möglichen Schadensausprägung S des Risikos durchgeführt (siehe dazu Kapitel 1.3 und Kapitel 2.2.2.6). Für die Parameter werden qualitative Bewertungen vorgenommen. Daraus ergibt sich ein möglicher Risikowert. Dieser Risikowert wird hier mit *„Handlungsbedarf"* betitelt. Ein hoher Risikowert hat einen hohen Handlungsbedarf zur Folge, den Mangel, aus dem das Risiko resultiert, zu beseitigen. Analog dazu hat ein geringer Risikowert auch einen geringen Handlungsbedarf zur Folge.

Der Zusammenhang dieser Parameter wird in folgender Tabelle[2] dargestellt:

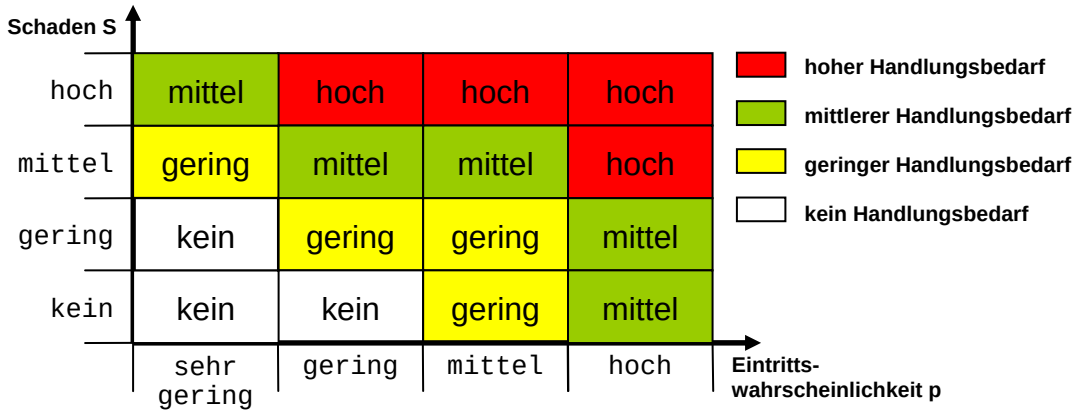



**Abbildung 12: Eintrittswahrscheinlichkeit – Schaden – Handlungsbedarf**

Nach jedem Kapitel wird eine Bewertung nach folgendem Schema durchgeführt:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | … |
| Schaden | = | … |
| Handlungsbedarf | = | … |

[2] *Hinweis:* Die Beurteilung ist „exemplarisch" zu verstehen und bedarf bei der Einschätzung einer endgültigen Beurteilung seitens der Firmenleitung und der IT-Verantwortlichen.

Entsprechend einer Vorgabe des Managements soll das Kapitel *„Bewertung und Risikoeinschätzung der aufgezeigten Sicherheitsmängel“* abgeschlossen lesbar sein. Daher werden die in der Anamnese (Kapitel 3.3) angeführten Mängel am Beginn jedes Kapitels verkürzt wiederholt.

### 3.4.2 Datensicherung und Notfallwiederherstellung

#### *3.4.2.1 Datensicherung*

- Keine schriftliche Datensicherungsrichtlinie
- Nur eine umfangreiche Komplettsicherung täglich
- Sicherungsbänder werden teilweise im Serverraum aufbewahrt

Durch die angeführten Mängel kann es zu Datenverlust kommen. Die Folgen von Datenverlust sind vielfältig und können sogar zu einem Systemausfall führen (Verlust der Lagerhaltungsdaten, Kundendatenbank, Programmierdaten,…). Es wird aber eine (nicht dokumentierte) Datensicherung durchgeführt.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

#### *3.4.2.2 Notfallwiederherstellung*

- Keine Notfallrichtlinie für ein geregeltes Wiederherstellen
- Keine Notfallrichtlinie bei Ausfall eines Bandlaufwerkes
- Keine geplanten Rücksicherungen
- Keine laufende Kontrolle der Sicherungsbänder
- Bänderlebensdauer als zu lang angenommen (30 Jahre)

Durch die fehlende Dokumentation ist im Anlassfall eine schnelle, routinierte Rückspielung nicht zu garantieren. Die angeführten Mängel können zu Datenverlust führen, was schon im vorangegangenen Kapitel 3.4.2.1 behandelt wurde.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

### 3.4.3 Computer- und Datensicherheit

#### *3.4.3.1 Firewalls*

- Keine Richtlinie und Notfallmaßnahmen bei einem Ausfall oder Angriff
- Keine ausgehende E-Mail Filterung durch die Firewall
- Keine regelmässige Überprüfung der Logfiles

Bei der Vergabe der Firewallverwaltung an eine Fremdfirma muss man dieser Firma vertrauen können, da eine mangelhaft gewartete oder verwaltete Firewall den Zugang zu Firmendaten über das Internet möglich macht. Ausgehende E-Mails könnten Schadsoftware enthalten und so zu einem Kunden gelangen, was zumindest zu einem Imageverlust führt. Logfiles enthalten wichtige Informationen zu Angriffen auf die Firewall. Eine regelmässige Überprüfung ist notwendig.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | mittel |
| Handlungsbedarf | = | **mittel** |

#### *3.4.3.2 Virenschutz*

- Keine Richtlinie und Notfallmaßnahmen bei einem Virenbefall
- Keine regelmässige Überprüfung der Logfiles
- Fehlende Schulung der Mitarbeiter in Bezug auf Viren

Schadsoftware kann erheblichen Schaden verursachen, wenn sie sich für längere Zeit unerkannt im Firmennetz befindet, da sie dann auch durch die Datensicherung mitgesichert wird und bei einer späteren Wiederherstellung wieder zurückgesichert wird. Der fehlende ausgehende Virenschutz ist zwar weniger für die interne Sicherheit des Unternehmens wichtig, wird aber Schadsoftware per E-Mail versendet, so kann dies bei einem Kunden oder Lieferanten zu einem Schaden führen und dies hat weiters einen Vertrauensverlust zur Folge. Logfiles enthalten Informationen zu einem Virenbefall. Eine regelmässige Überprüfung ist notwendig.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | mittel |
| Schaden | = | mittel |
| Handlungsbedarf | = | **mittel** |

### *3.4.3.3 Wireless LAN (WLAN)*

- Keine ausreichende Verschlüsselung der drahtlosen Kommunikation

Über Wireless LAN kann man auch von ausserhalb des Firmengebäudes Zugang zum Firmennetzwerk bekommen, falls der Accesspoint nicht ausreichend gesichert ist. Die Verschlüsselung der Accesspoints mittels WPA, wie im vorliegenden Fall, ist kein ausreichender Schutz gegen einen Angriff.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | mittel |
| Handlungsbedarf | = | **mittel** |

### *3.4.3.4 Auswahl der Passwörter*

- Speicherung der Benutzerpasswörter in einer Liste
- Keine direkte Änderungsmöglichkeit durch den Benutzer

Erfolgt die Authentisierung in einem IT-System über Passwörter, so ist die Sicherheit der Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gewählt und verwendet wird. Die vorliegende Vorgangsweise der Passwortvergabe, –änderung und –speicherung durch die IT-Abteilung ist zu hinterfragen. Durch die Speicherung der Passwörter in einer passwortgeschützten Datei im Excel-Format kann es zu mehreren Sicherheitsproblemen kommen:

- Die Datei könnte von einem IT-Mitarbeiter ausgedruckt werden, findet nun jemand dieses Dokument, wären ihm alle Passwörter bekannt.
- IT-Mitarbeiter können durch Anmeldung mit einem Benutzeraccount E-Mails im Namen eines anderen Benutzers verfassen. Abgesendete E-Mails können daher theoretisch nicht mehr genau einem Benutzer zugeordnet werden.
- Der Verwaltungsaufwand für die beschriebene Vorgangsweise (siehe 3.3.3.4) ist hoch, sodass z.B. die regelmässige Änderung der Passwörter in grossen Abständen erfolgen wird, was wiederum die Sicherheit beeinträchtigt.
- Eine rasche Passwortänderung durch den Benutzer ist nicht einfach machbar.

Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | mittel |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

### *3.4.3.5 Rechtestruktur auf Arbeitsplatzrechnern*

- Administratorrechte für alle Mitarbeiter der Entwicklungsabteilung
- Lokale Speicherung von Daten möglich

Um sicherzustellen, dass keine Programme mit unerwünschten Auswirkungen eingebracht werden und das System nicht über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird, muss das Einspielen nicht-freigegebener Software in Produktionssysteme bzw. ihre Nutzung verboten und - soweit technisch möglich - verhindert werden. Das Arbeiten mit Administratorrechten auf einer Arbeitsstation birgt folgende Risiken:

- Es kann uneingeschränkt Software installiert und deinstalliert werden.
- Schadsoftware, die versteckt arbeitet, arbeitet dann mit Administratorrechten.

Werden firmenrelevante Daten lokal auf dem Arbeitsplatzrechner gespeichert, werden diese Daten nicht bei der regelmässigen Datensicherung berücksichtigt.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | mittel |
| Schaden | = | mittel |
| Handlungsbedarf | = | **mittel** |

### *3.4.3.6 Wechselmedien*

- Keine schriftliche Vereinbarung für den Einsatz von Wechselmedien

Wechselmedien, wie etwa CD-ROMs, ZIP-Disketten, USB-Sticks, etc., ermöglichen raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich. Als derartige Risiken wären unter anderem zu nennen:

- unkontrolliertes Booten von Geräten etwa von Diskette oder CD-ROM
- unautorisierte Installation von Software
- unberechtigte Kopien von Daten auf Wechselmedien (Vertraulichkeitsverlust)
- Einschleppen von Malware (Viren, …)

Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | mittel |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

#### *3.4.3.7 Verschlüsselung*

- Keine Verschlüsselung von Firmennotebooks

Verschlüsselung trägt zur Sicherheit der Daten bei. Ist ein Datenträger nicht verschlüsselt, kann im Falle eines Diebstahls (PC, Laptop, Festplatte) sehr einfach der Inhalt des Datenträgers ausgelesen werden. Besonders bei Laptops sollte die Festplatte verschlüsselt sein, da bei diesen Geräten die Wahrscheinlichkeit eines Diebstahls oder Verlusts hoch ist, speziell bei Verwendung im Aussendienst und im Ausland. Verschlüsselung benötigt aber Ressourcen, sodass es zu Einbußen bei der Leistungsfähigkeit eines Systems kommt. Weiters ist ein Komfortverlust und ein Mehraufwand mit einer Verschlüsselung verbunden (Passworteingabe, Passwortverwaltung).
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | hoch |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

### 3.4.4 Datenaustausch und Benutzerverwaltung

#### *3.4.4.1 Active Directory Struktur (AD-Struktur)*

- Unübersichtliche und teilweise redundante Gruppenzuteilungen
- Keine Organisationsseinheiten (OUs) im AD
- Domaincontroller ist auch Exchange-Mailserver

Die Verwaltung der Benutzer und der Gruppenzugehörigkeit durch das Active Directory eines Domänencontrollers bringt viele Vorteile (Benutzerverwaltung, Gruppenverwaltung, Ressourcenvergabe,…). Eine unübersichtliche AD-Struktur, wie sie unter 3.3.4.1 beschrieben ist, kann aber zu mehreren Sicherheitsrisiken führen:

- Die Gruppenzugehörigkeit eines Benutzers kann durch verschachtelte Gruppen nicht eindeutig festgestellt werden. Benutzer können dadurch über zu viele Zugriffsrechte verfügen.
- Ein Benutzer erhält Zugriff auf Ressourcen, die nicht für ihn vorgesehen sind.
- Ausgeschiedene Mitarbeiter werden übersehen und werden nicht gelöscht/deaktiviert
- Rechte werden immer neu vergeben, aber selten wieder genommen.

Der Domaincontroller wird auch als Exchange-Mailserver verwendet, was aber aus Sicherheits- und Performancegründen nicht empfohlen wird [PETRI01].
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | mittel |
| Handlungsbedarf | = | **mittel** |

#### *3.4.4.2 Berechtigungen auf Serverlaufwerke*

- Verzeichnisrechte durch den Benutzer manipulierbar (Vollzugriff möglich)
- Confinement Problem (siehe dazu Kapitel 3.3.4.2)

Als Basis für die Berechtigungen auf Serverlaufwerke wird das Gruppenkonzept der AD-Struktur verwendet (siehe dazu auch Kapitel 3.4.4.1). Die bestehenden Freigabeberechtigungen ermöglichen eine Manipulation der Verzeichnisrechte, wodurch ein nicht kontrollierbarer Datenaustausch zwischen Firmenmitarbeitern über das Firmennetzwerk möglich wird. Mitarbeiter können so zu Informationen kommen, die nicht für sie bestimmt sind und deren Weiterverwendung der Firma in vielfältiger Weise schaden kann (Weitergabe von Angeboten, Lieferanten, Produktions- und Entwicklungsdaten, Kundendaten,…).
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

#### *3.4.4.3 Netztransfer*

- Beliebiger Datenaustausch zwischen allen Firmenmitarbeitern möglich
- Confinement Problem (siehe dazu Kapitel 3.3.4.2)

Das unter 3.3.4.3 beschriebene Netztransfer-Verzeichnis erlaubt den beliebigen, unkontrollierbaren Datenaustausch zwischen einzelnen Mitarbeitern (vgl dazu auch Kapitel 3.4.4.2). Weiters können „vergessene“ Daten im Netztransfer immer wieder von anderen gelesen werden, obwohl diese Daten vielleicht nicht mehr aktuell sind.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | mittel |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

### 3.4.5 Personelle Mängel

#### *3.4.5.1 Regelungen für Mitarbeiter*

- Keine IT-Richtlinie für Mitarbeiter

Die Mitarbeiter stellen eine der wichtigsten Ressourcen einer Organisation dar. IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter ein ausgeprägtes Sicherheitsbewusstsein haben und bereit und fähig sind, die Vorgaben in der täglichen Praxis umzusetzen. Andererseits stellen Mitarbeiter auch potentielle Angriffs- oder Fehlerquellen dar. Aus diesen Gründen ist der Schulung und Sensibilisierung für Fragen der IT-Sicherheit eine besondere Bedeutung zuzumessen.

Fehlende Regelungen können zu gefährlichem Fehlverhalten der Mitarbeiter führen (vgl. dazu Kapitel 3.7.1).

Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | hoch |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

#### *3.4.5.2 Regelungen für Fremdpersonal*

- Keine IT-Richtlinie für den Umgang mit Fremdpersonal

Fremdpersonal ist grundsätzlich ein Sicherheitsrisiko in einem Unternehmen, weil es nicht mit den Sicherheitsregeln des Unternehmens vertraut ist. Zusätzlich gelten auch für Fremdpersonal die gleichen Annahmen wie für Mitarbeiter, d.h. auch Fremdpersonal hat potentielle Angriffs- oder Fehlerquellen.

Mögliche Sicherheitsrisiken durch Fremdpersonal sieht man, wenn man sich die Regelungen für Fremdmitarbeiter durchliest und annimmt, einige dieser Regelungen werden nicht eingehalten.

Die empfohlenen Regelungen sind unter 3.7.2 zusammengefasst.

Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | hoch |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

### *3.4.5.3 Ausscheiden von Mitarbeitern*

- Keine IT-Richtlinie beim Ausscheiden von Mitarbeitern

Das ungeregelte Ausscheiden kann zu erheblichen Problemen und Sicherheitsrisiken führen.

Mögliche Sicherheitsrisiken sieht man, wenn man sich die Regelungen für ausgeschiedene Mitarbeiter durchliest und annimmt, einige dieser Regelungen werden nicht eingehalten.

Die empfohlenen Regelungen für ausgeschiedene Mitarbeiter sind unter 3.7.3 zusammengefasst.

Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | hoch |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

### *3.4.5.4 Social Engineering*

- Keine Schulung der Mitarbeiter über Social Engineering

Von Social Engineering spricht man immer dann, wenn ein Angreifer, z.B. für Zwecke der Industriespionage, menschliche Eigenschaften ausnutzt um an Informationen zu kommen. Social Engineering Angriffe sind leider eine extrem effiziente Methode zur Informationsbeschaffung und zwar ohne Einsatz von technischen Hilfsmitteln. Angreifer nutzen dafür natürliche menschliche Reaktionen aus: Positive Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit, Dankbarkeit, Stolz auf die Arbeit und das Unternehmen oder weniger positive Aspekte wie Gutgläubigkeit, Respekt vor Autoritäten oder gar Bestechlichkeit und auch Eigenschaften wie Konfliktvermeidung und Liebesbedürfnis und der Wunsch, ein guter Teamplayer zu sein. Oft sind solche Angriffe eine Vorbereitung für einen Einbruch in das Firmennetz, z.B. indem auf diese Weise Benutzername und Passwort eines Mitarbeiters erschlichen werden oder indem das Imitieren eines Telecom-Technikers für ein Eindringen auf das Werksgelände genutzt wird. Social Engineering kann aber auch mit Gesprächen im Wirtshaus beginnen, wo ein Mitarbeiter Vertrauliches ausplaudert (vielleicht erzählt er stolz, an welchen Angeboten er derzeit arbeitet oder was für eine tolle Technologie die Firma gerade entwickelt), oder über Anrufe beim Empfang oder einer Sekretärin als Mitarbeiter einer anderen Niederlassung, bis hin

zum Vorstand, der einem (falschen) Journalisten gern ein Interview über Zukunftspläne des Unternehmens gibt. [SICK05]

Die Sicherheitsrisiken durch Social Engineering sind vielfältig und nur begrenzt durch technische Sicherheitsmaßnahmen einzuschränken. Ein Problem entsteht immer dann, wenn die Mitarbeiter nicht wissen wie vertraulich eine jeweilige Information tatsächlich ist und welche alternativen Möglichkeiten sie haben, die Legitimierung des Anrufers festzustellen, wenn ein Anrufer sich auf dem normalen Weg nicht legitimieren kann.

Hilfe dazu gibt es unter 3.7.4.

Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | hoch |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

### 3.4.6 Bauliche und infrastrukturelle Mängel

#### *3.4.6.1 Schützenswerte Gebäudeteile*

Es konnten in diesem Bereich keine wesentlichen Mängel festgestellt werden. Die beiden Serverräume sind zentral im Gebäude untergebracht und somit weitgehend vor Wassereinbruch und schädlichen Umwelteinflüssen geschützt.

Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | keiner |
| Handlungsbedarf | = | **keiner** |

#### *3.4.6.2 Zutrittskontrolle und Schlüsselverwaltung*

Aus der Erhebung der Mängel unter 3.3.6.2 ergeben sich folgende Sicherheitsrisiken:

- Jeder Mitarbeiter mit einem Schlüssel kann jederzeit mit einem Schlüsselschalter in das Firmengebäude. Der Zutritt wird nicht protokolliert, eine spätere Beweisführung ist nicht möglich (z.B. nach einem Diebstahl).
- Die Schiebetür im Untergeschoß ermöglicht den Zutritt für jedermann und dies auch jederzeit. Dies stellt ein nicht zu akzeptierendes Sicherheitsrisiko dar.
- Wer Zugang zum Serverraum hat, kann nicht sicher gesagt werden, weil ein Schlüsselplan fehlt.

- Putzfrau und Hausmeister haben ebenfalls einen Zentralschlüssel, es muss daher ein großes Vertrauen gegenüber diesen Mitarbeitern vorhanden sein.

Der Zugang zum Firmengebäude ist während der Betriebszeiten relativ einfach möglich, was aber noch kein großes Sicherheitsrisiko darstellt, da die angrenzenden Räume abgesperrt oder durch Mitarbeiter besetzt sind. Das Problem sind die fehlenden Richtlinien und Schulungen für Mitarbeiter in Bezug auf den Umgang mit betriebsfremden Personen.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | hoch |
| Schaden | = | hoch |
| Handlungsbedarf | = | **hoch** |

#### *3.4.6.3 Brandschutz*

Der Brandschutz und die notwendigen Maßnahmen werden durch einen Brandschutzbeauftragten verwaltet. Der Brandschutz wird als ausreichend eingestuft, sofern der Brandschutzbeauftragte nicht länger ausfällt.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | sehr gering |
| Schaden | = | gering |
| Handlungsbedarf | = | **keiner** |

#### *3.4.6.4 Stromversorgung*

- Kein automatischer Neustart der Server nach einem Stromausfall

Nur die Server und die notwendigen Switches werden durch eine USV zum Zwecke des kontrollierten Abschaltens versorgt. Die Dimensionierung der USV reicht für eine Überbrückungszeit von ca. 15 Minuten. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben, so dass nach Abwarten dieser Zeitspanne noch 5 Minuten übrig bleiben, um die angeschlossene IT geordnet herunterfahren zu können, sollte der Stromausfall länger andauern. Es gibt keinen automatisierten Neustart, wenn die Stromunterbrechung wieder vorbei ist. Fällt vor dem Wochenende die Stromversorgung für 15 Minuten aus, so sind nachher alle Server abgeschaltet. Bis zum Eintreffen eines IT-Verantwortlichen, der die Server wieder startet, ist der Zugriff auf die Server nicht möglich. Auch der Anmeldevorgang kann verweigert werden, weil der Domaincontroller nicht verfügbar ist. Bei wiederholten

Stromausfällen (Bautätigkeit) kann es durch die Ladezeit der USV zu längeren Verzögerungen kommen, weil die USV einen minimalen Ladezustand braucht, um die Server kontrolliert herunterfahren zu können.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | gering |
| Schaden | = | gering |
| Handlungsbedarf | = | **gering** |

#### *3.4.6.5 Klimatechnik*

- Keine Meldung bei Ausfall der Klimaanlage

Die Klimaanlage funktioniert vollautomatisch, ist aber bei einem Stromausfall nicht aktiv. Dieser Aspekt ist aber nicht problematisch, da dann auch (nach ca. 10min) die Server durch die USV herunter gefahren werden und eine Wärmeentwicklung im Serverraum kein Problem mehr darstellt. Eine Versorgung der Klimaanlage über die USV ist leistungsmässig nicht zu empfehlen und in der vorliegenden Form ausreichend.
Ein Ausfall der Klimaanlage führt zur Überhitzung der EDV-Anlagen und kann deren Abschaltung oder auch deren Zerstörung zur Folge haben. Eine Überwachung der Temperatur im Serverraum ist notwendig.
Daraus ergibt sich folgende Bewertung:

| | | |
|---|---|---|
| Eintrittswahrscheinlichkeit | = | sehr gering |
| Schaden | = | hoch |
| Handlungsbedarf | = | **mittel** |

## 3.5 Vorgeschlagener Maßnahmenkatalog

### 3.5.1 Allgemeines

Im Maßnahmenkatalog werden Maßnahmen und Zuständigkeiten festgelegt, um die einzelnen Sicherheitsmängel der IST-Analyse zu beseitigen oder auf ein angemessenes Maß zu reduzieren. In den folgenden Kapiteln werden technische Aspekte und Details, Maßnahmen betreffend das Verhalten der Mitarbeiter, Maßnahmen betreffend Richtlinien und Maßnahmen und Empfehlungen für das Management angeführt. Die ausgewählten Maßnahmen beziehen sich immer auf Maßnahmen aus dem Maßnahmenkatalog des ÖSHB (Kapitel 2.3.2). Die verwendeten Maßnahmen werden immer durch die Referenznummer der Maßnahme aus dem ÖSHB angegeben (z.B. SYS 4.9). Es können auch mehrere Maßnahmen aus dem ÖSHB notwendig sein, um einen Sicherheitsmangel zu beseitigen. Zu der Referenznummer werden immer auch der Titel der Maßnahme und ein verkürzter Text, der die Maßnahme beschreibt, angegeben. Der genaue Wortlaut muss aber aus dem ÖSHB entnommen werden.

Unter 2.3.2.6 *„Informationssicherheitsmaßnahmen“* sind die Referenznummern nach Kapiteln aufgelistet.

### 3.5.2 Zuständigkeiten

Die Firmenleitung ist die oberste Instanz einer Firma und trägt die Verantwortung für die Umsetzung der IT-Sicherheitsmaßnahmen. Die Aufsicht über die Umsetzung der Sicherheitsmaßnahmen hat der IT-Sicherheitsbeauftragte. Diese Position wird vom IT-Leiter übernommen. Für die technische Umsetzung sind der IT-Leiter und seine IT-Mitarbeiter verantwortlich. Wird eine Tätigkeit von einer Fremdfirma erledigt, muss die erfolgreiche Umsetzung durch den IT-Leiter überprüft werden (Durchführungsprotokoll, Meßprotokoll,…). Die personellen Maßnahmen sind von jedem betroffenen Mitarbeiter umzusetzen. Die weiteren Zuständigkeiten werden in den einzelnen Kapiteln angeführt.

## 3.6 Maßnahmenkatalog: technische Aspekte und Details

### 3.6.1 Desaster Recovery Konzept

Im Zuge des Desaster Recovery Konzept werden die Anwendungen, die in einem Unternehmen laufen, und die IT-Infrastruktur aufgelistet. Die genaue Risikoanalyse des Disaster Recovery Konzepts ist dann aber sehr zeitintensiv und für die Einführung der Grundschutzmaßnahmen nicht unbedingt erforderlich. Das Konzept selbst ist aber hilfreich, die Anwendungen und die damit verbundene IT-Infrastruktur aufzulisten und die Geschäftsprozesse zu analysieren.

#### *3.6.1.1 Zweck/Ziel*

Das Desaster Recovery soll gegen alle Bedrohungen, die aus dem Eintreten einer Katastrophe entstehen können, vorsorgen. Dies können Naturkatastrophen sein wie Feuer, Wasser oder technische Katastrophen, wie der Ausfall von Geräten oder der Versorgung mit Strom und Wasser, oder auch Probleme, die durch Menschen verursacht werden, entweder durch Fehler, Nachlässigkeit oder sogar Vorsatz. Dieses Konzept soll helfen, geeignete Vorsorgen zu treffen, damit die Schäden, die durch solche Probleme entstehen, vermieden oder zumindest minimiert werden.
Bei der Analyse werden die Anwendungen und die Systeme angeführt und nach Wichtigkeit eingeteilt, dazu werden die RTO und RPO angegeben. [SICK02]

#### *3.6.1.2 RTO und RPO*

Die „Recovery Time Objective“ (RTO) ist die maximale Zeit vom Eintritt des Ausfalls bis zur Wiederaufnahme des Betriebs.
Die „Recovery Point Objective“ (RPO) ist der maximale zeitliche Abstand zwischen der letzten gesicherten Transaktion und einem Ausfall (tolerierter Datenverlust).
Die Bestimmung von RTO und RPO ist vom jeweiligen Unternehmen abhängig und wird daher hier nicht ausgeführt.

#### *3.6.1.3 Anwendungen und Basis-Infrastruktur*

Hier werden nun die Anwendungen und die Basis-Infrastruktur auszugweise angeführt. Aus Gründen der Anonymisierung wird auf firmenspezifische Anwendungen verzichtet.

Die Tabelle ist wie folgt aufgebaut:

| RTO | RPO | Beschreibung | Kurzbeschreibung der Anwendung bzw. Infrastruktur |
|---|---|---|---|
| | | Ort | Ort, wo die Anwendung installiert bzw. die Infrastruktur stationiert ist |
| Bezeichnung der Anwendung / Infrastruktur | | Basiert auf | System, das für den Betrieb der Anwendung/Infrastruktur notwendig ist |
| | | Maßnahmen | Maßnahmen, die eine Wiederherstellung der Funktion der Anwendung bzw. Infrastruktur im Fehlerfall sicherstellen |

Alle Anwendungen, die auf Servern laufen, benötigen für ihre Funktion immer das gesamte IT-Netzwerk und die Stromversorgung. Diese beiden Punkte werden in der Tabelle (Punkt: „basiert auf“) nicht angeführt. Bei der Risikoanalyse müssen diese beiden Aspekte jedoch mit einbezogen werden.

| RTO | RPO | Beschreibung | CRM, Projektmanagement, DMS, QM |
|---|---|---|---|
| | | Ort | Server SQL01 im Serverraum EDV1 |
| Axavia – AG | | Basiert auf | SQL-Datenbank |
| | | Maßnahmen | Sicherung der Datenbank → Richtlinie Datensicherung 5.2 |

| RTO | RPO | Beschreibung | ERP-System (Lager, Auftragsbearbeitung, Zeiterfassung, Einkauf) |
|---|---|---|---|
| | | Ort | Server DATEN03 im Serverraum EDV1 |
| Logistik Pur | | Basiert auf | NTFS-Freigaben, Active Directory |
| | | Maßnahmen | Sicherung des Dateisystems → Richtlinie Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Lohnverrechnung, Buchhaltung, Controlling |
|---|---|---|---|
| | | Ort | Server DATEN01 im Serverraum EDV1 |
| BMD | | Basiert auf | Datenbanksoftware SQL-Express lokal auf 4 Clients<br>Datenbank auf gemapptem Serverlaufwerk |
| | | Maßnahmen | Sicherung der Datenbank → Richtlinie Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Email, öffentliche Kalender, Besprechungskoordination |
|---|---|---|---|
| | | Ort | Server COMM01 im Serverraum EDV1 |
| Outlook | | Basiert auf | Microsoft Exchange |
| | | Maßnahmen | Sicherung der gesamten Datenbank, Betrifft Mailserver, Virenschutz, Firewall (erkennt Mailempfang),<br>→ Richtlinie Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Verwaltung der Benutzeraccounts, Anmeldeinformationen, Ressourcenvergabe |
|---|---|---|---|
| | | Ort | Server DC01 und COMM01 im Serverraum EDV1 |
| Active Directory<br>DNS<br>DHCP | | Basiert auf | Microsoft Windows 2003 Server |
| | | Maßnahmen | Sicherung der AD-Datenbank, Replizierung mit 2. AD-Server, 2 Standorte der Server, Umschalten auf alternativen Domaincontroller automatisch, → Richtlinie Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Dateiablage der Mitarbeiter und Abteilungen |
|---|---|---|---|
| | | Ort | Server DATEN01 im Serverraum EDV1 |
| Fileserver | | Basiert auf | Microsoft Windows 2003 Server Dateisystem |
| | | Maßnahmen | Sicherung der Daten → Richtlinie Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Verbindung zum Einwählen der Außendienstmitarbeiter |
|---|---|---|---|
| | | Ort | Firewall und Server ISA01 im Serverraum EDV1 |
| VPN – Außendienst | | Basiert auf | Checkpoint Firewall der Firma Securepoint |
| | | Maßnahmen | Sicherung der Firewall-Regeln → Richtlinie Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Checkpoint Firewall der Firma Securepoint |
|---|---|---|---|
| | | Ort | Hardware-Firewall im Serverraum EDV1 |
| Firewall | | Basiert auf | Checkpoint Firewall der Firma Securepoint |
| | | Maßnahmen | schnelle Reaktionszeit, Sicherung der Firewall-Regeln |

| RTO | RPO | Beschreibung | Ikarus Contentwall auf gleicher Hardware wie Firewall |
|---|---|---|---|
| | | Ort | Hardware-Firewall im Serverraum EDV1 |
| Virenschutz global | | Basiert auf | Ikarus Contentwall der Firma Securepoint |
| | | Maßnahmen | Regelmäßige automatische Updates |

| RTO | RPO | Beschreibung | Kaspersky Internet Security |
|---|---|---|---|
| | | Ort | Server FIREW01 im Serverraum EDV1 |
| Virenschutz lokal | | Basiert auf | Ikarus Contentwall der Firma Securepoint |
| | | Maßnahmen | Regelmäßige automatische Updates der Client,<br>Abschalten durch den Benutzer darf nicht möglich sein |

| RTO | RPO | Beschreibung | Blackberries für Email und Telefonie |
|---|---|---|---|
| | | Ort | Server COMM02 im Serverraum EDV1 |
| Blackberry | | Basiert auf | Blackberry Software über Microsoft Exchange |
| | | Maßnahmen | Sicherung der Exchange-Mail-Datenbank, → RL Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Blackberries für Email und Telefonie |
|---|---|---|---|
| | | Ort | Hardware-Firewall im Serverraum EDV1 |
| Internet | | Basiert auf | Lokaler Internet-Browser |
| | | Maßnahmen | Sicherstellen von Firewall, Contentwall und lokalem Virenschutz |

| RTO | RPO | Beschreibung | Knowledge Base, Pizzabestellung |
|---|---|---|---|
| | | Ort | Server INTRANET01 im Serverraum EDV1 |
| Intranet | | Basiert auf | Lokaler Internet-Browser |
| | | Maßnahmen | Sicherung der Intranet-Dateien, → RL Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Bandsicherung aller relevanten Firmendaten |
|---|---|---|---|
| | | Ort | Bandlaufwerke am DATEN01 und DATEN03 im Serverraum EDV1 |
| Datensicherung | | Basiert auf | BackupExec Sicherungssoftware, Bandlaufwerke |
| | | Maßnahmen | → RL Datensicherung 5.2 |

| RTO | RPO | Beschreibung | Telefonie |
|---|---|---|---|
| | | Ort | Telefonanlage AscoTel im Serverraum EDV1<br>Verwaltungssoftware auf FIREW01 im Serverraum EDV1 |
| Telefon | | Basiert auf | Leitungsnetz der Telekom |
| | | Maßnahmen | Strategische Verteilung von Firmenhandys, Informationsmeldung schalten, die auf die Handynummer verweist (Telekom). |

### 3.6.2 Datensicherung und Notfallwiederherstellung

Die Maßnahmen zur Datensicherung und –wiederherstellung sind sehr wichtig. Ziel ist es, nach einem Datenverlust, eine Datenwiederherstellung in einem akzeptablen Zeitraum zu gewährleisten. Wesentliche Werkzeuge, dieses Ziel zu erreichen, sind eine Richtlinie zur Datensicherung und ein Notfallplan zur Wiederherstellung. Bevor eine solche Richtlinie festgelegt werden kann, müssen die Geschäftsprozesse ermittelt werden, damit die zu sichernden Daten festgelegt werden können. Dies wird mit dem Desaster Recovery Konzept (Kapitel 3.6.1) gemacht. Weiters werden die Sicherungsmethode, das Sicherungsintervall und der Sicherungszeitpunkt festgelegt. Die Sicherungsmedien sind in der IT-Abteilung, dem Firmentresor und einem Bankschließfach zu verwahren, damit die Sicherungsmedien nicht an nur einem Ort gelagert werden und so z.B. durch Brand vernichtet werden können. Ein weiterer Faktor ist die Aktualisierung der Sicherungsmedien, d.h. es müssen die Sicherungsmedien und -laufwerke regelmässig erneuert werden, weil die Datenmenge regelmässig ansteigt, bzw. die Medien einer Alterung unterliegen. Hier bedarf es einer definierten Vorgehensweise, wie die bereits gesicherten Daten wieder auf die aktuellen Datenträger überspielt werden können. Produktionsdaten müssen 15 Jahre aufbewahrt werden und eine Wiederherstellung bis zu diesem Zeitraum gewährleistet sein. Hier ist auch sicher zu stellen, dass diese Daten auch noch von einer Anwendung interpretiert und gelesen werden können. Eine Möglichkeit, dies sicher zu stellen, ist es, die dazu passende Anwendung ebenfalls zu sichern und diese dann in einer virtuellen Maschine laufen zu lassen. Letztendlich müssen die gemachten Sicherungen periodisch geprüft werden, ob eine Wiederherstellung möglich ist. Die Notfallwiederherstellung und die Sicherungsmedien müssen jährlich getestet werden. All diese Anforderungen werden in der Richtlinie Datensicherung und dem Notfallplan Datenwiederherstellung festgelegt.

Der Richtlinie und dem Notfallplan liegen folgende Maßnahmen aus dem ÖSHB zugrunde:

| ***BCP 1.1*** | ***Regelmässige Datensicherung*** | ***ÖSHB Seite 299*** |
|---|---|---|

*Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist Folgendes festzulegen:*

- *Umfang der zu sichernden Daten: Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden.*
- *Zeitintervall: z.B. täglich, wöchentlich, monatlich*
- *Zeitpunkt: z.B. nachts, freitags abends*
- *Anzahl der aufzubewahrenden Generationen: z.B. Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitagabend-Sicherungen der letzten zwei Monate*
- *Speichermedien: z.B. Bänder, Kassetten, Disketten, Spiegelplatte*
- *Wiederaufbereitung der Datenträger (Löschung vor Wiederverwendung)*
- *Zuständigkeit für die Durchführung (Systemadministration, Benutzer/in)*
- *Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (verbleibender Platz auf den Speichermedien)*
- *Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung, gewählte Parameter, Beschriftung der Datenträger)*

| ***BCP 1.2*** | ***Entwicklung eines Datensicherungskonzeptes*** | ***ÖSHB Seite 301*** |
|---|---|---|

*Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt. Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist. Diese Lösung muss auch jederzeit aktualisierbar und erweiterbar sein. Weiters ist dafür Sorge zu tragen, dass alle betroffenen IT-Systeme im Datensicherungskonzept berücksichtigt werden und das Konzept stets den aktuellen Anforderungen entspricht.*

| ***BCP 1.5*** | ***Geeignete Aufbewahrung der Backup-Datenträger*** | ***ÖSHB Seite 303*** |
|---|---|---|

- *Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.*
- *Ein ausreichend schneller Zugriff im Bedarfsfall muss gewährleistet sein.*
- *Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner - auf jeden Fall in einem anderen Brandabschnitt, wenn möglich disloziert - aufbewahrt werden.*

## 3.6.3 Computer- und Datensicherheit

### *3.6.3.1 Firewalls*

Die Vernetzung vorhandener Teilnetze mit globalen Netzen wie dem Internet führt zu einem neuen Informationsangebot, lässt aber auch neue Gefährdungen entstehen, da prinzipiell nicht nur ein Informationsfluss von außen in das zu schützende Netz stattfinden kann, sondern auch in die andere Richtung. Die Kontrolle der Logfiles der Firewall muss regelmässig erfolgen, um versuchte Angriffe erkennen zu können. Ausgehende E-Mails sollten ebenfalls durch die Firewall auf Schadsoftware überprüft werden (vgl. Kapitel 3.4.3.2).

Die folgenden Maßnahmen aus dem ÖSHB sind für diesen Punkt wichtig:

| ***SYS 8.1*** | ***Erstellung einer Internet-Sicherheitspolitik*** | ***ÖSHB Seite 221*** |
|---|---|---|

- *Schutz des internen Netzes gegen unbefugten Zugriff von außen*
- *Schutz einer Firewall gegen Angriffe aus dem externen Netz, aber auch gegen Manipulationen aus dem internen Netz*
- *Schutz der lokalen Daten gegen Angriffe auf deren Vertraulichkeit oder Integrität*
- *Schutz der lokalen Netzkomponenten gegen Angriffe auf deren Verfügbarkeit*
- *Verfügbarkeit der Informationen des externen Netzes im zu schützenden internen Netz, (Die Verfügbarkeit dieser Informationen muss aber gegenüber dem Schutz der lokalen Rechner und Informationen zurückstehen!)*
- *Schutz vor Angriffen, die auf IP-Spoofing beruhen oder die Source-Routing Option, das ICMP-Protokoll bzw. Routingprotokolle missbrauchen*
- *Schutz vor Angriffen durch das Bekannt werden von neuen sicherheitsrelevanten Softwareschwachstellen*

*Im nächsten Schritt ist festzulegen, welche Arten der Kommunikation mit dem äußeren Netz zugelassen werden. Bei der Auswahl der Kommunikationsanforderungen müssen speziell die folgenden Fragen beantwortet werden:*

- *Welche Informationen dürfen durchgelassen werden?*
- *Welche Informationen sollen verdeckt werden?*
- *Welche Authentisierungsverfahren sollen benutzt werden?*
- *Welche Zugänge werden benötigt?*
- *Welcher Datendurchsatz ist zu erwarten?*

| ***SYS 8.2*** | ***Entwicklung eines Firewallkonzeptes*** | ***ÖSHB Seite 223*** |
|---|---|---|

*Die Firewall muss:*

- *auf einer umfassenden Sicherheitspolitik aufsetzen*
- *in dem IT-Sicherheitskonzept der Organisation eingebettet sein*
- *korrekt installiert und korrekt administriert werden.*

| *SYS 8.3* | ***Installation einer Firewall*** | ***ÖSHB Seite 225*** |
|---|---|---|

*Damit eine Firewall einen wirkungsvollen Schutz eines Netzes gegen Angriffe von außen bietet, müssen einige grundlegende Voraussetzungen erfüllt sein:*

- *Jede Kommunikation zwischen den beiden Netzen muss ausnahmslos über die Firewall geführt werden.*
- *Eine Firewall darf nur zwei Anschlüsse (sicheres / unsicheres Netz) haben.*
- *Eine Firewall darf ausschließlich als schützender Übergang zum internen Netz eingesetzt werden*
- *Ein administrativer Zugang zur Firewall darf nur über einen gesicherten Weg möglich sein, also z.B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz.*
- *Für die Konzeption und den Betrieb einer Firewall muss geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb einer Firewall darf nicht unterschätzt werden.*
- *Alleine die Auswertung der angefallenen Protokolldaten nimmt erfahrungsgemäß viel Zeit in Anspruch. Die Logfiles sollten täglich (mindestens jedoch zweimal pro Woche) kontrolliert werden. Ein Firewall-Administrator muss fundierte Kenntnisse über die eingesetzten IT-Komponenten besitzen und auch entsprechend geschult werden.*
- *Die Benutzer/innen des lokalen Netzes sollten durch den Einsatz einer Firewall möglichst wenige Einschränkungen hinnehmen müssen.*

| *SYS 8.4* | ***Sicherer Betrieb einer Firewall*** | ***ÖSHB Seite 226*** |
|---|---|---|

*Für einen sicheren Betrieb einer Firewall sind eine fachgemäße Administration sowie eine regelmäßige Überprüfung auf die korrekte Einhaltung der umgesetzten Sicherheitsmaßnahmen erforderlich. Insbesondere müssen die für den Betrieb der Firewall getroffenen organisatorischen Regelungen regelmäßig oder zumindest sporadisch auf ihre Einhaltung überprüft werden. Es sollte in zyklischen Abständen kontrolliert werden, ob neue Zugänge unter Umgehung der Firewall geschaffen wurden.*

### *3.6.3.2 Virenschutz*

Um für ein komplexes IT-System oder eine gesamte Organisation einen effektiven Virenschutz zu erreichen, ist ein mehrstufiges Schutzkonzept erforderlich, bei dem in jeder Stufe angemessene und aufeinander abgestimmte Schutzmaßnahmen realisiert werden. Schutzmaßnahmen sind zu treffen auf Ebene der Firewall, auf Server-Ebene und auf Client-Ebene. Neben den technischen Schutzmaßnahmen sind auch organisatorische und personelle Maßnahmen erforderlich, um einem Virenbefall soweit wie möglich vorzubeugen, bzw. im Falle eines Virenbefalls den Schaden möglichst zu begrenzen.

Die folgenden Maßnahmen aus dem ÖSHB sind für diesen Punkt wichtig:

| ***SYS 4.2*** | ***Generelle Maßnahmen zur Vorbeugung gegen Virenbefall*** | ***ÖSHB Seite 181*** |
|---|---|---|

- *Regelmäßige Durchführung einer Datensicherung (BCP 1.1)*
- *Sichere Aufbewahrung der Sicherheitskopien von Datenträgern (BCP 1.5)*
- *Überprüfung aller ein- und ausgehenden Datenträger (SYS 2.3)*
- *Überprüfung aller ein- und ausgehenden Dateien über externe Netzwerke*
- *Als vorbeugende Maßnahme gegen Virenbefall empfiehlt es sich, die Boot-Reihenfolge auf C: A: einzustellen oder das Booten von Diskette ganz zu unterbinden*
- *Die Unterteilung der Festplatte in mehrere Partitionen kann die Rekonstruktion von Daten nach einem Virus-Schaden erleichtern*
- *Es sollten nur vertrauenswürdige Programme zugelassen sein, die auch über entsprechende Sicherheitsfunktionen verfügen. Dies gilt in besonderem Maße für E-Mail-Programme. "Private" Insel-Lösungen auf einzelnen Arbeitsplatz-Rechnern sollten nicht zugelassen werden, um die Sicherheit des Gesamtsystems nicht zu gefährden.*
- *Für Probleme sollte ein zentraler Ansprechpartner (E-Mail-Adresse, Telefon- und Fax-Nummer) benannt werden.*

| ***SYS 4.5*** | ***Empfohlene Virenschutzmaßnahmen auf Client-Ebene und Einzelplatzrechnern*** | ***ÖSHB Seite 182*** |
|---|---|---|

- *Aktivierung aller vorhandenen Sicherheitsfunktionen des Rechners (Passwort-Schutz, Bildschirmschoner mit Passwort, etc.), damit während der Abwesenheit des berechtigten Benutzers Unbefugte keine Möglichkeit haben, durch unbedachte oder gewollte Handlungen den Rechner zu gefährden.*
- *Einsatz eines aktuellen Virenschutzprogrammes mit aktuellen Signatur-Dateien, das im Hintergrund läuft (resident) und bei bekannten Viren Alarm schlägt. (Auch wenn am Mail-Server bereits ein Virenschutzprogramm zum Einsatz kommt, empfiehlt sich die Installation dezentraler Virenschutzprogramme, um beispielsweise auch Schutz bei verschlüsselter Kommunikation zu erreichen.)*
- *Aktivierung der Anzeige aller Dateitypen im Browser bzw. Mailprogramm.*
- *Aktivierung des Makro-Virenschutzes von Anwendungsprogrammen (MS Word, Excel, Powerpoint, etc.) und Beachtung von Warnmeldungen.*
- *Sofern möglich: Wahl der höchsten Stufen in den Sicherheitseinstellungen von Internet-Browsern (Deaktivieren von aktiven Inhalten (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script, VBS), etc.).*
- *Keine Nutzung von Applikationsverknüpfung für Anwendungen mit potentiell aktivem Code im Browser, keine Aktivierung von Anwendungen über Internet.*
- *Die Ausführung von aktiven Inhalten in E-Mail-Programmen immer unterbinden (entsprechende Optionen setzen).*
- *Durch den Einsatz eines Firewall-Produkts auf den Einzelplatzrechnern (Personal Firewalls), die regeln, welche Programme auf das Internet zugreifen dürfen, kann der Schadsoftware ebenfalls gezielt entgegen gewirkt werden. Dadurch wird die zentrale Firewall, die keine Informationen über die aufrufenden Programme hat, wirkungsvoll ergänzt (SYS 8.4)*

| *SYS 4.9* | *Verhaltensregeln bei Auftreten eines Virus* | *ÖSHB Seite 186* |
|---|---|---|

- *Beenden der laufenden Programme und Abschalten des Rechners.*
- *Einlegen einer einwandfreien, schreibgeschützten System-Diskette (”Notfall-Diskette”) in Laufwerk A und Booten des Rechners von dieser Diskette*
- *Überprüfen des Rechners mit einem aktuellen Virenschutzprogramm um festzustellen, ob tatsächlich ein Virus aufgetreten ist und um welchen Virus es sich ggf. handelt.*
- *Entfernen des Virus abhängig vom jeweiligen Virustyp*

#### *3.6.3.3 Wireless LAN (WLAN)*

Ein Anschluss des Access-Points über eine zweite Netzwerkkarte direkt an einen PC wäre möglich, da der Handscanner nur für jeweils einen PC benötigt wird und der WLAN-Zugang sonst keine Funktion hat. Dadurch wäre ein direkter Zugang vom WLAN in das Firmennetz nicht möglich.

Folgende Maßnahme ist zu beachten, wenn es um die Installation und Konfiguration eines WLANs geht:

| *SYS 6.14* | *Wireless LAN (WLAN)* | *ÖSHB Seite 207* |
|---|---|---|

- *Geeignete Positionierung und Ausrichtung der Zugriffspunkte und Antennen:*
- *Testen des Umkreises: Der mögliche Empfang im Umkreis der Organisation muss überprüft werden. Bei unerwünschten Reichweiten müssen entsprechende Gegenmaßnahmen ergriffen werden.*
- *Deaktivieren des Sendens der Service Set ID: Die Service Set ID (SSID) ist ein Name des WLANs, über den Knoten an das Netz verbinden. Dessen Bekanntgabe an Knoten, die diese eindeutige SSID nicht kennen, ist zu verhindern.*
- *Verschlüsselungsoptionen aktivieren:*
- *Access (WPA), bieten Schutz vor Zugriffen durch Dritte. Es gibt im Allgemeinen die Wahl zwischen unterschiedlichen Schlüssellängen (bei WEP beispielsweise 40 Bit oder 128 Bit). Es ist dabei sinnvoll den Schlüssel mit der größten Länge zu wählen, sofern die verwendeten Endgeräte dies zulassen.*
- *Von WEP zahlreiche Schwächen bekannt. Es empfiehlt sich daher, auf verbesserte Sicherheitsmechanismen wie WPA bzw. künftig 802.11i wenn möglich zurück zu greifen*
- *Ändern von Standardeinstellungen (Passwörtern): Standardeinstellungen der Zugriffspunkte – etwa Service Set ID (SSID), SNMP Community String, Administrator-Passwort – sind werksseitig voreingestellt und müssen sofort geändert werden, da die Standardpasswörter Angreiferinnen bzw. Angreifern durchaus bekannt sind (SYS 1.5)*
- *MAC-Adressfilterung am Zugriffspunkt: Der Zugang zu Zugriffspunkten kann bei vielen Geräten auch über die MAC-Adresse kontrolliert werden. Dies sollte nach Möglichkeit genutzt werden.*

### *3.6.3.4 Auswahl der Passwörter*

Erfolgt die Authentisierung in einem IT-System über Passwörter, so ist die Sicherheit der Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gewählt und verwendet wird. Dafür ist es empfehlenswert, eine Regelung zum Passwortgebrauch einzuführen, die Benutzer diesbezüglich zu unterweisen und die Einhaltung zu kontrollieren.
Die Verifizierung und Speicherung der Passwörter, wie unter Kapitel 3.3.3.4 beschrieben, sollte in keinem Fall weiter verfolgt werden. Die möglichen Risiken dieser Vorgangsweise werden im Kapitel 3.4.3.4 angeführt.
Im Folgenden stehen die Aussagen des IT-Leiters, die vermeintlich für die bestehende Vorgangsweise sprechen und als Anreiz auch die Alternativen dazu, auf diese Vorgangsweise zu verzichten.

- *„Passwörter werden beim ersten Mal durch die IT-Abteilung vergeben“*

  Es kann auch weiterhin ein Passwort vergeben werden, das beim ersten Login durch den Benutzer geändert werden muss. Ein späteres Anmelden ist nur durch ein Rücksetzen des Mitarbeiter-Passwortes möglich. Der Mitarbeiter muss aber irgendwie informiert werden, dass sein Passwort zurückgesetzt wurde.

- *„Passwort-Änderungen werden halbjährlich oder im Anlassfall von der IT-Abteilung angeregt“*

  Passwörter können durch Alterung ablaufen und müssen dann neu gesetzt werden, ausserdem ist eine Änderung durch den Benutzer jederzeit möglich.

- *„Passwörter werden durch die IT-Abteilung verifiziert“*

  Passwörter können durch eine Domain-Richtlinie komplex gehalten werden, eine Verwendung von Geburtsdaten und Namen von Angehörigen kann aber nicht verhindert werden.

- *„Eine Anmeldung mit dem Benutzeraccount ist nötig, damit ein PC auf die Bedürfnisse eines Benutzers abgestimmt werden kann (z.B. Microsoft Outlook Postfach einrichten, Eigene Dateien auf den Server umleiten, Email-Signaturen einrichten, Telefon-Software,…)“.*

  Benutzereinstellungen können durch Kopieren des Benutzerprofils auf den „Default User“ für alle zur Verfügung gestellt werden. Es ist weiters möglich, den PC am Beginn einmal zu konfigurieren und dann das Passwort beim ersten Login des Benutzers durch den Benutzer ändern zu lassen (s.o.).

In der folgenden Maßnahme aus dem ÖSHB werden einige Grundregeln gegeben, die eine Art Mindeststandard für die Wahl und die Handhabung von Passwörtern darstellen:

| ***SYS 1.5*** | ***Regelungen des Passwortgebrauches*** | ***ÖSHB Seite 167*** |
|---|---|---|

- *Das Passwort sollte mindestens 6 Zeichen lang sein*
- *Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl)*
- *Passwörter mit spezieller Bedeutung, wie Namen, Geburtsdaten, etc. sind ebenso zu meiden wie Standardausdrücke wie TEST, SYSTEM und Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456, etc.*
- *Voreingestellte Passwörter müssen umgehend durch individuelle Passwörter ersetzt werden.*
- *Die Eingabe des Passwortes sollte unbeobachtet stattfinden*
- *Bei der Eingabe darf das Passwort nicht auf dem Bildschirm angezeigt werden*
- *Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein*
- *Das Passwort muss regelmäßig gewechselt werden, z.B. alle 90 Tage*

*Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:*

- *Die Wahl von Trivialpasswörtern (s.o.) sollte mit technischen Mitteln verhindert werden (”Stopwortliste”)*
- *Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können*
- *Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, die nach einmaligem Gebrauch gewechselt werden müssen*
- *Nach einer vorgegebenen Anzahl von Fehlversuchen (meist 3) ist eine vordefinierte Aktion zu setzen. Eine solche Aktion kann etwa eine Sperre der Benutzer-ID sein, aber auch eine Sperre des Gerätes oder ein Timeout, eine Warnmeldung oder Ähnliches*
- *Bei der Authentisierung in vernetzten Systemen sollten Passwörter verschlüsselt übertragen werden*
- *Der Passwortwechsel sollte vom System regelmäßig initiiert werden*
- *Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden. Dazu sollten alle alten Passwörter bzw. eine größere Anzahl zum Vergleich herangezogen werden (Passwort Historie)*

### *3.6.3.5 Rechtestruktur auf Arbeitsplatzrechnern*

Eine Programminstallation darf für einen „normalen“ Benutzer nicht möglich sein. Aus diesem Grund müssen alle Benutzer auf ihren Arbeitsstationen mit eingeschränkten Rechten arbeiten. Programminstallationen dürfen nur durch die IT-Abteilung gemacht bzw. genehmigt werden. Um sicherzustellen, dass keine Programme mit unerwünschten Auswirkungen eingebracht werden und das System nicht über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird, muss das Einspielen nicht-freigegebener Software in Produktionssysteme bzw. ihre Nutzung verboten und – soweit technisch möglich – verhindert werden.

| ***SYS 3.1*** | ***Nutzungsverbot nicht freigegebener Software*** | ***ÖSHB Seite 175*** |
|---|---|---|
| • *Das Nutzungsverbot nicht-freigegebener Software sollte schriftlich fixiert werden, alle Mitarbeiter sind darüber zu unterrichten.*<br>• *Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.*<br>• *Das unautorisierte Einspielen und/oder Nutzen von Software ist soweit möglich mit technischen Mitteln zu verhindern.* | | |

| ***SYS 3.2*** | ***Nutzungsverbot privater Hard- und Software*** | ***ÖSHB Seite 175*** |
|---|---|---|
| *Im Allgemeinen sollte ein Nutzungsverbot privater Software (SYS 3.1), Hardware (Disketten, Wechselplatte, PC, Notebook) und Daten ausgesprochen werden.* | | |

| ***SYS 3.5*** | ***Update von Software*** | ***ÖSHB Seite 177*** |
|---|---|---|
| *Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden. Ein Update ist insbesondere dann erforderlich, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Systems haben.* | | |

| ***SYS 3.7*** | ***Datenformate*** | ***ÖSHB Seite 179*** |
|---|---|---|
| *Durch die Vielzahl von Anwendungsprogrammen ist auch eine Vielzahl von Datenformaten in Verwendung. Bei gleichartigen Anwendungen verschiedener Hersteller, aber auch bei den verschiedenen Versionen ein und desselben Programms eines Herstellers können die gebräuchlichen Datenformate variieren. Für die Lebensdauer von Datenbeständen muss gewährleistet werden, dass für den Zugriff auf gesicherte Daten auch in Zukunft Anwendungen existieren, welche die entsprechenden Datenformate bearbeiten können. In diesem Zusammenhang ist im Rahmen der Datensicherung und –pflege ggf. eine Umformatierung vorzusehen.* | | |

### 3.6.3.6 Wechselmedien

Wechselmedien ermöglichen raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich. Zur Verringerung dieser Bedrohungen stehen – abhängig von der Art der Wechselmedien und dem zugrunde liegenden Betriebssystem – eine Reihe von Möglichkeiten zur Verfügung, die nun beispielhaft angeführt werden.

| ***SYS 5.3*** | ***Sicherung von Wechselmedien*** | ***ÖSHB Seite 189*** |
|---|---|---|

- *Verzicht auf Disketten-, CD-ROM-, USB-Sticks, ...Laufwerke (bzw. ihr nachträglicher Ausbau)*
- *(Physischer) Verschluss von Laufwerken (z.B. durch Einsatz von Diskettenschlössern)*
- *(Logische) Sperre von Schnittstellen: Viele Betriebssysteme bieten die Möglichkeit, Schnittstellen zu sperren. Dabei ist allerdings zu beachten, dass dies nicht immer technisch möglich (z.B. SCSI-Schnittstellen) und oft auch aus betrieblichen Gründen nicht durchführbar ist (z.B. ist die USB-Schnittstelle oft für den Anschluss eines Druckers offen zu halten)*
- *Verblenden und Verplomben von Schnittstellen Nach Anschluss aller erforderlichen Schnittstellen wird die Rückseite des Gerätes mit einer speziellen Abdeckung verblendet. Diese wird verplombt, so dass etwaige Manipulationen ersichtlich sind. Diese Vorgehensweise bietet einen relativ hohen Grad an Sicherheit (insbesondere an nachträglichen Nachweismöglichkeiten), es ist aber zu bedenken, dass damit die Flexibilität der Systeme stark eingeschränkt wird. Häufige Übersiedlungen, Konfigurationsänderungen etc. können die Akzeptanz dieser Maßnahme bei Benutzerinnen bzw. Benutzern und Systemverantwortlichen stark reduzieren.*

Die Verwendung von Wechselmedien ist standardmässig zu verbieten und nur in genehmigten Ausnahmefällen zu erlauben. Die USB-Schnittstellen an den Arbeitsstationen und Laptops sind derzeit trotzdem nicht gesperrt, da dies von der Firmenleitung und auch dem IT-Verantwortlichen als zu restriktiv angesehen wird. Hier wird an die Verantwortlichkeit der Mitarbeiter verwiesen.

Die Verwendung von Wechseldatenträgern muss durch eine Richtlinie festgelegt werden. Diese Verwendung ist in der *IT-Sicherheitsrichtlinie für Mitarbeiter* (Kapitel 5.1) festgelegt.

#### *3.6.3.7 Verschlüsselung*

Sind auf einem Arbeitsplatzsystem besonders schutzwürdige Daten gespeichert und wird dieses System in einer nicht oder nur unzureichend geschützten Umgebung betrieben oder aufbewahrt, so ist der Einsatz eines Verschlüsselungsproduktes zu erwägen. Dies gilt in besonderem Maße – aber nicht ausschließlich – für mobile IT-Geräte. Mobile IT-Geräte (Laptops) unterliegen einem höheren Risiko als Arbeitsstationen, die immer am Firmengelände bleiben.
Es sind mehrere Laptops in Verwendung, die auch im Aussendienst und im Ausland für Produktpräsentationen verwendet werden. Es kommt schon vor, dass ein Mitarbeiter mit seinem Laptop über den halben Erdball reist, um Produkte zu präsentieren. Ein Diebstahl eines Laptops ist dabei keine Seltenheit. Damit die Daten bei einem Verlust oder Diebstahl sicher sind, müssen diese mobilen Rechner verschlüsselt werden. Als zusätzliche Sicherheit sollte auf diesen Laptops nur die notwendigen Präsentationsdaten und sonst keine firmenrelevanten Daten gespeichert werden.
Für die Verschlüsselung bietet sich z.B. die Software „FREE CompuSec®“ an:
*„Die CompuSec® Software ist eine Vollversion ohne Einschränkungen. Es ist keine Demo- oder Testversion. Sie wird angeboten "so wie sie ist" zum Zeitpunkt der Auslieferung ohne jegliche Garantie. Das Produkt wurde umfangreich getestet und enthält keine bekannten Fehler (bugs) zum Zeitpunkt der Produktfreigabe, eine hundertprozentige Fehlerfreiheit kann aber nicht garantiert werden. Die Software kann sowohl im professionellen als auch im privaten Bereich kostenlos genutzt werden. Es werden ein kostenpflichtiger Hotline Support und Wartungsverträge angeboten. Die Software wurde entwickelt für Windows Vista - 32bit, Windows XP, Windows 2000, Windows 2003, Window XP Tablet und SuSe Linux.“* [COMP01]

Die Software FREE CompuSec® bietet folgende Funktionen:

- Zugangsschutz vor dem booten des Betriebssystems
- Festplattenverschlüsselung mit 256-bit AES und Hibernation Modus
- Verschlüsselung von Wechselmedien wie USB Laufwerke oder Memory Sticks
- Verschlüsselung einzelner Dateien
- Datenübertragung via E-Mail und FTP (neu DataCrypt)
- Verschlüsselung von Dateien und Verzeichnissen auf Servern (SafeLan)

- Single-Sign-On unter Windows
- Identitätsmanagement für Passwortverschlüsselung local und für das Internet
- [ClosedTalk]® für sichere VoIP Kommunikation
- Tablet PC Unterstützung
- [DriveCrypt] für Verschlüsselung von Container

Folgende Maßnahmen aus dem ÖSHB sind für diesen Punkt relevant:

| ***INF 5.4*** | ***Nutzung und Aufbewahrung mobiler IT-Geräte*** | ***ÖSHB Seite 112*** |
|---|---|---|
| • *Die Benutzer mobiler IT-Geräte sind über die potentiellen Gefahren bei Mitnahme und Nutzung eines solchen Gerätes außerhalb der geschützten Umgebung eingehend zu informieren und zu sensibilisieren*<br>• *Werden auf mobilen IT-Geräten eingeschränkte, vertrauliche, geheime und/oder streng geheime bzw. personenbezogene und/oder sensible Daten gespeichert und verarbeitet, so ist die Installation eines Zugriffsschutzes sowie einer Festplatten- oder Dateiverschlüsselung dringend zu empfehlen*<br>• *Nach Möglichkeit sollten die Zeiten, in denen das Gerät unbeaufsichtigt bleibt, minimiert werden*<br>• *Werden mobile IT-Geräte in einem Kraftfahrzeug aufbewahrt, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe*<br>• *Wird ein mobiles IT-Gerät in fremden Büroräumen vor Ort benutzt, so ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das Gerät ausgeschaltet werden, um über das Bootpasswort die unerlaubte Nutzung zu verhindern*<br>• *In Hotelräumen sollte ein mobiles IT-Gerät nicht offen aufliegen. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe* | | |

| ***SYS 5.5*** | ***Einsatz eines Verschlüsselungsproduktes für Arbeitsplatzsysteme*** | ***ÖSHB Seite 191*** |
|---|---|---|
| • *Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne Kenntnis des verwendeten Schlüssels praktisch nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Praktisch nicht möglich bedeutet dabei, dass der erforderliche Aufwand zum Brechen des Algorithmus bzw. zum Entschlüsseln deutlich höher ist als der dadurch erzielbare Informationsgewinn*<br>• *Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden*<br>• *Der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel und die zugehörige Passphrase getrennt und geschützt zu halten. Ein hohes Maß an Sicherheit wird erreicht, wenn der Schlüssel auf einer Chipkarte gehalten wird* | | |

#### *3.6.3.8 Keine lokale Anmeldung möglich*

Alle Arbeitsstationen und Laptops müssen Mitglied der Firmendomäne sein, dadurch können diese Systeme zentral administriert werden. Die Domäne wird durch einen Microsoft Windows Server 2003 Domänencontroller verwaltet. Jedem Benutzer ist nur eine Anmeldung mit dem benutzereigenen Domänenaccount zu ermöglichen, eine lokale Anmeldung muss vermieden werden. Der lokale Administrations-Account ist durch ein sicheres Passwort zu schützen. Ist eine Nutzung ausserhalb der Domäne geplant (Ausland, Aussendienst), so muss sich der Benutzer einmal an diesem Laptop anmelden, wenn die Verbindung zur Domäne besteht. Das ermöglicht eine spätere Anmeldung ohne Verbindung zur Domäne, da das Benutzerprofil lokal gespeichert wird.

#### *3.6.3.9 Microsoft Outlook-Cache abschalten*

Für die Kalender- und Emailverwaltung wird Microsoft Exchange Mailserver eingesetzt. Durch Deaktivieren des Outlook-Cache werden keine Emails und Kontakte mehr lokal auf dem Rechner gespeichert und nur durch eine Verbindung zum Mailserver können Kontakte und Emails gelesen werden.
Aussendienstmitarbeiter verfügen neben einem Firmenlaptop zusätzlich über einen „Blackberry“. Die E-Mails und Termine dieser Mitarbeiter werden direkt zu diesem tragbaren Gerät gesendet. Es ist daher eine Verwendung der E-Mail-Funktion nur in Einzelfällen notwendig, daher soll der Outlook-Cache abgeschaltet werden.

Der Outlook-Cache wird folgendermaßen abgeschaltet:

- Unter Microsoft Outlook im Menü *Extras* auf *Kontoeinstellungen* klicken
- Unter der Registerkarte *E-Mail* auf das Exchange Server-Konto wechseln
- Das Kontrollkästchen *Exchange-Cache-Modus verwenden* deaktivieren

[MIC01]

Für die Arbeitsstationen am Firmengelände ist diese Einstellung nicht zu empfehlen, da dann die Synchronisationszeit sehr hoch ist und die Vorteile des Outlook-Cache auch nicht genutzt werden könnten (siehe dazu [MIC01]).

#### 3.6.3.10 Updates der Arbeitsstationen automatisieren

Arbeitsstationen müssen immer mit den notwendigen Software-Updates versorgt werden. Die notwendigen Betriebssystem- und Software-Updates, sowie Updates der Virenschutzsoftware der Clientrechner müssen automatisch erfolgen.
Diese Aktualisierung kann durch den *Windows Server Update Service* (WSUS) und die servergestützte Virenschutzsoftware durchgeführt werden.
Eine Abschaltung dieser Services durch den Anwender darf nicht möglich sein.

#### 3.6.3.11 Entsorgung alter Hard- und Software

Alte Hard- und Software darf nicht einfach sorglos in den Müll geworfen werden. Alte Datenträger (Disketten, Festplatten, CDs,…) und auch Aufzeichnungen und Ausdrucke auf Papier müssen fachgerecht entsorgt werden. Diese Vorgangsweise ist in der *IT-Sicherheitsrichtlinie für Mitarbeiter* (Kapitel 5.1) und der *Richtlinie Datenschutz* (Kapitel 5.3) dokumentiert.

#### 3.6.3.12 Sicherheit des Internetzugangs

Der Zugang zum Internet ist durch eine Hardware-Firewall und eine Contentwall mit Spamschutz und Greylister geschützt. Auf jeder Arbeitsstation und jedem Server muss ein lokaler Virenschutz installiert sein, der idealerweise zentral verwaltet wird. Auf Laptops muss eine Personal Firewall aktiv sein, wenn diese nicht im Firmennetz eingebunden sind.
Der Internetzugang muss auf jene PCs eingeschränkt werden, die diesen Zugang benötigen. Auf PCs, die keinen Internetzugang benötigen (z.B. PCs für den reinen Produktionsbetrieb), soll dieser auch nicht möglich sein.
Der Internet-Browser muss durch automatische Updates immer auf neuestem Stand gehalten werden. Eine Abschaltung dieser Updates durch den Anwender darf nicht möglich sein.
Die empfohlenen Maßnahmen sind in der *Richtlinie Datenschutz* (Kapitel 5.3) dokumentiert.

### 3.6.4 Datenaustausch und Benutzerverwaltung

Durch organisatorische und technische Vorkehrungen ist sicherzustellen, dass der Zugriff zu IT-Systemen, Netzwerken, Programmen und Daten nur berechtigten Personen oder Prozessen und nur im Rahmen der festgelegten Regeln möglich ist.

Folgende Maßnahmen aus dem ÖSHB unterstützen dieses Vorhaben:

| ***SYS 1.1*** | ***Grundsätzliche Festlegungen zur Rechteverwaltung*** | ***ÖSHB Seite 163*** |
|---|---|---|

- *welche Subjekte (z.B. Personen, Programme, Prozesse, ...) und welche Objekte (z.B. IT-Anwendungen, Daten, ...) unterliegen der Rechteverwaltung*
- *welche Arten von Rechten (z.B. Lesen, Schreiben, Ausführen, ...) können zwischen Subjekten und Objekten existieren*
- *wer darf Rechte einsehen, vergeben bzw. ändern*
- *welche Regeln müssen bei Vergabe bzw. Änderung eingehalten werden (Authentisierung, ev. 4-Augen-Prinzip)*
- *welche Rollen müssen durch die Rechteverwaltung definiert werden (z.B. Administrator, Revision, Benutzer/innen,…)*
- *welche Rollen sind miteinander unvereinbar (z.B. Benutzer/in und Revision, Administrator und Auditor,…)*
- *wie erfolgen Identifikation und Authentisierung*

| ***SYS 1.2*** | ***Vergabe und Verwaltung von Zugriffsrechten*** | ***ÖSHB Seite 163*** |
|---|---|---|

- *Die Rechteverwaltung darf nur durch einen Berechtigten und nur im Rahmen der in der Zugriffskontrollpolitik festgelegten Regeln durchgeführt werden*
- *Grundsätzlich sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist (”Need-to-know-Prinzip”)*
- *Jeder Benutzer soll seine Rechte innerhalb einer Anwendung einsehen können, ebenso jeder Verantwortliche für seinen Bereich*
- *Personelle und aufgabenbezogene Änderungen müssen innerhalb der Rechteverwaltung unverzüglich berücksichtigt werden*
- *Es muss ein geregeltes Verfahren für den temporären Entzug von Zugriffsrechten (z.B. bei Urlaub, Karenz, ...) bestehen*
- *Bei Ausscheiden eines Mitarbeiters sind dessen Kennung und die zugehörigen Rechte unverzüglich zu deaktivieren bzw. zu löschen*
- *Nicht mehr aktive Benutzerkennungen dürfen nicht für Nachfolger reaktiviert werden*
- *Zusätzlich sollte in definierten Abständen eine Suche nach “toten Benutzerkennungen”, also Kennungen, die seit einem längeren, systembezogen zu definierenden Zeitraum nicht benutzt wurden, vorgesehen sein*

### *3.6.4.1 Active Directory Struktur*

Die im Kapitel 3.3.4.1 angeführten Mängel machen eine Neuplanung der AD-Struktur notwendig.

Für die Neuplanung empfiehlt sich folgende Vorgangsweise:

- Die bestehende AD-Struktur anfangs nicht verändern, damit der Betrieb aufrecht bleiben kann.
- Planung einer übersichtlichen Gruppenstruktur (Abteilungen, Projekte,…) und Freigabestrategie der Verzeichnisse
- Namensgebung der AD-Gruppen sinnvoll gestalten, evt. gleiche Gruppen mit gleichen Vorsilben ausstatten (Abt-Entwicklung, Abt-Produktion,…)
- Mitarbeiter neu im AD anlegen (per Skript). Dadurch kann der Anmeldenamen neu vergeben und veraltete Accounts werden nicht noch mal angelegt. Alternativ können auch die alten Accounts weiter verwendet werden.
- Zuteilung der Mitarbeiter zu den AD-Gruppen
- Das neue System ausgiebig testen
- Deaktivieren der alten AD-Gruppen
- Das System mit den neuen Gruppen starten
- Wenn das System zufriedenstellend läuft, sind die alten Gruppen zu löschen

Eine weitere Hilfestellung bietet die folgende Maßnahme aus dem ÖSHB:

| ***SYS 6.10*** | ***Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz*** | ***ÖSHB Seite 201*** |
|---|---|---|
| *In der Sicherheitsstrategie muss aufgezeigt werden, wie ein Client-Server-Netz für die jeweilige Organisation sicher aufgebaut, administriert und betrieben wird. Nachfolgend werden die einzelnen Entwicklungsschritte mit der Überschrift vorgestellt:*<br>*1. Definition der Client-Server-Netzstruktur*<br>*2. Regelung der Verantwortlichkeiten*<br>*3. Festlegen der Namenskonventionen*<br>*4. Festlegen der Regeln für Benutzeraccounts*<br>*5. Einrichten von Gruppen*<br>*6. Festlegen von Benutzerrechten*<br>*7. Festlegen der Vorgaben für Protokollierung*<br>*8. Regelungen zur Datenspeicherung*<br>*9. Einrichten von Projektverzeichnissen*<br>*10. Vergabe von Zugriffsrechten*<br>*11. Verantwortlichkeiten für Administratoren und Benutzer im Client-Server-Netz*<br>*12. Schulung* | | |

### 3.6.4.2 Berechtigungen auf Serverlaufwerke

Aufgrund der Erkenntnisse aus dem Kapitel vorher ist auch die Rechte- und Verzeichnisstruktur der freigegebenen Serverlaufwerke von vielen Altlasten belegt. Mitarbeiter verfügen über zu viele Zugriffsrechte auf Daten und Verzeichnisse. Diese Zugriffsrechte gehören auch überarbeitet und neu vergeben. Die Lösung ist, wie auch im vorigen Kapitel 3.6.4.1 über das Active Directory, eine Neuanlage von Gruppen und Gruppenzugehörigkeiten, d.h. es wird parallel eine neue Gruppenstruktur mit Organisationseinheiten geschaffen und auch die Verzeichnisstruktur wird parallel neu angelegt. Nachdem die Gruppenzugehörigkeiten neu gemacht wurden, wird das alte Gruppenkonzept zuerst deaktiviert und dann endgültig gelöscht.

Das Freigabeproblem, welches unter 3.4.4.2 beschrieben ist, kann durch eine Änderung der Freigabeberechtigung gelöst werden. Die Freigabeberechtigung am Verzeichnis \\Daten01\Verwaltung muss so geregelt sein, dass Administratoren zwar Vollzugriff haben, die Domänenbenutzer aber nur Änderungsrechte.

Die Erklärung liegt in der verwendeten Windows Server Version, bei der eine zu offene Freigabeberechtigung zu diesem Ergebnis führt.

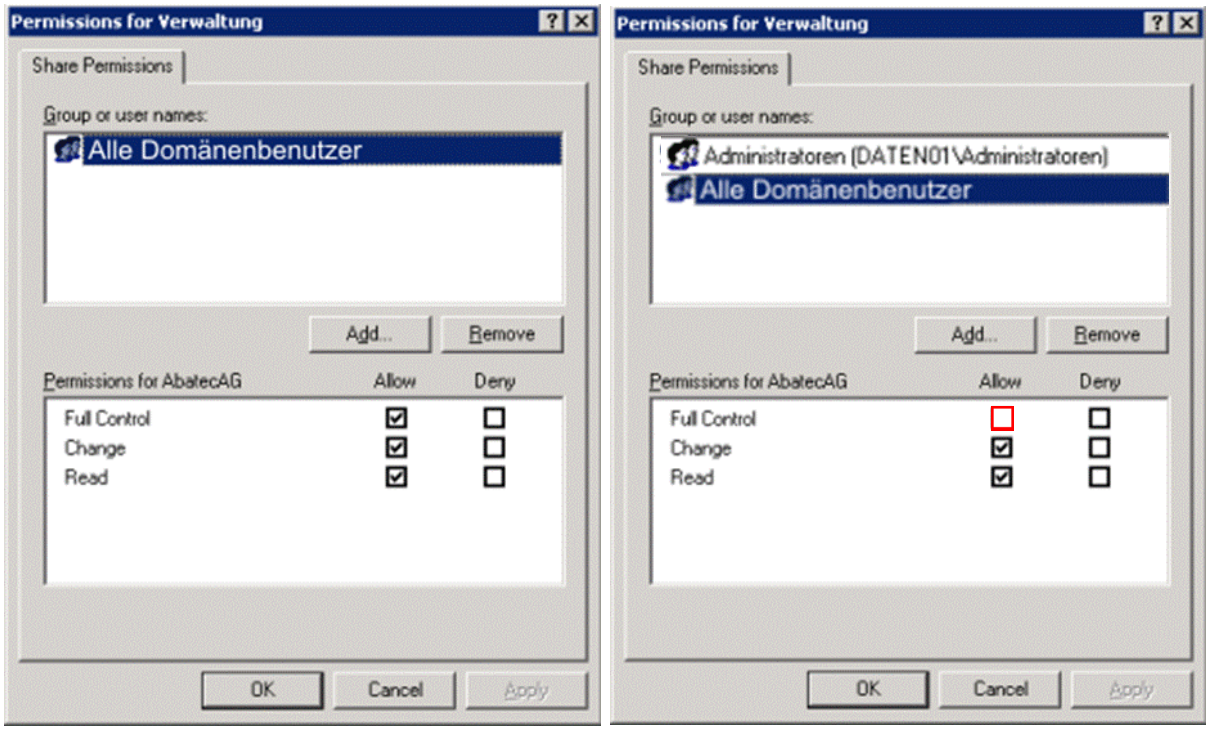



**Abbildung 13: Berechtigung auf Serverlaufwerke – Lösung**

#### *3.6.4.3 Netztransfer*

Das „Netztransfer-Laufwerk“, das unter dem Kapitel 3.3.4.3 beschrieben wird, ist zu entfernen. Ein Datenaustausch darf nur mehr über die regulären Verzeichnisberechtigungen am Datenserver möglich sein.
Der IT-Mitarbeiter/Administrator kann immer noch die administrativen Laufwerksfreigaben der Festplatten nutzen, um auf die Festplatte eines Systems zugreifen zu können. Ein Datenaustausch sollte aber nur über die regulären Verzeichnisberechtigungen am Datenserver erfolgen.

### 3.6.5 Bauliche und infrastrukturelle Mängel

#### *3.6.5.1 Schützenswerte Gebäudeteile*

Schützenswerte Räume oder Gebäudeteile dürfen nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein. Insbesondere ist zu beachten:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoss sind durch Vandalismus und Einbruch gefährdet.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.
- Serverräume sollen versperrbar und zentral angeordnet sein.

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.
Das Firmengebäude steht bereits, es kann daher nicht mehr Rücksicht in Bezug auf die Planung des Gebäudes genommen werden (INF 1.1). Die Anordnung von schützenswerten Gebäudeteilen ist ebenfalls nur mehr zur Kenntnis zu nehmen, weil die einzelnen Räume schon bestehen und auch der Neubau fertig geplant ist (INF 1.2). Es sind alle Anforderungen der beiden angeführten Richtlinien aus dem ÖSHB erfüllt. Auf detaillierte Maßnahmen wird nicht weiter eingegangen, da nach erfolgter geringer Risikoeinschätzung dieser Punkt nicht weiter betrachtet wird.
Idealerweise ist der Serverraum aussen mit einem Türknopf gesichert, ein Zugang soll nur mit einem speziellen Schlüssel möglich sein, den nur die Firmenleitung und die IT-Mitarbeiter haben. Es existieren zwei baulich getrennte Serverräume in zwei

aneinanderliegenden Gebäuden. Die Ausstattung der Serverräume ist unter 4.2.1 beschrieben.

Maßnahmen für Serverräume aus dem ÖSHB lauten wie folgt:

| ***INF 5.2*** | ***Geeignete Aufstellung eines Servers*** | ***ÖSHB Seite 111*** |
|---|---|---|
| *Um Vertraulichkeit, Integrität und Verfügbarkeit im Betrieb von Servern sicherzustellen, ist es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen. Diese kann realisiert werden als:*<br>• *Serverraum: Raum zur Unterbringung von Servern sowie weiterer Hardware. Im Serverraum ist im Allgemeinen kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten*<br>• *Serverschrank, wenn kein separater Serverraum zur Verfügung steht. Sie dienen zur Unterbringung von IT-Geräten und sollen den Inhalt gegen unbefugten Zugriff, Feuer und schädigenden Stoffen schützen.* | | |

| ***INF 5.6*** | ***Serverräume*** | ***ÖSHB Seite 113*** |
|---|---|---|
| *Für Serverräume sollten folgende Maßnahmen besonders beachtet werden:*<br>• *INF 1.4 Zutrittskontrolle*<br>• *INF 2.2 Raumbelegung unter Berücksichtigung von Brandlasten*<br>• *INF 2.8 Handfeuerlöscher*<br>• *INF 2.11 Rauchverbot*<br>• *INF 3.2 Not-Aus-Schalter*<br>• *INF 3.4 Lokale unterbrechungsfreie Stromversorgung*<br>• *INF 3.6 Überspannungsschutz (Innerer Blitzschutz)*<br>• *INF 4.6 Vermeidung von wasserführenden Leitung*<br>• *INF 6.4 Geschlossene Fenster und Türen*<br>• *INF 6.5 Alarmanlage*<br>• *INF 6.6 Fernanzeige von Störungen*<br>• *INF 6.7 Klimatisierung*<br>• *PER 2.3 Beaufsichtigung oder Begleitung von Fremdpersonen* | | |

### *3.6.5.2 Zutrittskontrolle und Schlüsselverwaltung*

Der Zugang zum Firmengebäude soll nur mit Transponder oder Schlüssel möglich sein. Die Außentüren sollten mit einem Türknopf und keiner Klinke ausgestattet sein. Dadurch kann eine geschlossene, aber nicht versperrte Tür nur mit Transponder oder Schlüssel geöffnet werden. Für die Zugangstüren muss ein Schlüsselplan erstellt werden. Mitarbeiter sollten nur Zugang zu ihrem Tätigkeitsbereich haben.

Empfohlen wird, dass der Zugang nur mehr mit einem Transponder möglich ist und dieser Zugang auch mitprotokolliert wird.

Die defekte Schiebetür im Kellerbereich muss unbedingt repariert werden, damit sie nicht mehr durch Muskelkraft geöffnet werden kann.
Der zentrale Eingang (Besucher, Fremdpersonal, Lieferanten) muss immer durch einen Empfang besetzt. Die Empfangsmitarbeiter müssen im Umgang mit Fremdpersonal geschult sein. Es darf sich keine betriebsfremde Person ohne Genehmigung am Firmengelände aufhalten.

Ein Vorteil ist, dass der Hausmeister in einem Teil des Firmengebäudes wohnt, wodurch ein gewisser Abschreckungsgrad für Einbrecher gegeben ist.

Weitere Aspekte der Zutrittskontrolle bietet folgende Maßnahme aus dem ÖSHB:

| ***INF 1.4*** | ***Zutrittskontrolle*** | ***ÖSHB Seite 91*** |
|---|---|---|

*Das Zutrittskontrollkonzept legt die generellen Richtlinien für den Perimeter-, Gebäude- und Geräteschutz fest. Dazu gehören:*

- *Festlegung der Sicherheitszonen: Zu schützende Bereiche können etwa Grundstücke, Gebäude, Rechnerräume, Archive und die Haustechnik sein. Die einzelnen Bereiche können unterschiedliche Sicherheitsstufen aufweisen.*
- *Generelle Festlegung der Zutrittskontrollpolitik: Hier wird grundsätzlich festgelegt, welche Personengruppen Zutritt zu welchen Bereichen benötigen.*
- *Bestimmung eines Verantwortlichen für Zutrittskontrolle: Dieser vergibt die Zutrittsberechtigungen an die einzelnen Personen*
- *Definition von Zeitabhängigkeiten: Es ist zu klären, ob zeitliche Beschränkungen der Zutrittsrechte erforderlich sind. Solche Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit oder befristeter Zutritt bis zu einem fixierten Datum*
- *Festlegung der Zutrittskontrollmedien: Es ist festzulegen, ob die Identifikation bzw. die Authentisierung durch Überwachungspersonal oder durch automatische Identifikations- und Authentisierungssysteme wie Zugangscodes (Passwörter, PINs), Karten oder biometrische Methoden erfolgen soll*
- *Festlegung der Rechteprüfung: Im Zutrittskontrollkonzept ist festzulegen, wo, zu welchen Zeiten und unter welchen Randbedingungen eine Rechteprüfung erfolgen muss, sowie welche Aktionen bei versuchtem unerlaubten Zutritt zu setzen sind*
- *Festlegung der Beweissicherung: Hier ist zu bestimmen, welche Daten bei Zutritt zu und Verlassen von einem geschützten Bereich protokolliert werden. Dabei bedarf es einer sorgfältigen Abwägung zwischen den Sicherheitsinteressen des Systembetreibers und den Schutzinteressen der Privatsphäre des Einzelnen*
- *Behandlung von Ausnahmesituationen: Es ist u.a. sicherzustellen, dass im Brandfall die Mitarbeiter schnellstmöglich die gefährdeten Zonen verlassen können*

### 3.6.5.3 Brandschutz

Beide Serverräume sind durch geeignete Brandschutzmaßnahmen weitgehend brandsicher ausgestattet.
Von der Lagerung der Sicherungsmedien im Serverraum muss abgesehen werden.

Für den Brandschutz sind einige Maßnahmen aus dem ÖSHB vorgesehen, die hier nur mit dem Titel angeführt werden, da der Brandschutz nach erfolgter geringer Risikoeinschätzung nicht weiter betrachtet wird:

| | | |
|---|---|---|
| ***INF 2.1*** | ***Einhaltung von Brandschutzvorschriften und Auflagen*** | ***ÖSHB Seite 95*** |
| ***INF 2.2*** | ***Raumbelegung unter Berücksichtigung von Brandlasten*** | ***ÖSHB Seite 96*** |
| ***INF 2.3*** | ***Organisation Brandschutz*** | ***ÖSHB Seite 96*** |
| ***INF 2.4*** | ***Brandabschottung von Trassen*** | ***ÖSHB Seite 96*** |
| ***INF 2.5*** | ***Verwendung von Brand- und Sicherheitstüren*** | ***ÖSHB Seite 97*** |
| ***INF 2.6*** | ***Brandmeldeanlagen*** | ***ÖSHB Seite 98*** |
| ***INF 2.7*** | ***Brandmelder*** | ***ÖSHB Seite 98*** |
| ***INF 2.8*** | ***Handfeuerlöscher*** | ***ÖSHB Seite 99*** |
| ***INF 2.9*** | ***Löschanlagen*** | ***ÖSHB Seite 99*** |
| ***INF 2.10*** | ***Brandschutzbegehungen*** | ***ÖSHB Seite 100*** |
| ***INF 2.11*** | ***Rauchverbot*** | ***ÖSHB Seite 101*** |
| ***INF 2.12*** | ***Rauchschutzvorkehrungen*** | ***ÖSHB Seite 101*** |

### 3.6.5.4 Stromversorgung

Die Stromversorgung ist weitgehend abgesichert und durch eine USV werden die Server bei Stromausfall sicher herunter gefahren. Es sollte aber ein automatisches Hochstarten der Server vorgesehen werden, damit dies nicht manuell erfolgen muss. Dies kann über eine Schnittstelle zur USV und geeigneter Software, die normalerweise mit einer USV geliefert wird, realisiert werden.
Eine Notstromversorgung für die gesamte IT ist nicht vorgesehen, da bei einem Stromausfall auch die Produktionsmaschinen nicht laufen und eine Notstromversorgung der ganzen Firma nicht ökonomisch vertretbar ist.

Für die Stromversorgung sind einige Maßnahmen aus dem ÖSHB vorgesehen, die hier nur mit dem Titel angeführt werden, da die Stromversorgung nach erfolgter geringer Risikoeinschätzung nicht weiter verfolgt wird:

| | | |
|---|---|---|
| ***INF 3.1*** | ***Angepasste Aufteilung der Stromkreise*** | ***ÖSHB Seite 101*** |
| ***INF 3.2*** | ***Not-Aus-Schalter*** | ***ÖSHB Seite 102*** |
| ***INF 3.3*** | ***Zentrale Notstromversorgung*** | ***ÖSHB Seite 102*** |
| ***INF 3.4*** | ***Lokale unterbrechungsfreie Stromversorgung*** | ***ÖSHB Seite 102*** |

### *3.6.5.5 Klimatechnik*

Um den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes manchmal nicht aus, so dass der Einbau einer Klimatisierung erforderlich wird. Deren Aufgabe ist es, die Raumtemperatur durch Kühlung unter dem von der IT vorgegebenen Höchstwert zu halten.

In beiden Serverräumen ist eine zweistufige Klimaanlage eingebaut, die von zwei unabhängigen Stromkreisen versorgt wird.

Eine Überwachung der Serverraumtemperatur ist notwendig, um einen Ausfall der Klimaanlage rechtzeitig erkennen zu können. Dies kann durch einen Sensor im Serverraum gewährleistet werden, der im Fehlerfall z.B. ein E-Mail an eine verantwortliche Person sendet und/oder Server kontrolliert herunter fahren lässt. Eine Beispiel einer solchen Anwendung findet man unter [BELLE].

Im ÖSHB ist folgende Maßnahme vorgesehen:

| | | |
|---|---|---|
| ***INF 6.7*** | ***Klimatisierung*** | ***ÖSHB Seite 118*** |
| *Klimaanlagen helfen den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten. Werden darüber hinaus Forderungen an die Luftfeuchtigkeit gestellt, kann ein Klimagerät durch Be- und Entfeuchtung auch diese erfüllen.*<br>*Dazu muss das Klimagerät allerdings an eine Wasserleitung angeschlossen werden. (INF 4.6 „Vermeidung von wasserführenden Leitungen“). Die Luftumwälzung durch eine Klimaanlage kann auch Emissionen aus der Umgebung in die Nähe von empfindlichen IT-Komponenten bringen kann. So ist etwa bei baulichen Maßnahmen darauf zu achten, dass Kleber, Anstriche, etc. säurefrei sind, um eine Korrosion von IT-Bauteilen durch vorbeigeführte Luft aus der Klimaanlage zu vermeiden.* | | |

## 3.7 Maßnahmenkatalog: Verhalten der Mitarbeiter

### 3.7.1 Regelungen für Mitarbeiter

Die wichtigste personelle Maßnahme ist die Schulung der Mitarbeiter, um sie in den Fragen der IT-Sicherheit zu sensibilisieren. In kleinen Gruppen (ca. 10 Personen) sollen die Mitarbeiter ihrem Tätigkeitsbereich entsprechend mit den Fragen der IT-Sicherheit vertraut gemacht werden.

Die Schulung sollte die folgenden Themengebiete umfassen:

- Social Engineering (siehe Kapitel 3.7.4)
- Umgang mit Personendaten
- clear desk / clear screen
- Umgang mit Passwörtern
- Verhalten im Internet
- Risiken durch mobile (private) Datenträger
- Verfahren für die Aufnahme und das Ausscheiden von Mitarbeitern
- Umgang mit betriebsfremden Personen
- IT-Richtlinie für Mitarbeiter

Im Zuge dieser Schulung muss auch die *IT-Sicherheitsrichtlinie für Mitarbeiter* (Kapitel 5.1) durchbesprochen werden, die für alle Mitarbeiter bindend ist. In dieser Richtlinie sind die wesentlichen Kapitel der Schulung dokumentiert. Nach der Klärung aller Fragen muss diese Richtlinie von den Mitarbeitern unterschrieben werden.

Die wichtigsten Maßnahmen aus dem ÖSHB sind:

| ***PER 1.1*** | ***Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*** | ***ÖSHB Seite 121*** |
|---|---|---|
| *Bei der Einstellung von Mitarbeitern sind diese zur Einhaltung einschlägiger Gesetze (z.B. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 i.d.g.F.) § 15 "Datengeheimnis", § 14 "Datensicherheitsmaßnahmen" und § 13 "Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland"), Vorschriften und interner Regelungen zu verpflichten. Damit sollen neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen zur IT-Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und gegenzeichnen zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur Einsichtnahme vorzuhalten.* | | |

| ***PER 1.7*** | ***Clear Desk Policy*** | ***ÖSHB Seite 124*** |
|---|---|---|
| *Jeder Mitarbeiter sollte vor seiner Abwesenheit seine Unterlagen und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank, PC und Telefon. Dies gilt insbesondere für Großraumbüros, aber auch in den anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (Besucher, Reinigungspersonal, unbefugte Mitarbeiter,...) Zugriff zu Schriftstücken, Datenträgern und IT-Komponenten haben.* | | |

| ***PER 1.9*** | ***Verpflichtung der PC-Benutzer zum Abmelden*** | ***ÖSHB Seite 125*** |
|---|---|---|
| *Der erforderliche Schutz mittels einer Zugriffskontrolle kann nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung bzw. bei Verlassen des Arbeitsplatzes am PC abmeldet. Ist es jemandem möglich, an einem PC unter der Identität eines Anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle PC-Benutzer zu verpflichten, sich bei Verlassen des Arbeitsplatzes abzumelden.* | | |

| ***SYS 5.1*** | ***Herausgabe einer PC-Richtlinie*** | ***ÖSHB Seite 188*** |
|---|---|---|

*Möglicher inhaltlicher Aufbau einer PC-Richtlinie:*

- *Zielsetzung und Begriffsdefinitionen: Dieser erste Teil der PC-Richtlinie soll dazu dienen, die PC-Anwender/innen für IT-Sicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert und eine einheitliche Sprachregelung geschaffen*
- *Geltungsbereich: In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die PC-Richtlinie gilt*
- *Rechtsvorschriften und interne Regelungen: Hier wird auf wichtige Rechtsvorschriften (z.B. das Datenschutzgesetz 2000 (DSG2000), BGBl. I Nr. 165/1999 i.d.g.F. und das Urheberrechtsgesetz, BGBl. Nr. 111/1936 i.d.g.F.) hingewiesen. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen*
- *Verantwortungsverteilung: In diesem Teil wird definiert, wer im Zusammenhang mit dem PC-Einsatz welche Verantwortung trägt. Dabei sind insbesondere die Funktionen IT-Benutzer, Vorgesetzte, PC-Administratoren, Datenschutz-/IT-Sicherheitsbeauftragte, Bereichs-IT-Sicherheitsbeauftragte und Applikations-/Projektverantwortliche zu unterscheiden*
- *Umzusetzende und einzuhaltende IT-Sicherheitsmaßnahmen: Im letzten Teil der PC-Richtlinie ist festzulegen, welche IT-Sicherheitsmaßnahmen von dem IT-Benutzer einzuhalten bzw. umzusetzen sind. Es kann je nach Schutzbedarf auch über die IT-Grundschutzmaßnahmen hinausgehen*

*Die PC-Richtlinie muss regelmäßig – insbesondere im Hinblick auf die IT-Sicherheitsmaßnahmen – aktualisiert werden. Es ist dafür Sorge zu tragen, dass jeder PC-Benutzer ein Exemplar dieser Richtlinie besitzt und dass die Einhaltung regelmäßig überprüft wird.*

### 3.7.2 Regelungen für Fremdpersonal

Mitarbeiter müssen im Umgang mit betriebsfremdem Personal geschult werden.

Für den Umgang mit Fremdpersonal sind folgende Maßnahmen aus dem ÖSHB umzusetzen:

| ***PER 2.1*** | ***Regelungen für den kurzfristigen Einsatz von Fremdpersonal*** | ***ÖSHB Seite 126*** |
|---|---|---|
| *Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, d.h. dass also etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeitern der Behörde bzw. des Unternehmens erlaubt ist etc. (vgl. dazu etwa INF 1.6 Portierdienst).* | | |

| ***PER 2.2*** | ***Verpflichtung externer Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*** | ***ÖSHB Seite 126*** |
|---|---|---|
| *Externe Mitarbeiter, die über einen längeren Zeitraum in einer oder für eine Organisation tätig sind und ev. Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind ebenfalls schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.* | | |

| ***PER 2.3*** | ***Beaufsichtigung oder Begleitung von Fremdpersonal*** | ***ÖSHB Seite 126*** |
|---|---|---|
| *Fremde (Besucher, Handwerker, Wartungs- und Reinigungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch INF 1.4 Zutrittskontrolle und INF 1.6 Portierdienst). Wird es erforderlich, einen Fremden allein im Büro zurückzulassen, sollte man einen Kollegen ins Zimmer oder den Besucher zu einem Kollegen bitten.* | | |

| ***PER 2.4*** | ***Information externer Mitarbeiter über die IT-Sicherheitspolitik*** | ***ÖSHB Seite 127*** |
|---|---|---|
| *Externe Mitarbeiter sind - so weit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist - über hausinterne Regelungen und Vorschriften zur IT-Sicherheit sowie die organisationsweite IT-Sicherheitspolitik zu unterrichten* | | |

### 3.7.3 Ausscheiden von Mitarbeitern

Beim Ausscheiden von Mitarbeitern müssen mehrere Maßnahmen gesetzt werden.

Einen guten Anhaltspunkt bietet die folgende Maßnahme aus dem ÖSHB:

| ***PER 1.4*** | ***Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*** | ***ÖSHB Seite 123*** |
|---|---|---|
| • *Vor dem Ausscheiden ist eine Einweisung des Nachfolgers durchzuführen*<br>• *Von dem Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise einzuziehen*<br>• *Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z.B. mittels eines gemeinsamen Passwortes), so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern*<br>• *Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine im Rahmen der Tätigkeit erhaltenen Informationen weitergegeben werden dürfen*<br>• *Nach Möglichkeit sollte eine Neuvergabe der User-ID an einen anderen Mitarbeiter vermieden/ausgeschlossen werden*<br>• *Ist die ausscheidende Person ein Funktionsträger in einem Notlaufplan, so ist der Notlaufplan zu aktualisieren*<br>• *Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Portierdienst, sind über das Ausscheiden des Mitarbeiters zu unterrichten*<br>• *Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren*<br>• *Optional kann sogar für den Zeitraum zwischen Aussprechen der Kündigung und dem Ausscheiden der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden*<br>• *Als ein praktikables Hilfsmittel haben sich Laufzettel erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen des Unternehmens zu erledigen hat* | | |

### 3.7.4 Social Engineering

Social Engineering ist ein wichtiger Teil der Regelungen für Mitarbeiter und wurde auch extra bewertet (vgl. Kapitel 3.4.5.4), darum wird dieses Thema in einem eigenen Kapitel angeführt.

Die Mitarbeiter müssen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten bekannt gegeben werden. Da Social Engineering oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten Mitarbeiter regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

Die Sensibilisierung der Mitarbeiter kann auch mit Hilfe der Maßnahme aus dem ÖSHB verstärkt werden:

| ***PER 3.3*** | ***Schulung und Sensibilisierung zu IT-Sicherheitsmaßnahmen*** | ***ÖSHB Seite 128*** |
|---|---|---|
| • *Sensibilisierung für IT-Sicherheit*<br>• *Die mitarbeiterbezogenen IT-Sicherheitsmaßnahmen*<br>• *Die produktbezogenen IT-Sicherheitsmaßnahmen*<br>• *Das Verhalten bei Auftreten eines Virus auf einem PC*<br>• *Der richtige Einsatz von Zugangscodes und Zugangskontrollmedien*<br>• *Die Bedeutung der Datensicherung und deren Durchführung*<br>• *Der geregelte Ablauf eines Datenträgeraustausches*<br>• *Der Umgang mit personenbezogenen Daten*<br>• *Die Einweisung in Notfallmaßnahmen*<br>• *Richtiges Verhalten bei Auftreten von Sicherheitsproblemen (IHP)*<br>• *Vorbeugung gegen Social Engineering* | | |

Weiterführende Informationen zu Social Engineering findet man auch unter [SICK05].

## 3.8 Maßnahmenkatalog: Richtlinien

IT-Sicherheitsrichtlinien und Notfallpläne sind wichtige Werkzeuge für die Gewährleistung des IT-Grundschutzes. Sie bilden eine wesentliche Grundlage einer unternehmensweiten Informationssicherheitspolitik. Die IT-Sicherheitsrichtlinien beschreiben Abläufe und Verhaltensweisen, um mögliche Sicherheitsrisiken zu erkennen und sich davor zu schützen. Notfallpläne werden eingesetzt, um im Bedarfsfall die richtigen Schritte für eine Ausschaltung von Bedrohungen und Systemausfällen bereit zu haben.
Die Erstellung und Wartung dieser Richtlinien und Pläne ist sehr zeitintensiv, daher sollten nur unbedingt notwendige Informationen in einer Richtlinie festgehalten werden. IT-Sicherheitsrichtlinien können dennoch sehr umfassend sein, die Richtlinien sollen aber leicht gelesen und verstanden werden können. Notfallpläne dokumentieren für einen Anlassfall (Ausfall von Hardware, Daten werden gelöscht, Virenbefall,…) genaue Abläufe, wie der entstandene Schaden (Datenverlust,…) gering gehalten oder behoben werden kann.
IT-Sicherheitsrichtlinien und Notfallpläne sollten nicht nur am Serverlaufwerk gespeichert werden, sondern auch noch in ausgedruckter Form vorliegen, damit sie im Bedarfsfall (Ausfall der IT) griffbereit sind.
Die notwendigen IT-Sicherheitsrichtlinien und Notfallpläne werden in dieser Arbeit anonymisiert erstellt, firmenspezifische Eigenheiten werden entfernt. Die erstellten Richtlinien und Notfallpläne befinden sich im Anhang der Masterarbeit (Kapitel 5).

Folgende Richtlinien und Notfallpläne wurden ausgearbeitet:

- IT-Sicherheitsrichtlinie für Mitarbeiter (Kapitel 5.1)
- Richtlinie Datensicherung (Kapitel 5.2)
- Richtlinie Datenschutz (Kapitel 5.3)
- Notfallplan Datenwiederherstellung (Kapitel 5.4)

Die Richtlinien müssen regelmässig aktualisiert werden. Diese Aufgabe obliegt dem IT-Leiter.

## 3.9 Maßnahmen und Empfehlungen an das Management

Die Hauptaufgabe für das Management ist es, eine unternehmensweite Informationssicherheitspolitik zu entwerfen und auch zu kommunizieren (z.B. das Verbot von USB-Sticks oder von privatem E-Mail-Verkehr in der Arbeitszeit muss vom Management ausgesprochen werden).

Der IT-Leiter muss vom Management (Firmenleitung) unterstützt werden, damit er die ausgewählten Maßnahmen auch umgesetzen kann. Es müssen Zeit, Geld und Ressourcen für die so notwendigen Schulungen der Mitarbeiter zur Verfügung stehen.

Aufgabe des Managements ist es auch, einen IT-Sicherheitsbeauftragten zu rekrutieren.

Ein wesentlicher Punkt zum Schluss ist, auch Zeit für die Weiterentwicklung der IT-Sicherheit zur Verfügung zu stellen, um als IT-Leiter nicht nur auf Sicherheitsprobleme reagieren zu müssen.

# 4 ERWEITERUNG DER IT-INFRASTRUKTUR

## 4.1 Allgemeines

Im Zuge der Ermittelungen für diese Masterarbeit in der Elektronikfirma wurde auch der Ist-Zustandes der IT-Infrastruktur erhoben. Die Ermittlung ergab, dass die IT-Infrastruktur „aus allen Nähten platzt“, was schon ein Blick in den Serverraum verriet. Dieser Zustand hatte mehrfache Gründe:

Die Firma erfuhr in den letzten Jahren einen enormen Zuwachs an Mitarbeitern und damit verbunden auch mehr Arbeitsstationen und Server. Das Firmengebäude wurde erweitert, der Serverraum blieb aber immer gleich groß und die Anzahl der Netzwerkkabel wurde immer mehr. Auch die Telefonanlage ist im Serverraum untergebracht. So war es der Wunsch der Firmenleitung und vor allem des IT-Leiters, die bestehende IT-Infrastruktur im Zuge dieser Masterarbeit zu erweitern. Die Erweiterung der IT-Infrastruktur war auch für die Einführung des Sicherheitsstandards wichtig, da mit der bestehenden IT-Infrastruktur über längere Sicht kein sicherer Betrieb mehr möglich gewesen wäre, wie aus der Ist-Analyse im Kapitel 4.2 ersichtlich wird.

Die Erweiterung der IT-Infrastruktur wird folgendermaßen durchgeführt:

Zuerst wird der Ist-Zustand der IT-Infrastruktur erhoben. Die Anzahl der Arbeitsstationen, Drucker, Netzwerkdosen, Server, Switch und die Verkabelung werden dokumentiert. Weiters werden die Struktur des Active Directory (Benutzerverwaltung, Gruppenkonzept,…) und die Verteilung der IP-Adressen dokumentiert. Es folgt nun die Planungphase. Der Ausbau des Firmengebäudes und die notwendige Erweiterung der IT wird in die Planung mit eingebracht. Die IP-Adressbereiche werden erweitert, um genügend IP-Adressen zur Verfügung zu haben. Es folgt die Planung der Netzwerkkomponenten. Eine Glasfaserverbindung zwischen den Serverräumen soll mit einer Geschwindigkeit von 10Gbit/s betrieben werden. Schlussendlich soll die geplante IT-Infrastruktur in Betrieb genommen werden, ohne den laufenden Betrieb zu stören.

Die folgenden Kapitel beschreiben den Ablauf bei der Erweiterung.

## 4.2 Ist-Zustand der IT-Infrastruktur

Dieses Kapitel beschreibt den Ist-Zustand der IT vor den Erweiterungsmaßnahmen.

### 4.2.1 Serverraum

Es gibt einen Serverraum im 1.Stock des Firmengebäudes. Er ist mit zwei 19 Zoll Schränken ausgestattet, worin sich einerseits die Patchpanele und die Switches und andererseits die Einbauserver befinden. Die beiden Schränke sind durch die Vielzahl an nachverdrahteten Netzwerkanschlüssen so überfüllt, dass zwei Stück 24-Port Patchpanele gar nicht mehr eingebaut werden konnten, sondern seitlich an den Schränken mit Kabelbindern befestigt sind. Die eingebauten Switches sind voll ausgelastet und nur noch vereinzelte Ports sind verfügbar. Die Patchkabel sind quer über beide Serverschränke gespannt, sodass keine Komponenten (Switch, Server, Patchpanel,…) mehr aus- oder eingebaut werden können, ohne eine Vielzahl dieser Patchkabel ausstecken zu müssen. Die Patchkabel folgen keiner farblichen Trennung, es wurden jene Patchkabel verwendet, die der Länge nach passen, daher kann auch keine Unterscheidung nach der Farbe der Patchkabel auf die Funktion des angeschlossenen Gerätes getroffen werden. Will man hier einer Verbindung zwischen Patchpanel, Switch und Server auf den Grund gehen, muss man schon Geduld aufbringen.
Durch die geplante und bereits begonnene Erweiterung des Firmengebäudes und der geplante zweite Serverraum werden die bestehenden Büros wieder entlastet. Dadurch sinkt die notwendige Anzahl der Netzwerkanschlüsse im bestehenden Serverraum, wodurch eine Erweiterung der Serverschränke nicht notwendig ist.

### 4.2.2 Gebäudeplan und -verkabelung

Das Firmengebäude verfügt über ein Hauptgebäude für Verwaltung und Entwicklung und eine Produktionshalle. Beide Gebäude sind mit einem Glasfaserkabel miteinander verbunden. In der Produktionshalle befindet sich ein Verteilerschrank, in dem sich auch ein Switch und die Patchpanele der Netzwerkdosen der Produktion befinden. Im Hauptgebäude befindet sich der Serverraum im 1.Stock.
Der bereits geplante und begonnene Ausbau des Firmengebäudes bringt ein neues Produktions- und Entwicklungsgebäude. Es sind ein zweiter Serverraum im 2.Stock und ein Verteilerraum im 1.Stock eingeplant. Es konnte in die Planung noch soweit eingegriffen werden, dass eine Klimatisierung in den neuen Serverraum eingebaut

wird. Dieses neue Gebäude wird ebenfalls mit einer Glasfaserverbindung an die bestehenden Gebäude angebunden. Die neuen Glasfaserverbindungen dürfen bei dem verwendeten Kabel eine Länge von 110m nicht übersteigen, um eine Geschwindigkeit von 10GBit/s zu ermöglichen.

Die folgende Grafik zeigt schematisch die Gebäude und die Glasfaserverbindungen:

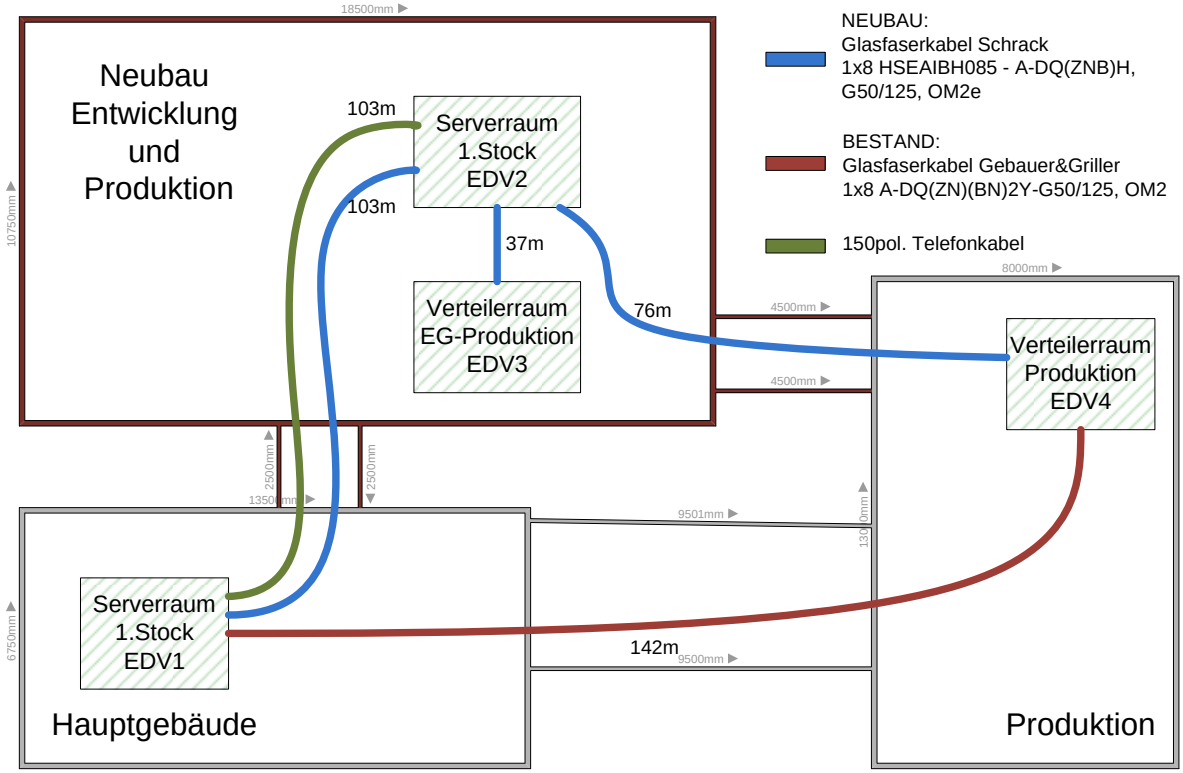



**Abbildung 14: Gebäudeplan**

Durch die kreisförmige Anordnung der Glasfaserleitungen gibt es mehr Möglichkeiten, die einzelnen Verteiler- und Serverräume zu verbinden und diese Redundanz erhöht die Ausfallsicherheit der Backbone-Glasfaserverkabelung. Zusätzlich wurde noch ein 150-poliges Telefonkabel zwischen den Serverräumen verlegt, um die Telefone betreiben zu können. Die Gebäudeverkabelungen sind beiderseits an ein Patchpanel aufgelegt.

Die Patchpanele der Glasfaserleitungen sind mit SC-Steckern ausgestattet.


[GFI-SC]

### 4.2.3 Switchlandschaft

Im Serverraum im Hauptgebäude (EDV1) sind zwei Switches eingebaut. Es sind dies ein „HP ProCurve 5406zl“ und ein „HP ProCurve 4000m“. Durch den Wildwuchs bei der Patchverkabelung können nur vereinzelt freie Switchports entdeckt werden. Die beiden Switches sind mit 1GBit/s über einen Switchport miteinander verbunden.

In der Produktion (EDV4) ist ein nicht managebarer Switch eingesetzt, der über einen LWL-Port über die Glasfaserleitung mit dem Serverraum verbunden ist.

Die folgende Abbildung zeigt die derzeitige Switchlandschaft. Die einzelnen Module der Switches sind angeführt, daraus kann die Anzahl der Switchports errechnet werden.

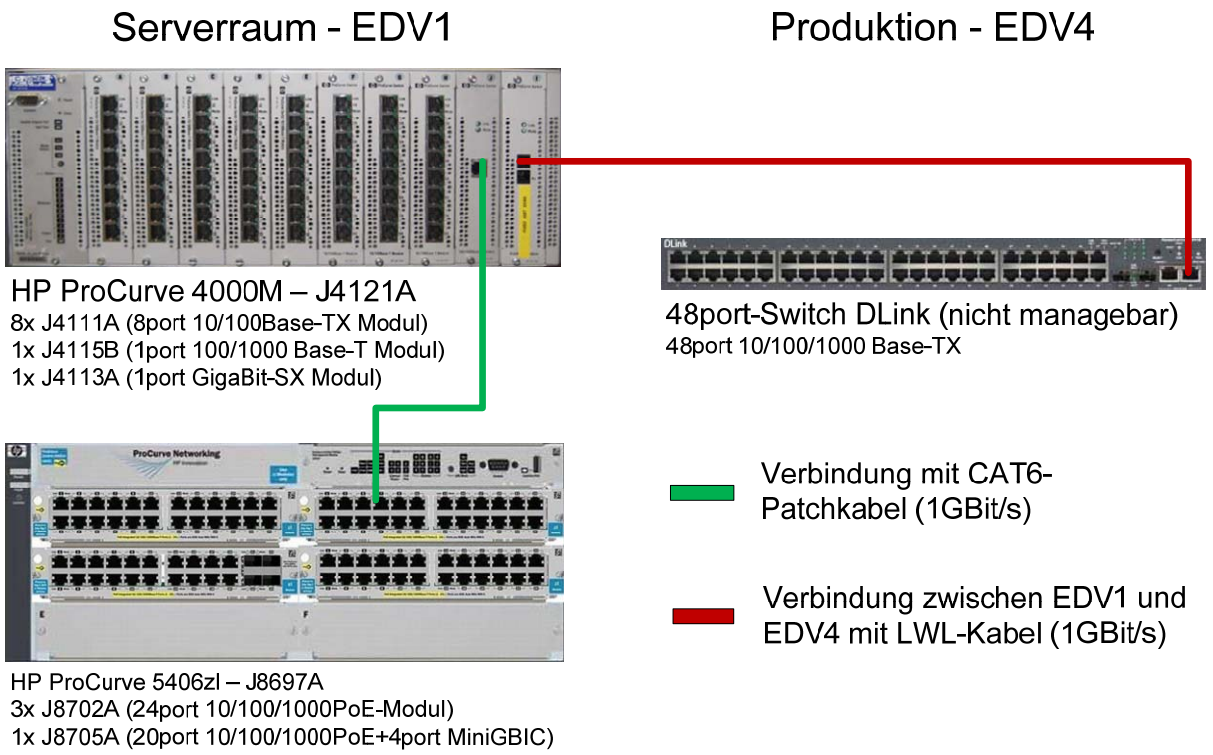



**Abbildung 15: Switchlandschaft alt**

Folgende Anzahl an Switchports ist verfügbar (LWL-Ports ausgenommen):

- 64 Ports 10/100Base-TX
- 93 Ports 10/100/1000Base-T im Hauptgebäude
- 48 Ports 10/100/1000Base-T in der Produktion

### 4.2.4 Server

Die IT-Infrastruktur der Firma enthält viele Serversysteme. Von diesen Serversystemen sind meist alle im Serverraum im Hauptgebäude (EDV1) im Serverschrank als 19 Zoll Einbauserver ausgeführt. Die Anzahl der Server ergibt sich einerseits durch das Wachstum der Firma sowie durch die Übernahme mehrerer Firmen, deren IT-Infrastruktur (hauptsächlich Server) übernommen werden und direkt in das eigene Firmennetz integriert werden. Einige Server sind nur mehr in geringem Maße in Verwendung (CRM01, TERM02, DATEN03). Die notwendigen Anwendungen dieser Server sollten auf bestehende Server verteilt werden. Auf dem Server COMM01 läuft der Microsoft Exchange-Server (Email-Verwaltung). Gleichzeitig ist dieser Server auch Domain Controller (DC). Diese Kombination sollte aus Sicherheitsgründen vermieden werden, sinnvoll wäre ein eigener Server für die Email-Verwaltung.

**Bei der Vielzahl der Server sollte auch über Virtualisierungstechniken nachgedacht werden!** Auf Virtualisierung wird aber nicht eingegangen, da dies eine umfangreiche Planung erfordert und die bestehende Server-Infrastruktur obsolet machen würde (dies wäre eine gesonderte Empfehlung).

Die folgende Abbildung zeigt die vorhandenen Server und die Verbindung zum Internet über die Firewall. Auf die Angabe von IP-Adressen wird hier verzichtet.

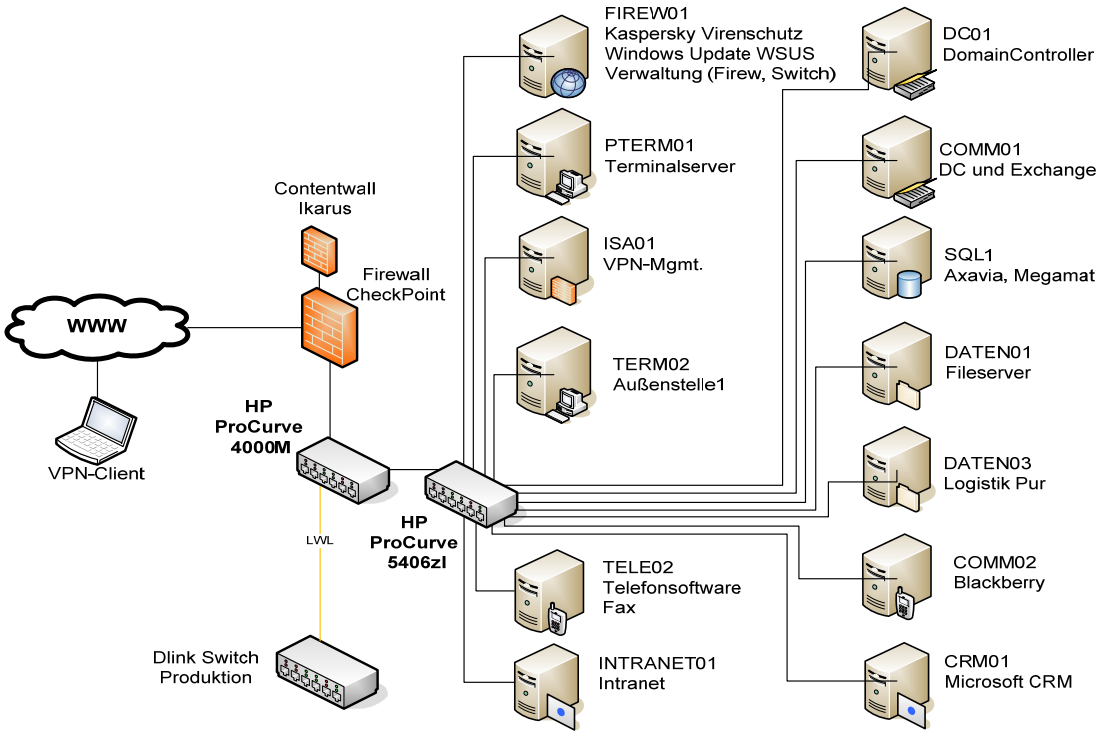



**Abbildung 16: Server Istzustand**

### 4.2.5 DHCP-Server und IP-Adressen

Der interne IP-Adressbereich der gesamten Firma ist auf eine Klasse-C-Adresse (`192.168.100.0/24`) begrenzt. Die IP-Adressen werden statisch und per DHCP-Server vergeben [RFC2131]. Statische Adressen werden für Server, Switches, Netzwerkdrucker, Produktionsmaschinen, Firewall und Telefonanlage vergeben. Arbeitsstationen bekommen durch den DHCP-Server ihre IP-Adresse zugewiesen, wobei hier zwischen zwei Gruppen unterschieden werden muss:

- Arbeitsstationen mit Internetzugang
- Arbeitsstationen, bei denen der Internetzugang gesperrt ist (z.B. Produktion)

Arbeitsstationen mit Internetzugang erhalten eine freie IP-Adresse aus dem verfügbaren Adressbereich. Die Internet-Sperre der anderen Arbeitsstationen wird durch eine Firewallregel (noInet) auf der Firewall gelöst, die bestimmten IP-Adressen (gesperrte IPs) den Zugang zum Internet sperrt. Hat eine Arbeitsstation eine solche gesperrte IP-Adresse, wird diese Firewallregel angewendet. Damit dies funktioniert, sind am DHCP-Server Reservierungen angelegt. Die MAC-Adressen der Netzwerkkarten in jenen Arbeitsstationen, denen der Zugang zum Internet verweigert werden soll, werden durch eine Reservierung mit einer fixen IP-Adresse gebunden. Diese IP-Adresse ist aus dem Bereich der gesperrten IPs. Die IP-Adressen sind mit der Zeit knapp geworden, sodass die Reihung in verschiedene Gruppen (1.Server, 2.Switches, 3.Netzwerkdrucker, 4.Produktionsmaschinen, usw.) nicht mehr möglich war und daher ein bunter Mix in der IP-Adressliste entstanden ist. Dieser Aspekt macht die IP-Adressliste unübersichtlich.

In der folgenden Tabelle ist ein kleiner Auszug aus der IP-Adressliste zu sehen:

| | | |
|---|---|---|
| DC01 | 192.168.100.1 | Domaincontroller1 |
| Tele02 | 192.168.100.4 | Server Telefonie, Fax |
| Server CRM | 192.168.100.6 | CRM01 + SQL 2000 |
| HP 9200C | 192.168.100.9 | Dokumentenscanner Verwaltung |
| Firew01 | 192.168.100.12 | Firewall-Konsole, Medien-Server |
| Comm02 | 192.168.100.14 | Server für Telefonie, Blackberry |
| Daten01 | 192.168.100.16 | Server Daten01, Daten |
| HP Scanjet 7650 | 192.168.100.19 | Netzwerkscanner Entwicklung |
| SMD neu | 192.168.100.20 | Produktionsmaschine 1 |
| Telefonanlage | 192.168.100.40 | Telefonanlage |
| Intranet01 | 192.168.100.50 | Server für das Intranet |
| pc-noInet01 | 192.168.100.199 | PC mit gesperrtem Internetzugang |
| HP Switch | 192.168.100.250 | HP ProCurve 4000M |
| HP Switch | 192.168.100.252 | HP ProCurve 5406zl |
| Gateway | 192.168.100.254 | Netzwerk Gateway |

**Tabelle 4: IP-Adressen Istzustand**

## 4.3 Erweiterung des IP-Adressbereiches

Der IP-Adressbereich ist für die Anzahl der Systeme zu klein geworden, es ist auch keine Gruppierung der einzelnen Systemgruppen mehr möglich, dadurch wird der IP-Adressbereich unübersichtlich. Als erster Schritt werden der interne IP-Adressbereich erweitert und die IP-Adressen in Gruppen eingeteilt, dann wird der neue Adressbereich im laufenden Betrieb umgestellt. Die Umstellung erfolgt einerseits durch die Konfiguration des DHCP-Servers und andererseits durch die manuelle Umkonfiguration der statisch eingestellten Systeme.

### 4.3.1 Änderung des IP-Adressbereichs

Die Änderung des IP-Adressbereichs ist eine notwendige Maßnahme, da durch die Verwendung einer einfachen C-Klasse-Adresse die nutzbaren IP-Adressen auf einen Bereich von `192.168.100.0` bis `192.168.100.255` begrenzt sind. Die maximal möglichen IP-Adressen ergeben sich daher wie folgt:

Hosts im Netz: $2^8-2 = 254$

Der IP-Adressbereich wird durch die Änderung der Subnetzmaske von `255.255.255.0 (/24)` auf `255.255.252.0 (/22)` vergrößert. Die Verwendung dieser Netzmaske (Subnetmask) ist seit der Einführung von Classless Interdomain Routing (CIDR) möglich, da dadurch die feste Zuordnung einer IP-Adresse zu einer Netzklasse fällt. [RFC1519]

Es ergibt sich dadurch folgender neuer Adressbereich:

`192.168.100.0` bis `192.168.103.255`

Die Änderung der Netzmaske ist die einfachste Variante, um während des laufenden Betriebs die IP-Adressen schrittweise zu erweitern. Es ergeben sich dadurch **1022** mögliche IP-Adressen, was für die nächste Zukunft ausreichend erscheint:

```
Addresse:  192.168.100.0   11000000.10101000.01100100.00000000
Netzmaske: 255.255.252.0   11111111.11111111.11111100.00000000
Netzwerk: 192.168.100.0/22 11000000.10101000.01100100.00000000
MinHost:   192.168.100.1   11000000.10101000.01100100.00000001
MaxHost:   192.168.103.254 11000000.10101000.01100111.11111110
Broadcast: 192.168.103.255 11000000.10101000.01100111.11111111
Hosts im Netz: 2^10-2 = 1022
```

Sollte dieser Adressbereich wieder zu klein werden, kann der Adressbereich nach der gleichen Vorgangsweise wieder erweitert werden.

### 4.3.2 Gruppierung der Systeme

Die IP-Adressen werden entweder statisch durch fixe Einstellung oder dynamisch durch einen DHCP-Server vergeben. Die statisch vergebenen IP-Adressen werden in einer IP-Tabelle verwaltet. Für die Übersichtlichkeit in der IP-Tabelle und die Vergabe der IP-Adressen ist eine Einteilung in verschiedene Gruppen (Server, Switches, Netzwerkdrucker, Produktionsmaschinen, usw.) sinnvoll. Bei der Einteilung der Gruppen muss die voraussichtliche Anzahl der in den Gruppen befindlichen Systeme abgeschätzt werden. In dieser IP-Tabelle sollten auch die dynamisch vergebenen Bereiche angegeben werden.
Die Gruppierung wurde folgendermaßen festgelegt:

| Art | von IP | Bis IP | Beschreibung | Anzahl |
|---|---|---|---|---|
| Server | 192.168.100.1 | 192.168.100.29 | Server, Netzwerkspeicher | 29 |
| Management | 192.168.100.30 | 192.168.100.59 | Managementports der Server | 30 |
| Maschinen | 192.168.100.60 | 192.168.100.99 | Produktionsmaschinen, Telefon | 40 |
| Drucker | 192.168.100.100 | 192.168.100.179 | Drucker, Scanner | 80 |
| Switches | 192.168.100.180 | 192.168.100.219 | Switch, Router, Wireless | 40 |
| frei | 192.168.100.220 | 192.168.100.249 | derzeit nicht belegt | 30 |
| Gateway | 192.168.100.250 | 192.168.100.255 | Gateway, ISA-Server | 6 |
| Test | 192.168.101.0 | 192.168.101.49 | Testzwecke | 50 |
| DHCP | 192.168.101.50 | 192.168.102.199 | DHCP-Bereich | 406 |
| frei | 192.168.102.200 | 192.168.102.255 | derzeit nicht belegt | 56 |
| Test | 192.168.103.0 | 192.168.103.49 | Testzwecke | 50 |
| DHCP-noInet | 192.168.103.50 | 192.168.103.199 | DHCP-Bereich für noInet-PCs | 150 |
| frei | 192.168.103.200 | 192.168.103.254 | derzeit nicht belegt | 55 |
| Broadcast | 192.168.103.255 | | Broadcastadresse des Netzwerks | 1 |

**Tabelle 5: Gruppierung der IP-Adressen**

Bei der Gruppierung wurden einzelne Bereiche frei gelassen, da derzeit die festgelegten Adressbereiche genügend freie IP-Adressen bereit halten. Eine Erweiterung eines Gruppierungsbereichs oder die Einführung einer neuen Gruppe ist dann durch Nutzung eines freien Bereichs möglich. Die Testbereiche sind für Versuchsaufbauten reserviert und können nach Absprache mit der IT-Abteilung frei verwendet werden. Durch die Aufstellung sind nun **406** Adressen für den DHCP-Bereich und **150** Adressen für den DHCP-noInet-Bereich verfügbar. Der DHCP-noInet-Bereich ist für Systeme, bei denen der Internetzugang gesperrt ist. Die Vergabe dieser Adressen erfolgt ebenfalls durch einen DHCP-Server.

Der folgende Auszug aus der IP-Tabelle soll einen Überblick über die vergebenen IP-Adressen geben und auch ein Bespiel zeigen, wie diese IP-Adressen in einer Tabelle gelistet werden.

| Systemname | IP-Adresse | Subnetmaske | Beschreibung |
|---|---|---|---|
| **Server** | **192.168.100.1** | **192.168.100.29** | **Server, Netzwerkspeicher** |
| DC01 | 192.168.100.1 | 255.255.252.0 | Domaincontroller |
| TELE02 | 192.168.100.4 | 255.255.252.0 | Server Telefonie, Fax |
| TERM01 | 192.168.100.7 | 255.255.252.0 | Terminalserver |
| **Management** | **192.168.100.30** | **192.168.100.59** | **Managementports der Server** |
| USV | 192.168.100.30 | 255.255.252.0 | Managementport - USV |
| daten01-rmm | 192.168.100.31 | 255.255.252.0 | Managementport - Daten01 |
| **Maschinen** | **192.168.100.60** | **192.168.100.99** | **Produktionsmaschinen, Telefon** |
| Telefon | 192.168.100.60 | 255.255.252.0 | Telefonanlage |
| PLK1602A | 192.168.100.63 | 255.255.252.0 | Siemens-Rechner SMD-Maschine |
| **Drucker** | **192.168.100.100** | **192.168.100.179** | **Drucker, Scanner** |
| HP2025 | 192.168.100.106 | 255.255.252.0 | HP2025, Color LaserJet A4, Entwicklung |
| HP9200C | 192.168.100.107 | 255.255.252.0 | Dokumentenscanner HP9200C, Verwaltung |
| **Switches** | **192.168.100.180** | **192.168.100.219** | **Switch, Router, Wireless** |
| HP2910al | 192.168.100.180 | 255.255.252.0 | ProCurve 2910al-48G Switch (J9147A) EDV1 |
| HP2910al | 192.168.100.181 | 255.255.252.0 | ProCurve 2910al-48G Switch (J9147A) EDV2 |
| HP4204vl | 192.168.100.182 | 255.255.252.0 | ProCurve Switch 4204vl-48GS (J9064A) EDV1 |
| HP4204vl | 192.168.100.183 | 255.255.252.0 | ProCurve Switch 4204vl-48GS (J9064A) EDV2 |
| HP4204vl | 192.168.100.184 | 255.255.252.0 | ProCurve Switch 4204vl-48GS (J9064A) EDV2 |
| HP4204vl | 192.168.100.185 | 255.255.252.0 | ProCurve Switch 4204vl-48GS (J9064A) EDV3 |
| HP4204vl | 192.168.100.186 | 255.255.252.0 | ProCurve Switch 4204vl-48GS (J9064A) EDV3 |
| HP5406zl | 192.168.100.187 | 255.255.252.0 | ProCurve Switch 5406zl-48G (J8699A) EDV1 |
| HP4000m | 192.168.100.188 | 255.255.252.0 | ProCurve Switch 4000M (J4121A) EDV4 |
| **frei** | **192.168.100.220** | **192.168.100.249** | **derzeit nicht belegt** |
| **Gateway** | **192.168.100.250** | **192.168.100.255** | **Gateway, ISA-Server** |
| ISA01 | 192.168.100.253 | 255.255.252.0 | ISA-Server |
| Gateway | 192.168.100.254 | 255.255.252.0 | Firewall Gateway |
| **Test** | **192.168.101.0** | **192.168.101.49** | **Testzwecke** |
| Test1 | 192.168.101.1 | 255.255.252.0 | Test-PC1 (Linux) E-Labor |
| Test2 | 192.168.101.2 | 255.255.252.0 | Test-PC2 (Linux) E-Labor |
| **DHCP** | **192.168.101.50** | **192.168.102.199** | **DHCP-Bereich** |
| **frei** | **192.168.102.200** | **192.168.102.255** | **derzeit nicht belegt** |
| **Test** | **192.168.103.0** | **192.168.103.49** | **Testzwecke** |
| **DHCP-noInet** | **192.168.103.50** | **192.168.103.199** | **DHCP-Bereich für noInet-PCs** |
| noInet1 | 192.168.103.199 | 255.255.252.0 | PC1 mit gesperrtem Internet |
| noInet2 | 192.168.103.198 | 255.255.252.0 | PC2 mit gesperrtem Internet |
| noInet3 | 192.168.103.197 | 255.255.252.0 | PC3 mit gesperrtem Internet |
| noInet4 | 192.168.103.196 | 255.255.252.0 | PC4 mit gesperrtem Internet |
| **frei** | **192.168.103.200** | **192.168.103.254** | **derzeit nicht belegt** |
| **Broadcast** | **192.168.103.255** | | **Broadcastadresse des Netzwerks** |

**Tabelle 6: Tabelle der IP-Adressen**

### 4.3.3 Konfiguration des DHCP-Servers

Der DHCP-Server wird für den neuen DHCP-Bereich konfiguriert und die zusätzlichen Parameter (Netzmaske, Gateway, DNS) eingestellt. Arbeitsstationen mit Internetzugang erhalten nun nach einem Neustart oder dem Einschalten am nächten Arbeitstag eine freie IP-Adresse aus dem verfügbaren Adressbereich.
Für jede Arbeitsstationen mit gesperrtem Internetzugang muss am DHCP-Server einmalig die bestehende Reservierung gelöscht und neu angelegt werden, da keine Änderung einer Reservierung möglich ist. Bei dieser Reservierung wird der MAC-Adresse der Netzwerkkarte der Arbeitsstation eine fixe IP-Adresse aus dem Bereich „DHCP-noInet“ zugeordnet. Nach einem Neustart dieser Arbeitsstation wird die neue IP-Adresse zugeteilt, siehe dazu auch [MCSE07]

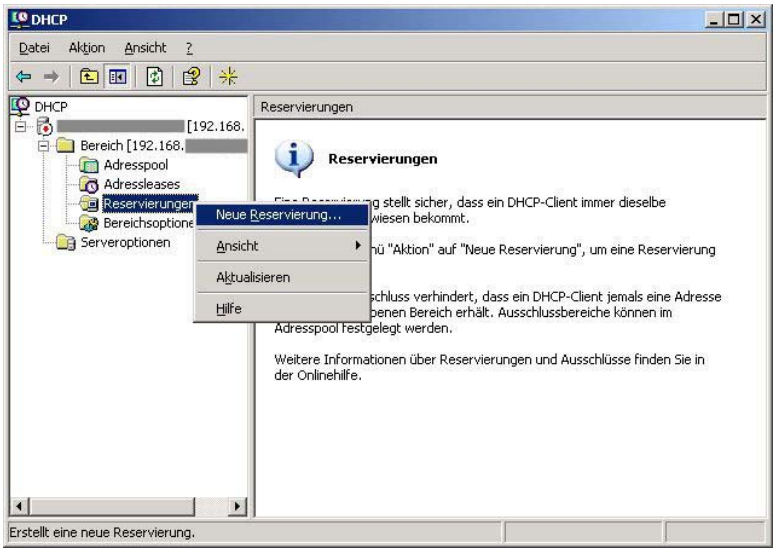



**Abbildung 17: DHCP-Server Reservierung**

Damit der DHCP-Server eine reservierte IP-Adresse vergibt, sollte diese IP-Adresse nicht im eigentlichen DHCP-Bereich liegen, d.h. am DHCP-Server wird nur der Bereich `192.168.101.50` bis `192.168.102.199` für die automatische Vergabe eingestellt. Die reservierten IP-Adressen im Bereich `192.168.103.50` bis `192.168.103.199` werden trotzdem korrekt vergeben.

Auf der Firewall muss noch die „noInet-Regel“ dahingehend geändert werden, dass der Bereich der gesperrten IP-Adressen auf den neuen Bereich festgelegt wird.

### 4.3.4 Erweiterung im laufenden Betrieb

Die Umstellung der IP-Adressen wird im laufenden Betrieb durchgeführt. Arbeitsstationen, egal ob mit oder ohne Internetzugang erhalten nach einem Neustart oder dem Einschalten am nächten Arbeitstag eine freie IP-Adresse aus dem verfügbaren Adressbereich. Durch eine IT-Richtlinie ist festgelegt, dass Arbeitsstationen am Ende eines Arbeitstages abgeschaltet werden müssen, Ausnahmen sind der IT-Leitung bekannt, diese Stationen müssen manuell neu gestartet werden.
Die Server werden manuell umgestellt. Die Server werden nur über die freigegebenen Pfade (z.B. \\daten01\verwaltung) angesprochen, daher wirkt sich eine Änderung der IP-Adresse nicht aus, da der DNS-Server die neue IP-Adresse mit dem Namen verknüpft.
Die Drucker werden über ein Startscript des Active Directory an die Arbeitsstationen zugewiesen. IP-Adressen der Drucker werden manuell geändert und dann im Active Directory neu eingestellt.
Die Produktionsmaschinen werden manuell umgestellt und müssen gleichzeitig auch an einer Arbeitsstation in der Produktion geändert werden. Da es sich hier nur um vereinzelte Maschinen handelt, wird dies direkt mit der Produktionsabteilung abgesprochen, wann eine Umstellung sinnvoll ist. Durch die Umstellung kommt es zu keiner Unterbrechung der Produktion, da die Maschinen dabei weiterlaufen können.

Zur Umstellung der Switches muss gesagt werden, dass die neuen Switches schon mit der richtigen IP-Adresse konfiguriert werden. Die Auswahl und Konfiguration neuen Switches werden im Kapitel 4.4 und 4.6 beschrieben.

Die bestehenden Switches werden manuell umgestellt, die Änderung betrifft nur die IP-Adresse zur Konfiguration der Switches. Auch hier kommt es zu keiner Unterbrechung der Produktion.

## 4.4 Glasfaserverkabelung Backbone

### 4.4.1 Allgemeines

Die einzelnen Firmengebäude sind mit einem Glasfaserkabel miteinander verbunden, wie dies schon im Kapitel 4.2.2 beschrieben ist. Es gibt zwei Typen von Glasfaserkabeln im Firmengebäude. Das länger bestehende Kabel verbindet das Hauptgebäude mit der alten Produktion (siehe Kapitel 4.4.2). Im Zuge des Firmenausbaus werden die alten und neuen Teile des Firmengebäudes ebenfalls mit Glasfaserkabeln miteinander verbunden. Das neue Kabel war zum Zeitpunkt dieser Masterarbeit bereits vor Ort und die Verlegung wurde schon begonnen, es konnte daher nicht mehr in die Auswahl des Kabels eingegriffen werden. Nach einer Typprüfung des neuen Kabels konnte zumindest noch darauf Rücksicht genommen werden, dass die maximale Kabellänge von 110m nicht überschritten werden darf, um eine Übertragungsgeschwindigkeit von 10Gbit/s zu ermöglichen (siehe Kapitel 4.4.3).

Für die Verbindung der beiden Serverräume soll eine Backbonegeschwindigkeit von 10GBit/s angestrebt werden, weil die Arbeitsstationen bereits fast alle mit 1GBit-Netzwerkkarten ausgestattet sind und eine 10-fache Backbonegeschwindigkeit möglich sein soll.

Für die bestehende Verbindung vom Hauptgebäude zum alten Produktionsgebäude bleibt die Geschwindigkeit von 1Gbit/s, da die Kabelverbindung zu lang ist. Eine Erweiterung auf 10Gbit/s wäre nur durch einen Austausch des LWL-Kabels möglich, Ein Austausch ist aber wirtschaftlich nicht sinnvoll und derzeit nicht notwendig, weil die Arbeitsstationen im alten Produktionsgebäude nur mit 100Mbit/s betrieben werden und diese Geschwindigkeit ausreichend ist. Ausserdem kann die Produktion zukünftig über das neue Kabel vom Serverraum im Neubau angebunden werden. Dies ist aber derzeit nicht geplant.

Für eine 10Gbit-Verbindung ist nicht nur das Glasfaserkabel entscheidend sondern auch die Auswahl der Switches mit den erforderlichen Modulen. Die Auswahl der geeigneten Netzwerkkomponenten wird im Kapitel 4.4 vorgenommen.

### 4.4.2 Kenndaten der bestehenden Glasfaserverkabelung

Die bestehende Glasfaserverbindung führt vom Hauptgebäude zum nunmehr alten Produktionsgebäude. Die Kabelstrecke ist 142m lang.
Die folgende Tabelle listet die Kenndaten des Glasfaserkabels auf:

| | |
|---|---|
| *Hersteller* | ***Gebauer&Griller*** |
| *Typbezeichung* | ***A-DQ(ZN)(BN)2Y-G50/125*** |
| *Fasertyp* | *G50/125, OM2, Gradientenfaser (Multimode)* |
| *Faserkerndurchmesser* | *50µm* |
| *Anzahl der Fasern* | *8* |
| *Dämpfung bei 850nm* | *≤ 2,6 dB/km* |
| *Bandbreite (OFL) bei 850nm* | *≥ 500 MHz*km* |
| *max. Linklänge* | *1000BASE-SX (1Gbit): 550m*<br>*10GBASE-SR (10Gbit): 82m* |

**Tabelle 7: Kenndaten LWL-Kabel Gebauer&Griller**

Bei der verlegten Länge von 142m ist eine Übertragungsgeschwindigkeit von 1Gbit/s möglich. [GUG01], [GUG02]

### 4.4.3 Kenndaten der neuen Glasfaserverkabelung

Die neue Glasfaserverkabelung verbindet das Hauptgebäude mit dem Neubau. Die Verkabelung ist im Kapitel 4.2.2 zu sehen.
Die folgende Tabelle listet die Kenndaten des verwendeten Glasfaserkabels auf:

| | |
|---|---|
| *Hersteller* | ***Schrack*** |
| *Typbezeichung* | ***HSEAIBH085 – A-DQ(ZNB)H*** |
| *Fasertyp* | *G50/125, **OM2e**, Gradientenfaser (Multimode)* |
| *Faserkerndurchmesser* | *50µm* |
| *Anzahl der Fasern* | *8* |
| *Dämpfung bei 850nm* | *≤ 2,5 dB/km* |
| *Bandbreite (OFL) bei 850nm* | *≥ 600 MHz*km* |
| *max. Linklänge* | *1000BASE-SX (1Gbit): 750m*<br>*10GBASE-SR (10Gbit): 150m* |

**Tabelle 8: Kenndaten LWL-Kabel Schrack**

Bei der verlegten Länge von 103m ist eine Übertragungsgeschwindigkeit von 10Gbit/s möglich. Mit dieser Geschwindigkeit sollen die beiden Serverräume miteinander verbunden werden. Die Firma Schrack garantiert 10Gbit/s mit dem verwendeten Kabel. Dies kann auf den verwendeteten Fasertyp OM2e zurück geführt werden. Das zusätzliche Datenblatt wird dieser Masterarbeit als Datei beigefügt. [SCHR01], [KSI02]

## 4.5 Planung und Auswahl der Netzwerkkomponenten

### 4.5.1 Ablauf

Am Beginn der Planung müssen die zu erwartenden Netzwerkanschlüsse und die verwendeten Geräte in den verschiedenen Gebäuden definiert werden. Dies ist die Grundlage für die Anzahl der notwendigen Switchports und die damit verbundene Anzahl von Switches bzw. Switchmodulen. Für den Umbau müssen genügend Kat6-Patchkabel zur Verfügung stehen, die Beschaffung sollte früh genug erfolgen. Die Netzwerkdosen im Neubau wurden bereits eingebaut und installiert. Es existieren 2 Serverräume (Hauptgebäude, Neubau) und zwei Unterverteiler (Produktion alt und neu). Als nächster Schritt erfolgen die Auswahl der Switches und der geeigneten Module für die 10Gbit-Verbindung der beiden Serverräume. Am Ende wird der Netzwerkplan erstellt.

### 4.5.2 Anzahl der Netzwerkanschlüsse

Nach einer Aufstellung der geplanten Arbeitsplätze wird die Anzahl der notwendigen Switchports ermittelt. Die Aufstellung muss alle Systeme, wie Arbeitsplatze, Netzwerkdrucker, Server, Firewall, Produktionsmaschinen, aber auch Reserveports und Ports für Testzwecke enthalten. Weiters müssen auch die Verbindungsports zwischen den Switches und Serverräumen eingeplant werden. Die Aufstellung sollte realistisch sein, damit der wirtschaftliche Aspekt auch berücksichtigt wird und die Kosten im Rahmen bleiben.
Nach dieser Einschätzung ergibt sich für die Verteiler- und Serverräume folgende Aufstellung:

| Raum | Art | Anzahl | Beschreibung |
|---|---|---|---|
| Serverraum Hauptgebäude | 10GBase-SR<br>1000Base-SX<br>1000Base-T | 1<br>1<br>150 | Verb. EDV1 – EDV2<br>Verb. EDV1 – EDV4<br>Switchports 1Gbit |
| Serverraum Neubau 1.Stock | 10GBase-SR<br>1000Base-SX<br>1000Base-T | 1<br>2<br>100 | Verb. EDV2 – EDV1<br>Verb. EDV2 – EDV3<br>Switchports 1Gbit |
| Verteilerraum Produktion alt | 1000Base-SX<br>100Base-T | 1<br>45 | Verb. EDV4 – EDV1<br>Switchports 100Mbit |
| Verteilerraum Produktion neu | 1000Base-SX<br>1000Base-T | 2<br>60 | Verb. EDV3 – EDV2<br>Switchports 1Gbit |

**Tabelle 9: Anzahl der geplanten Switchports**

### 4.5.3 Auswahl der Switches

In diesem Kapitel werden die benötigten Switches und Module ausgewählt. Die bestehenden HP ProCurve Switches sind qualitativ hochwertige Geräte und nach wie vor zeitgemäß, daher werden sie auch weiterhin eingesetzt und in die IT-Infrastruktur integriert. Ein wichtiges Kriterium bei der Suche war die benötigte 10Gbit-Verbindung der beiden Serverräume. Die gewählten Switches mussten zumindest einen 10Gbit-Anschluss anbieten können. Weiters sollten die Kosten für die IT-Infrastruktur im Rahmen bleiben. Die gewählten Module sind im Kapitel 4.5.4 bereits angeführt.

Für die IT-Infrastruktur wurde schließlich die ProCurve-Familie von HP gewählt, weil bereits ein Bestand an HP Switches vorhanden war und die Switches eine gute Qualität aufweisen. Anstatt eines großen Hauptswitches wurden mehrere kleine Switches auf die Server- und Verteilerräume aufgeteilt. Dies gewährleistet bei einem Ausfall eines Switches einen raschen Umstieg der wichtigsten Anwendungen auf den noch funktionierenden Switch. Die Switches können fast alle noch durch Module nachgerüstet werden, um flexibel auf eine Erweiterung reagieren zu können.
In den folgenden Tabellen werden die bestehenden und neu ausgewählten Switches und Module kurz beschrieben. Als Orientierungshilfe ist immer die HP-eigene Artikelnummer dazu angegeben:

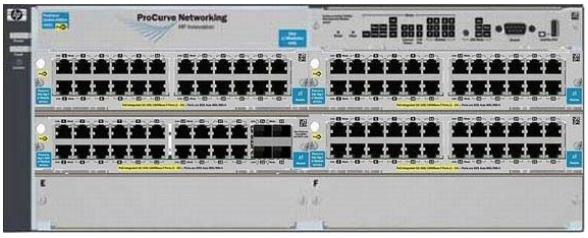
| | |
|---|---|
| *Herstellerbez.* | *HP – J8699A* |
| *Bezeichnung* | *ProCurve Switch 5406zl-48G (Bestand)* |
| *Ausstattung* | *3x 24port ProCurve 10/100/1000 PoE (J8702A)*<br>*1x 20port ProCurve 10/100/1000 PoE mit 4port MiniGBIC (J8705A)* |
| *Ports* | *92 Ports 1Gbit PoE (Power over Ethernet)*<br>*4 Ports MiniGBIC* |
| *Abbildung* |  |

**Tabelle 10: HP ProCurve J8699A [HP8699]**

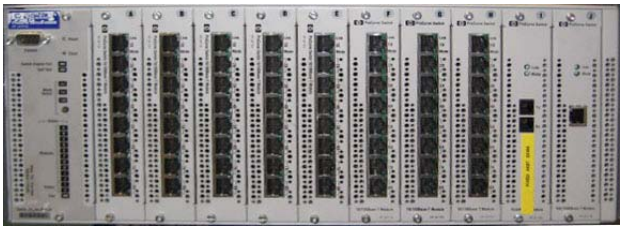
| | |
|---|---|
| *Herstellerbez.* | *HP – J4121A* |
| *Bezeichnung* | *ProCurve Switch 4000M (Bestand)* |
| *Ausstattung* | *8x 8port ProCurve 10/100 (J4111A)*<br>*1x 1port ProCurve 100/1000Base-T (J4115B)*<br>*1x 1port ProCurve 1000Base-SX (J4113A)* |
| *Ports* | *64 Ports 10/100Mbit, 1 Port 1Gbit SX, 1 Port 1Gbit über Kupfer* |
| *Abbildung* |  |

**Tabelle 11: HP ProCurve J4121A [HP4121]**

| | |
|---|---|
| *Herstellerbez.* | *HP – J9064A* |
| *Bezeichnung* | *ProCurve Switch 4204vl-48GS* |
| *Ausstattung* | *1x 24port ProCurve vl Gig-T (J8768A)*<br>*1x 20port ProCurve vl Gig-T + 4port SFP (J9033A)* |
| *Ports* | *44 Ports 1Gbit über Kupfer*<br>*4 Ports SFP-Steckplätze* |
| *Abbildung* |  |

**Tabelle 12: HP ProCurve J9064A [HP9064]**

| | |
|---|---|
| *Herstellerbez.* | *HP – J9147A* |
| *Bezeichnung* | *ProCurve Switch 2910al-48G* |
| *Ausstattung* | *44port 10/100/1000 1000Base-T*<br>*4 Dual Personality Ports (1000Base-T oder mini-GBIC Transceiver)*<br>*Unterstützung für 10Gbit-Ports mit rückseitigen Modulen (optional), siehe dazu 4.5.4. (J9008A mit J9150A):*<br>*ProCurve 10-GbE SFP+ al-Modul & 10GbE SFP+ SR Transceiver* |
| *Abbildung* |  |

**Tabelle 13: HP ProCurve J9147A [HP9147]**

### 4.5.4 Module für 10Gbit

Die Auswahl der Module für die 10Gbit-Verbindung der beiden Serverräume gestaltete sich nicht so einfach. Zuerst musste abgeklärt werden, ob das verwendete Glasfaserkabel überhaupt die Spezifikation erfüllt. Dies war nach längerem Telefonkontakt mit der Herstellerfirma bestätigt. Weiters mussten Switches ausgewählt werden, die überhaupt einen Port bzw. Einschub für ein 10Gbit-Modul unterstützten. Die Auswahl der Switches erfolgt im Kapitel 4.5.3.
Letztendlich fiel die Auswahl auf folgende Module:

| | |
|---|---|
| *Herstellerbez.* | *HP – J9008A* |
| *Bezeichnung* | *HP ProCurve 10-GbE 2-port SFP+ al Module (J9008A)* |
| *Beschreibung* | *2-port 10Gbit Modul für Switch HP ProCurve 2910al*<br>*Erweiterung auf 2 10GbE SFP+ Steckplätze* |
| *Abbildung* |  |

**Tabelle 14: HP ProCurve J9008A [HP9008]**

| | |
|---|---|
| *Herstellerbez.* | *HP – J9150A* |
| *Bezeichnung* | *ProCurve 10-GbE SFP+ SR Tranceiver* |
| *Beschreibung* | *1-port 10Gbit SFP+ SR-Modul für J9008A*<br>*Tranceivermodul zum Einsatz im Modul J9008A*<br>*Unterstützt einen 10Gb-SR Steckplatz* |
| *Abbildung* |  |

**Tabelle 15: HP ProCurve J9150A [HP9150]**

Die beiden Module werden in die ausgewählten Switches HP ProCurve 2910al eingebaut und bieten dann jeweils einen LC-10Gbit-Port. Zur Verbindung des Moduls mit dem LWL-Patchfeld im Serverraum muss ein LC-SC-Patchkabel verwendet werden, da die Patchpanele der Glasfaserkabel mit SC-Steckern ausgeführt sind.

### 4.5.5 Module für 1Gbit

Für die 1Gbit-Verbindung über Glasfaser zur Verbindung des Hauptgebäudes (EDV1) mit dem bestehenden Produktionsgebäude (EDV4) und der Verbindung der beiden Standorte im neuen Firmengebäude (EDV2, EDV3) werden SX-Mini-GBICs verwendet. 1000Base-SX-Module sind Module für Multimode-Glasfaserkabel mit einer Wellenlänge von 850nm. Die Module werden in Mini-GBIC-Steckplätzen von Switches eingesteckt.
Für den 1Gbit-Betrieb wurde folgendes Modul ausgewählt:

| | |
|---|---|
| *Hersteller* | *HP – J4858C* |
| *Bezeichnung* | *ProCurve Gigabit SX-LC Mini-GBIC* |
| *Beschreibung* | *1-port Gigabit SX-LC Mini-GBIC Modul*<br>*Tranceivermodul zum Einsatz in Mini-GBIC-Steckplätzen für den Anschluß eines LC-Patchkabels* |
| *Abbildung* |  |

**Tabelle 16: HP ProCurve J4858C [HP4858]**

### 4.5.6 Trunk-Ports

Sind in einem Server- oder Verteilerraum mehrere Switches vorhanden, müssen sie miteinander verbunden werden. Die einfachste Variante ist die Verwendung von Port-Trunks. Dabei werden mehrere Switchports zu einem virtuellen Trunkport zusammengefasst. Dieser Trunk muss auf beiden Switches, die verbunden werden sollen, eingerichtet werden. In diesem Fall werden Trunks immer zum 10Gbit-Switch HP ProCurve 2910al gelegt. Der Nachteil dieser Methode ist, dass man dafür mehrere Switchports benötigt, aber in diesem Fall sind genügend vorgesehen.

Der Netzwerkplan mit den Port-Trunks ist im Kapitel 4.5.7 ersichtlich.

### 4.5.7 Netzwerkplan

Im Netzwerkplan sind die Switches und die Verkabelung der Switches dargestellt. Die einzelnen Mini-GBICs und SFP+ Module sind der Übersichtlichkeit wegen nicht eingezeichnet.

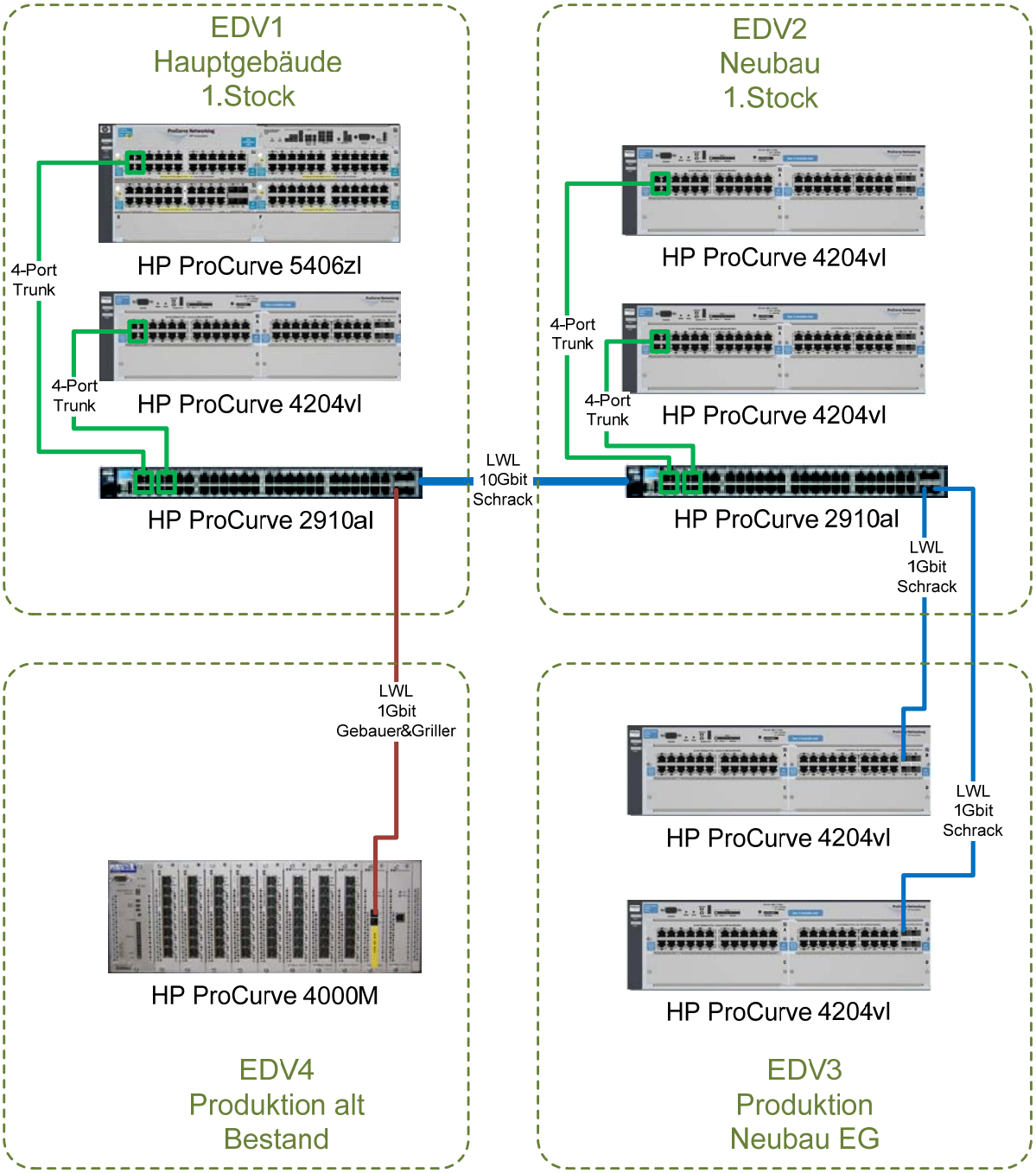



**Abbildung 18: Netzwerkplan**

## 4.6 Switch Konfiguration

Die Switchkonfiguration wird hier anhand des HP ProCurve 2910al durchgespielt. Die anderen Switches werden analog dazu konfiguriert. In den folgenden Kapiteln sind die wichtigsten Einstellungen zusammengefasst.

### 4.6.1 Erstkonfiguration

Die Erstkonfiguration erfolgt über die serielle Schnittstelle am Switch selbst. Dabei wird das mitgelieferte Konsolenkabel verwendet. Mit dem Programm „PuTTY“ [PUTTY] kann man sich nun mit der Einstellung „seriell“ an den Swtich verbinden. Damit eine Verbindung entsteht, mehrfach „Enter“ drücken. Die Konsole meldet sich mit dem Prompt:

- `SWITCH1#`

Nach Eingabe von „configure“ wechselt der Prompt in den Konfigurationsmodus:

- `SWITCH1<config>#`

Die Eingabe „menu“ öffnet das Konfigurationsmenü. Über die Menüpunkte „Switch Konfiguration“ und „IP Configuration“ kann man die IP-Adresse des Switch einstellen. Welche IP-Adresse eingestellt werden muss, ist im Kapitel 4.2.1 nachzulesen. Nach der Erstkonfiguration kann der Switch über das Web-Interface weiter konfiguriert werden. Dazu muss einfach die eingestellte IP-Adresse im Web-Browser eingegeben werden, die Verbindung sollte mit einem „ping“ zuerst überprüft werden.

### 4.6.2 System Info

Nach dem Begrüßungsbildschirm wechselt man in den Reiter „Configuration“ und in das Untermenü „System Info“. Unter diesem Punkt werden der Systemname, der Standort und der Kontakt eingeben:

- System Name: HP2910al-EDV1
- System Location: EDV1
- System Contact: IT

### 4.6.3 IP-Adresse überprüfen

Im Reiter „Configuration“ wechselt man in das Untermenü „IP Configuration“. Dort wird die vorher eingestellte IPv4-Adresse, die Netzmaske und der Default-Gateway eingestellt. Als VLAN wird das „DEFAULT_VLAN“ ausgewählt.

### 4.6.4 Trunk-Ports definieren

Die beiden ProCurve2910al-Switches sind jeweils per Trunk mit den beiden anderen Switches im gleichen Serverraum miteinander verbunden. 4 Ports werden zu einem Trunk zusammengefasst. Informationen zu den gewählten Trunks sind im Kapitel 4.5.6 und 4.5.7 ersichtlich.
Die Trunk-Ports werden im Menü „Configuration“ und dem Untermenü „Port Configuration“ eingestellt. Dazu werden zuerst die Ports 1-4 des Switches ausgewählt und einem Trunk (hier TRK1) zugewiesen. Nachher werden die Ports 5-8 zu einem Trunk (hier TRK2) zusammengefasst. Bei den beiden anderen Switches, die mit diesem Switch verbunden sind, muss natürlich nur ein Trunk angelegt werden. Dazu werden die ersten 4 Ports benutzt.

### 4.6.5 Passwortschutz des Switches

Aus Sicherheitsgründen und um eine versehentliche Misskonfiguration durch einen Dritten zu vermeiden, werden die Switches mit einem Passwort geschützt. Im Menüreiter „Security“ und dem Untermenü „Device Passwords“ kann zwischen zwei Benutzern unterschieden werden:

- Operator mit „read-only-access“
- Manager mit “read-write-access”

In diesem Fall wird zwischen den beiden Benutzern nicht unterschieden und für beide der gleiche Benutzername und das gleiche Kennwort vergeben. Dadurch wird der Benutzer „Operator“ nicht verwendet, weil dann bei einem Login automatisch der Benutzer „Manager“ eingeloggt wird. Eine Anmeldung als „Operator“ ist derzeit nicht vorgesehen, man erspart sich das Merken eines weiteren Logins.

### 4.6.6 Zugriff einschränken

Es ist sinnvoll, den Zugriff auf den Switch nur mehr von authorisierten Systemen zu erlauben. Im Menüreiter „Security“ und dem Untermenü „Authorized Addresses“ können die IP-Adressen der authorisierten Systeme eingetragen werden. Die Eingabe der IP-Adresse erfolgt mit der Netzmaske 255.255.255.255. Der Zugriff ist nur mehr von den eingetragenen Adressen möglich. Es wird hier die IP-Adresse eines Verwaltungsrechners und des DC eingetragen. Beachten muss man, dass man sich nicht selber aussperrt, die erste eingetragene IP-Adresse sollte jene sein, von der man gerade den Switch konfiguriert, sonst wird man „ausgesperrt“.

### 4.6.7 Telnet und Konsolenzugriff absichern

Der Zugriff über Telnet ist standardmässig eingeschaltet und kann auch eingeschaltet bleiben. Da der Zugriff auf den Switch auf wenige IP-Adressen beschränkt ist, ist auch ein Telnet-Zugriff nur über diese Systeme möglich.

Die Konsole, also der direkte Zugriff über das serielle Kabel auf die Konsolenschnittstelle des Switches, ist durch kein Passwort geschützt. Um sich über die Konsole auf den Switch zu verbinden, muss man physischen Zugriff auf den Switch haben. Die Serverräume sind aber abgesperrt und nur für das IT-Personal zugänglich, daher ist die Konsole damit ausreichend abgesichert.

Ein Aspekt, warum kein Passwort für die Konsole verwendet wird, ist die Tatsache, dass Passwörter ob ihrer Anzahl leicht vergessen werden und das Problem auf Passwort-Dateien und deren Sicherung verlagert wird.

Ein Konsolenpasswort ist nur sehr aufwendig wieder zurück zu setzen.

## 4.7 Umbau und Inbetriebnahme der IT-Infrastruktur

Nachdem die IT-Infrastruktur geplant und bereits geliefert ist, muss sie in Betrieb genommen werden. Dies sollte nach Möglichkeit den laufenden Betrieb nur gering beeinträchtigen. Die geplante Umstellung findet während des Umzugs in das neue Firmengebäude statt. Viele Mitarbeiter wechseln vom Hauptgebäude in das neue Firmengebäude. Im Zuge dessen müssen viele Patcharbeiten durchgeführt werden. Der neue Serverraum sollte bereits mit der Switch-Architektur ausgestattet sein. Derzeit sind nur die bestehenden Switches im Hauptgebäude und der alten Produktion in Betrieb. Die Ist-Situation ist in Kapitel 4.2.3 beschrieben.

Als erster Schritt wird die 10Gbit-Verbindung zwischen den beiden Serverräumen aufgebaut. Die beiden HP ProCurve 2910al werden rückseitig mit den SFP+ Modulen bestückt und in Betrieb genommen. Die restlichen Switches im Neubau werden ebenfalls eingebaut und miteinander laut Netzwerkplan im Kapitel 4.5.7 verbunden. Der nicht managebare Switch im alten Produktionsgebäude bleibt in Betrieb. Das Firmennetzwerk ist derzeit noch normal in Betrieb und die neue Infrastruktur läuft parallel dazu. Um die beiden Netze zu verbinden, wird im Serverraum EDV1 der HP ProCurve 2910al durch einen freien 1Gbit-Port mit dem HP ProCurve 5406zl und damit mit dem Firmennetz verbunden.

Ein Problem sind jetzt noch die beiden Serverschränke im Serverraum EDV1 (siehe Beschreibung im Kapitel 4.2.1). Die gesamte Patchverkabelung muss zuerst entfernt werden, um die geplante Infrastruktur aufzubauen. Dieses Vorhaben wird für ein Wochenende eingeplant und an einem Freitagnachmittag nach einer längeren Vorankündigung gestartet. Die Patch- und Telefonkabel wurden vor dem Ausstecken dokumentiert. Für die Neuverkabelung werden Kat6-Patchkabel verwendet, welche in ausreichender Menge verfügbar sein müssen. Es empfiehlt sich, für gleiche Systeme auch gleiche Farben der Patchkabel zu verwenden (Drucker, Server, Arbeitsstationen, Firewall, Telefon…).

Nach dem Abstecken werden die IT-Komponenten umgebaut und schrittweise wieder angesteckt. Die Server werden alle am zentralen HP ProCurve 2910al angeschlossen. Die Arbeitsstationen und Telefone werden wieder angepatcht.

Parallel dazu werden im neuen Firmengebäude die bereits umgezogenen Arbeitssplätze gepatcht. Der Umbau war nach 48 Stunden soweit erledigt, sodass alle Mitarbeiter am darauf folgenden Montag wieder ihrer Arbeit nachgehen konnten.

# 5 ANHÄNGE

## 5.1 IT-Sicherheitsrichtlinie für Mitarbeiter

Die IT-Sicherheitsrichtlinie und die enthaltenen Regeln wurden in Zusammenarbeit mit dem IT-Leiter der Elektronikfirma erstellt.

### 5.1.1 Kenndaten der Richtlinie

#### *5.1.1.1 Zweck der Richtlinie*

Die Maßnahmen der vorliegenden Richtlinie unterstützen insbesondere die folgenden Ziele:

- Schutz aller Firmendaten
- Sicherstellung der Kontinuität des Netzwerkbetriebs
- Schadensvermeidung und Schadenbegrenzung
- Gewährleistung eines angemessenen Sicherheitsniveaus

#### *5.1.1.2 Zielsysteme der Richtlinie*

Die IT-Sicherheitsrichtlinie gilt für alle Teile der Firmen IT-Infrastruktur.

#### *5.1.1.3 Geltungsbereich der Richtlinie*

Die IT-Sicherheitsrichtlinie gilt verpflichtend für alle Mitarbeiter, welche die IT Infrastruktur der Firma nutzen, oder mit ihr in Berührung kommen.

#### *5.1.1.4 Verantwortlichkeit für die Richtlinie*

Die Erstellung und Änderung der IT-Sicherheitsrichtlinie obliegt dem IT-Prozesseigner. Für den Inhalt tragen der IT-Leiter und der Vorstand die Verantwortung.

#### *5.1.1.5 Organisation zur Umsetzung dieser Richtlinie*

Für die Umsetzung der IT-Sicherheitsrichtlinie sind alle Mitarbeiter, die mit Computersystemen arbeiten im Zusammenwirken mit der IT-Abteilung sowie dem Vorstand verantwortlich.

#### *5.1.1.6 Überprüfung Einhaltung der IT-Richtlinie*

Die Einhaltung der IT-Sicherheitsmaßnahmen wird regelmäßig aber auch anlassbezogen überprüft.

#### *5.1.1.7 Meldung von sicherheitsrelevanten Vorkommnissen*

Sicherheitsrelevante Vorkommnisse oder Sicherheitsmängel sind von allen Mitarbeitern umgehend dem Vorgesetzten sowie dem IT-Leiter zu melden.

#### *5.1.1.8 Einhaltung von Sicherheitsbestimmungen*

Alle von dieser Richtlinie erfassten Mitarbeiter sind verpflichtet, die vorgesehenen und auf sie anwendbaren Sicherheitsbestimmungen zu beachten und einzuhalten.

#### *5.1.1.9 Richtlinienverstöße*

Da das Unternehmen in hohem Maße von der Funktionsfähigkeit der informationstechnischen Einrichtungen abhängig ist, können fahrlässige Verstöße gegen diese Richtlinien zu disziplinären Maßnahmen führen. Diese reichen von mündlicher Verwarnung bis zur Beendigung des Dienstverhältnisses. In Fällen, die großen Schaden für die Firma verursachen, sind auch zivil- und strafrechtliche Konsequenzen nicht auszuschließen.

### 5.1.2 Benützung von Computersystemen

#### *5.1.2.1 Zweck*

Sicherstellung eines zweckmäßigen und sicheren Umgangs mit den firmeneigenen Computersystemen.

#### *5.1.2.2 Zielsysteme*

Alle von Mitarbeitern benutzten Systeme wie Desktop PCs, Notebooks, PDAs, Blackberrys, Handys, Drucker, Scanner.

#### *5.1.2.3 Gültigkeit*

Gilt für alle Mitarbeiter die mit einem der oben genannten Systeme arbeiten.

#### *5.1.2.4 Regeln*

*(1) Wer trägt die Verantwortung für ein bestimmtes Computersystem?*

Jener Mitarbeiter, dem das System von der IT-Abteilung überantwortet wurde (in den meisten Fällen ist das der Hauptbenutzer des Systems). Viele Rechner (meist Produktion) werden von mehreren Mitarbeitern benutzt. Es gibt aber auch für diese Rechner einen Verantwortlichen, den sogenannten Halter des Computers. Dieser Halter wird von der EDV in Absprache mit der jeweiligen Abteilung bestimmt.

*(2) Wer darf ein Computersystem benutzen?*

Der Halter und alle anderen befugten Personen, die von der zuständigen Bereichsleitung oder IT-Abteilung zu befugten Personen erklärt wurden.

*(3) Welche Software muss auf einem Computersystem installiert sein?*

Auf Systemen, die für den Internetzugang genutzt werden, muss ein aktueller Virenschutz installiert sein und laufen.

*(4) Wer darf auf einem Computersystem Software installieren? (Der Begriff Software umfasst auch Tools, Utilities, Treiber, Bildschirmschoner, Demos, Spiele u.ä.)*

Software darf nur von der IT-Abteilung installiert werden.
*Ausnahmen:* Entwicklungspersonal darf ausschließlich im Rahmen seiner Entwicklungstätigkeit Software installieren. Entwickler dürfen aber auch nur dann SW installieren, wenn die Installation dieser mit der IT-Abteilung abgesprochen wurde und den störungsfreien Betrieb des Netzwerkes nicht gefährdet. Von der IT-Abteilung beauftragte Personen dürfen fallweise genehmigte Software auf Clients installieren. Diese Ausnahmen sind nur dann möglich, wenn damit nicht gegen Lizenzrechte oder Urheberrechte verstoßen wird.

*(5) Muss ich meinen Rechner am Ende des Arbeitstages ausschalten?*

Ja.
*Ausnahmen:* Falls es aus relevanten Gründen notwendig ist, dass der Rechner weiterlaufen muss. Um Unbefugten den Zugang zu Firmendaten zu verwehren wird dringend empfohlen auf Rechnern, die längere Zeit unbeaufsichtigt laufen müssen, den Standardbildschirmschoner mit Kennwortschutz zu aktivieren.

*(6) Was muss der Halter eines Notebooks zusätzlich beachten?*

Alle von der Firma zur Verfügung gestellten Notebooks sind als Firmeneigentum zu betrachten und dürfen daher auch nur für Firmenzwecke eingesetzt werden. Ein Firmennotebook ersetzt keinesfalls den eigenen PC zu Hause und darf auch nicht mit einem solchen vernetzt werden. Beim Verwenden eines Notebooks außerhalb der Firmenstandorte ist sicherzustellen, dass keiner unbefugten Person Zugriff auf Firmendaten ermöglicht wird.

*(7) Dürfen private Notebooks oder firmenfremde Notebooks von Verkäufern oder Geschäftspartnern usw. an unser Firmennetzwerk angeschlossen werden?*

Diese dürfen nicht an das Firmennetzwerk angeschlossen werden. Zu beaufsichtigen und gegebenenfalls zu verhindern ist das von jenen Mitarbeitern, die zur Aufenthaltszeit dieser Geschäftspartner bzw. Verkäufer mit ihnen in Verbindung stehen.

*(8) Welche Regelung gilt für die Benutzung von PDAs u. Handys?*

Private PDAs und Handys dürfen nicht mit Firmenrechnern gekoppelt werden. Datenübertragungen und Synchronisierungen mit Firmenrechnern gibt es nur mit den dafür vorgesehenen und von der IT genehmigten Produkten (derzeit nur Blackberrys).

*(9) Was haben die Halter von Firmen-Blackberrys zu beachten?*

Passwörter können maximal siebenmal falsch eingegeben werden.
Falls ein Gerät verloren oder gestohlen wurde, ist umgehend die IT-Abteilung zu alarmieren. Geräte speichern sensible Firmendaten, deswegen abgelegte Geräte immer sperren. Geräte dürfen ausschließlich zum Telefonieren, E-Mailen, SMS verschicken verwendet werden (auch wenn das Gerät andere Möglichkeiten zulassen würde).

*(10) Was ist im Umgang mit Druckern und Scannern zu beachten?*

Da Farbseiten ca. die zehnfachen Kosten von schwarz/weiss-Seiten verursachen, ist nur im Bedarfsfall in Farbe zu drucken.
Falls ein Drucker oder Scanner defekt ist, ist die IT Abteilung zu benachrichtigen.
Toner dürfen nur von Personen gewechselt werden, die das auch können.
Papierstau darf nur von Personen behoben werden, die das auch können.
Bei Unklarheiten ist die IT-Abteilung zu informieren.

### 5.1.3 Passwörter und deren Verwendung:

#### *5.1.3.1 Zweck*

Konsequent sicherer Umgang mit Passwörtern.

#### *5.1.3.2 Zielsysteme*

Alle passwortgeschützten Systeme.

#### *5.1.3.3 Gültigkeit*

Gilt für alle Mitarbeiter die Passwörter verwenden.

#### *5.1.3.4 Regeln*

*(1) Wie bekomme ich als neuer Mitarbeiter mein erstes Passwort?*

Das erste Passwort wird von einem Mitarbeiter der IT-Abteilung mitgeteilt.

*(2) Wie muss ich mein Passwort aufbewahren?*

Passwörter werden ohne Ausnahme nur im Gedächtnis aufbewahrt.
Sollte jemand sein Passwort vergessen, so ist das kein Problem. Er wird es von der IT-Abteilung ein neues Passwort erhalten.

*(3) Was muss ich tun, wenn ich den Verdacht habe, dass andere mein Passwort kennen?*

Bei der IT-Abteilung ist ein neues Passwort zu beantragen.

*(4) Was muss ich beim Eintippen meines Passwortes beachten?*

Passwörter können maximal dreimal falsch eingetippt werden, dann wird der Zugang automatisch gesperrt.
Beim Tippen eines Passwortes nicht von anderen zusehen lassen.
Umgekehrt gilt, dass man kurz wegschaut, wenn sich jemand gerade anmeldet. (vergleichbar mit dem Bankomat)

*(5) Darf ich mein Passwort einer anderen Person weiter geben?*

Nein.
*Ausnahme:* Der Vorgang wurde mit der IT abgesprochen.

*(6) Wie oft muss ich mein Passwort erneuern?*

Immer wenn der Verdacht gegeben ist, dass jemand anderer das Passwort auch kennt.
Spätestens alle drei bis sechs Monate kommt von der IT-Abteilung die Anforderung, ein neues Kennwort bekannt zu geben.

*(7) Wie soll mein Passwort ausschauen?*

Genehmigt werden nur Passwörter mit mindestens 8 Zeichen. Es muss zumindest eine Kombination von Buchstaben und Zahlen sein. Es darf weder Namensteile, noch Geburtsdaten, noch Wohnort oder Postleitzahl der eigenen Person oder Familie enthalten. Keine Kennwörter verwenden, die früher schon einmal verwendet wurden.

### 5.1.4 Umgang mit Firmendaten, Datensicherheit

#### *5.1.4.1 Zweck*

Sicherstellung eines zweckmäßigen und sicheren Umgangs mit Firmendaten.

#### *5.1.4.2 Zielsysteme*

Alle Systeme auf denen Daten gehalten werden.

#### *5.1.4.3 Gültigkeit*

Gilt für alle Mitarbeiter, die mit firmeneigenen Computersystemen arbeiten.

#### *5.1.4.4 Regeln*

*(1) Wer ist verantwortlich für die Sicherheit der Firmendaten?*

Jeder Mitarbeiter, der mit firmeneigenen Computersystemen arbeitet.

*(2) Wo und wie werden Daten abgelegt?*

Firmenrelevante Daten müssen auf den dafür vorgesehenen, den Mitarbeitern bekannten Serverspeicherplätzen abgelegt werden.
Lokal bearbeitete Daten müssen vom jeweiligen Mitarbeiter in vertretbaren Abständen (normalerweise täglich, mindestens wöchentlich, bei Dienstreisen unmittelbar nach Rückkehr) am Server gesichert werden.
Daten sind in geeigneter, wenn möglich geringer Größe (z.B. Bildmaterial) abzuspeichern.
Jeder Mitarbeiter hat seinen Datenbereich in Ordnung zu halten.

*(3) Wer kümmert sich um die weitere Sicherung der zur Datenablage vorgesehenen Server?*

Dies unterliegt der Verantwortung der IT Abteilung.

*(4) Dürfen Firmendaten an andere Firmen oder firmenfremde Personen weitergegeben werden?*

Firmendaten dürfen nur in Zusammenhängen, die im vorteilhaften Interesse der eigenen Firma stehen, nach außen gegeben werden. Dabei muss vor Preisgabe dieser Daten überprüft werden, ob diese nicht einen Schaden für die eigene Firma mit sich bringt.
Jeder Mitarbeiter, der Daten weitergibt ist auch dafür verantwortlich, dass die Interessen der eigenen Firma dabei gewahrt bleiben.
Im Zweifelsfall ist das OK des jeweiligen Bereichsleiters oder des Vorstandes einzuholen.

### *(5) Was ist bei der Bereitstellung von Daten auf unserem firmeninternen FTP-Server zu beachten?*

Firmendaten dürfen nur in Zusammenhängen, die im vorteilhaften Interesse der eigenen Firma stehen, nach außen gegeben werden. Dabei muss vor Preisgabe dieser Daten überprüft werden, ob diese nicht einen Schaden für die eigene Firma mit sich bringt.
Jeder Mitarbeiter, der Daten weitergibt ist auch dafür verantwortlich, dass die Interessen der eigenen Firma dabei gewahrt bleiben.
Im Zweifelsfall ist das OK des jeweiligen Bereichsleiters oder des Vorstandes einzuholen.

### *(6) Welche Regeln gelten in Bezug auf Datenverschwiegenheit?*

Der Mitarbeiter sichert zu, dass er alle, ihm im Rahmen des Vertragsverhältnisses und seiner Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten des Unternehmens, seiner Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich behandelt und geheim hält.
Er versichert, dass er derartige Informationen Dritten nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben wird, außer in Erfüllung seiner vertraglichen Pflichten.
Zieht der Mitarbeiter im Auftrage des Unternehmens Dritte zur Mitarbeit hinzu, ist er verpflichtet, diesen die gleiche Verschwiegenheitspflicht aufzuerlegen.

### *(7) Welche Datenbereiche darf ein Mitarbeiter nutzen und welche nicht?*

Mitarbeiter dürfen nur in Datenbereiche vordringen, die aufgrund ihrer Tätigkeit und Funktion für sie vorgesehen sind. Mitarbeiter dürfen nicht versuchen, auf Bereiche des Firmennetzwerkes vorzudringen, die nicht für den Mitarbeiter und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Ressourcenvergabe oder technische Mängel möglich ist.
Über derartige fehlerhafte Ressourcenvergabe oder technische Mängel ist die EDV-Abteilung ohne Verzug zu informieren.

### *(8) Ist zusätzlicher Passwortschutz von Firmendaten erwünscht?*

Firmendaten dürfen nicht zusätzlich mit Passwörtern geschützt werden. Das gilt im Besonderen für ZIP-Archive und Microsoft Office-Dokumente.
Daten auf Notebooks werden durch eine Verschlüsselungssoftware geschützt.

### *(9) Dürfen Fernwartungsunterstützungsangebote von Fremdfirmen angenommen werden?*

Grundsätzlich nein, Ausnahmen müssen vorher bei der IT Leitung gemeldet und von dieser genehmigt werden.

### 5.1.5 E-Mail Verwendung

#### *5.1.5.1 Zweck*

Sicherstellung eines zweckmäßigen und sicheren Umgangs mit dem firmeneigenen E-Mail-System.

#### *5.1.5.2 Zielsysteme*

Alle Systeme, die E-Mail-Verkehr ermöglichen, wie PCs, Notebooks, Blackberrys.

#### *5.1.5.3 Gültigkeit*

für alle Mitarbeiter, die mit einem E-Mail-System arbeiten.

#### *5.1.5.4 Regeln*

*(1) Welches E-Mail-Programm muss verwendet werden?*

Ausschließlich das von der IT-Abteilung zur Verfügung gestellte E-Mail-Programm.

*(2) Darf das firmeneigene E-Mail-System auch für private Zwecke genutzt werden?*

Nein.

*(3) Was hat ein Mitarbeiter bei der Verwaltung seines Postfachs zu beachten?*

Postfächer sind aufzuräumen und nicht, oder nicht mehr, firmenrelevante E-Mails sind regelmäßig zu löschen.

*(4) Was soll in einer E-Mail-Signatur stehen?*

Der Inhalt der E-Mail-Signatur in einem geschäftlichen E-Mail ist durch das Gesetz über das elektronische Handelsregister und Genossenschaftsregister geregelt und soll folgende Angaben enthalten: [PNC01]

- Rechtsform und der Sitz der Gesellschaft
- das Registergericht des Sitzes der Gesellschaft
- die Handelsregisternummer
- alle Geschäftsführer oder den Aufsichtsratsvorsitzenden

Es sollte zusätzlich ein ähnlicher Wortlaut wie „Der Austausch von Nachrichten via e-mail ist unverbindlich“ enthalten sein.

*(5) Was ist beim Versenden von E-Mails beachten?*

E-Mails an mehrere Adressanten sind mit der IT-Abteilung abzusprechen, wenn das Produkt aus E-Mail-Größe und Empfängeranzahl 30MB überschreitet.
Es können keine E-Mails mit Anhängen > 4MB versendet werden.
Es dürfen keinerlei Spam, Kettenbriefe, oder ähnliches versendet werden.
Jedes E-Mail ist mit einem passenden Betreff zu versehen.

### *(6) Was ist beim Empfang eines E-Mails zu beachten?*

Dieser Punkt ist etwas umfangreicher. Beim E-Mail-Empfang sollte auf folgende Aspekte Rücksicht genommen werden:

- Auch bei E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern muss geprüft werden, ob der Inhalt der Nachricht zum Absender passt und ob das E-Mail bzw. das Attachment auch erwartet wurde. Englischsprachige E-Mails von deutschsprachigen Partnern sind ein klares Alarmsignal, aber auch unerwartete Inhalte oder der fehlende Bezug zu aktuellen Vorgängen sollten Vorsichtsmaßnahmen auslösen.

- Mehrere E-Mails mit gleichem Betreff sind verdächtig, insbesondere wenn sie von verschiedenen Absendern stammen.

- Als Attachment gesendete Programme oder Skripts (d.h. Dateien mit den Endungen .com, .exe, .bat, .vbs etc.) dürfen nur ausgeführt werden, wenn sie vom Empfänger erwartet wurden und ihre Rechtmäßigkeit klar feststeht. Besondere Vorsicht ist bei doppelten, „merkwürdigen“ Dateinamen-Endungen („.jpg.vbs“ oder „gif.exe“) geboten. Sie sollen dem Empfänger eine harmlose Datei vortäuschen, sind aber ausführbare Schadprogramme.

- Auch E-Mails im HTML-Format oder Office-Dokumente (*.doc, *.xls, *.ppt etc.) sowie Bildschirmschoner (*.scr) können Schadensfunktionen enthalten. Sie dürfen ebenfalls nur geöffnet werden, wenn der Absender vertrauenswürdig ist bzw. die Datei erwartet wurde.

- Phishing-Mails, d.h. E-Mails, in denen zur Übermittlung von persönlichen Daten oder Passwörtern (z.B. PIN oder TAN) aufgefordert wird, dürfen auf keinen Fall beantwortet werden. Auch darin angegebene Webseiten dürfen nicht geöffnet werden. Bei Erhalt einer derartigen E-Mail sollten auch die anderen Mitarbeiter darauf hingewiesen werden, dass es sich dabei um einen Betrugsversuch handelt.

- Bei besonderen „Angeboten“, für die nur ein Link im E-Mail angeklickt werden muss, ist besondere Vorsicht geboten: Beim Aufruf dieser URL wird möglicherweise Schadsoftware installiert oder eine gefälschte Phishing-Webseite aufgerufen. Im Fall von HTML-Mails muss die Adresse, die im E-Mail als Link angezeigt wird, nicht mit der Seite übereinstimmen, die dann tatsächlich aufgerufen wird.

- Spam-Mails, Werbemails und andere unaufgefordert erhaltene Zusendungen sollte man nie beantworten. Auch die Aufforderung an den Absender, weitere Zusendungen zu unterlassen, ist sinnlos: Die Rückmeldung bestätigt dem Versender nur die Gültigkeit der Mail-Adresse, erhöht also nur das Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellungen sinnvoll.

### 5.1.6 Internetverwendung

#### *5.1.6.1 Zweck*

Sicherstellung eines zweckmäßigen und sicheren Umgangs mit den firmeneigenen Internetzugängen.

#### *5.1.6.2 Zielsysteme*

Alle Systeme, die Internetverkehr ermöglichen wie PCs, Notebooks.

#### *5.1.6.3 Gültigkeit*

Gilt für alle Mitarbeiter, die die Möglichkeit haben, durch ein Firmensystem in das Internet zu gelangen.

#### *5.1.6.4 Regeln*

*(1) Welcher Internetbrowser muss verwendet werden?*

Ausschließlich das von der IT-Abteilung zur Verfügung gestellte Browserprogramm.

*(2) Ist privates Internetsurfen erlaubt?*

Während der Pausen darf der Mitarbeiter seinen Internetzugang für Informationszwecke nutzen. Diese Nutzung muss maßvoll erfolgen und es dürfen dabei keine Dateien heruntergeladen werden.

*(3) Welche Internetseiten sind überhaupt verboten?*

Grundsätzlich verboten ist das Aufrufen von Crackseiten, Filesharingseiten, Spielseiten, Glückspielseiten, pornografische Seiten.

*(4) Welche Art von Internetaufrufen ist zusätzlich verboten?*

Es dürfen keine Streemingmedien (z.B. Youtube Videos, Internet Radio, oder Ähnliches) aufgerufen werden.

*(5) Darf Software aus dem Internet heruntergeladen und installiert werden?*

Grundsätzlich ist weder der Download, noch die Installation von Software aus dem Internet erlaubt. Ausnahmen müssen mit der IT Abteilung abgesprochen sein.

*(6) Dürfen Instant Messaging Programme benutzt werden?*

Instant Messaging Programme, wie ICQ, Skype, Windows Life Messenger oder ähnliche Programme dürfen nicht verwendet werden. Ausnahmen müssen von der IT Leitung genehmigt werden.

### 5.1.7 Umgang mit externen Speichern

#### *5.1.7.1 Zweck*

Sicherstellung eines zweckmäßigen und sicheren Umgangs mit externen Speichermedien.

#### *5.1.7.2 Zielsysteme*

USB Sticks, externe Festplatten, Speicherkarten, CDs, DVDs, FTP oder ähnliche externe Speicherplätze.

#### *5.1.7.3 Gültigkeit*

Gilt für alle Mitarbeiter, die mit firmeneigenen Computersystemen arbeiten.

#### *5.1.7.4 Regeln*

*(1) Dürfen externe Speichersysteme, wie USB-Sticks, externe Festplatten, Speicherkarten eingesetzt werden?*

Der Einsatz von externen Speichermedien ist grundsätzlich verboten.
*Ausnahme:* Der Einsatz wird vom EDV Leiter genehmigt.
Üblicherweise dürfen genehmigte externe Datenträger auch nur zum Austausch von Daten zwischen firmeninternen Systemen verwendet werden, wenn einzelne Systeme nicht am Firmennetz angeschlossen sind. (Ausnahmen müssen mit EDV Leiter abgeklärt werden).

*(2) Wann und wie dürfen Daten von externen CDs, DVDs, FTP od. ähnliche externe Speicherplätze verwendet werden?*

Wenn, aus für die Firma gewichtigen Gründen, externe Datenträger mit firmenfremden Daten (z.B. Kundendaten) an Firmenrechnern verwendet werden, so darf es sich ausschließlich um Daten aus seriösen Quellen handeln. Die Beurteilung der Seriosität und damit die Verantwortung liegen beim einzelnen Mitarbeiter. Dabei ist noch zusätzlich zu beachten, dass diese Daten nur an einem Rechner mit aktuellem Virenscanner eingelesen werden dürfen, bevor sie auf anderen firmeninternen Rechnern auch verwendet werden dürfen.

*(3) Sind private Datenträger im Unternehmen erlaubt?*

Private externe Datenträger dürfen nicht in die Firma mitgenommen werden.
Grundsätzlich dürfen keine privaten Datenbestände auf Firmensystemen kopiert werden. Die Mitnahme von Firmendaten ist nur nach Absprache mit der IT- oder Firmenleitung gestattet.

### 5.1.8 Ausnahmen und Änderungen

Ausnahmen und Änderungen müssen generell möglich sein, da ein Regelwerk nicht alle Eventualitäten vorhersehen kann.
Es ist jedoch zunächst eine Vorgangsweise zu wählen, die der geltenden IT-Sicherheitsrichtlinie entspricht. Erst wenn dies technisch oder organisatorisch nicht möglich oder kaufmännisch bedenklich ist, kann über eine Ausnahmeregelung entschieden werden.
Ausnahmen werden nur zeitlich begrenzt genehmigt, da sie sonst von Regeln nicht mehr unterscheidbar sind. Die Dauer der Ausnahme wird in der Dokumentation vermerkt.
Eine mögliche Verlängerung muss neu genehmigt werden.

Ausnahmen werden darüber hinaus auf Zweck, Ort und Benutzerkreis eingeschränkt.

Ausnahmen müssen hinsichtlich Antrag, Genehmigung, Verlängerung und Ablaufdatum dokumentiert werden. Sie werden einem eigenen Ordner in der IT-Abteilung gesammelt und beschrieben und periodisch überprüft.

Ausnahmen werden kontrolliert und im Falle des Auslaufens ohne Neuantrag nach entsprechender Frist aufgehoben.

## 5.2 Richtlinie Datensicherung

### 5.2.1 Kenndaten der Richtlinie

#### *5.2.1.1 Zweck/Ziel*

Diese Richtlinie soll vor dem Verlust von Daten schützen und eine spätere Wiederherstellung der Daten ermöglichen. Es werden die Sicherungsmedien und die zu sichernden Daten angeführt.

#### *5.2.1.2 Geltungsbereich*

Die Richtlinie gilt verpflichtend für alle Mitarbeiter, welche mit der Datensicherung und allfälliger Wiederherstellung von Daten in Berührung kommen.

#### *5.2.1.3 Verantwortlichkeit*

Die Erstellung und Änderung der Richtlinie obliegt dem IT-Prozesseigner. Für den Inhalt tragen der IT-Leiter und der Vorstand die Verantwortung.

#### *5.2.1.4 Überprüfung der Einhaltung*

Die Einhaltung der Richtlinie wird regelmäßig aber auch anlassbezogen überprüft.
Die notwendigen Maßnahmen, die im Wiederherstellungsfall zu ergreifen sind, sind im *Notfallplan Datenwiederherstellung* (Kapitel 5.4) angeführt.

### 5.2.2 Sicherungsmedien und Lagerungsdauer

#### *5.2.2.1 Sicherungsmedien*

Zur Datenarchivierung finden HP Ultrium Sicherungsdatenbänder Verwendung. Diese haben bei ordnungsgemäßer Lagerung (Verpackung, Temperatur, Luftfeuchtigkeit) eine Datenerhaltungsdauer bis zu 30 Jahren. Sichergestellt wird die ordnungsgemäße Lagerung durch Aufbewahrung in einem Bankschließfach.

#### *5.2.2.2 Lagerungsdauer der Daten*

Die Daten müssen zumindest 15 Jahre im Bankschließfach aufbewahrt werden. Durch die stetige Aktualisierung der Sicherungslaufwerke und Sicherungsmedien wird diese Lagerungszeit möglich.

#### 5.2.2.3 Aktualisierung der Sicherungsmedien

Werden die Sicherungslaufwerke und die Sicherungsmedien auf eine neue Technologie umgestellt, werden alle vorhandenen Datensicherungen auf die neuen Medien kopiert, dies schließt auch alle Datenträger mit ein, die im Bankschließfach gelagert sind. Ein solcher Technologietransfer hat spätestens alle 10 Jahre zu erfolgen (in der Praxis wird dieser durch den sich stetig steigernden Datenzuwachs schon früher erfolgen). Durch diesen Technologietransfer ist gewährleistet, dass die Lagerungsdauer der Sicherungsmedien weiter verlängert wird. Der erfolgreiche Transfer der Daten auf die neuen Sicherungsmedien wird durch eine Datenintegritätsüberprüfung überprüft. Diese Überprüfung wird durch das Sicherungsprogramm nach dem Kopieren gemacht. Nach dieser Überprüfung werden die alten Sicherungsmedien zerstört, sodass keine Wiederherstellung von alten Medien mehr möglich ist.

#### 5.2.2.4 Überprüfung der Sicherungsmedien

Die Sicherungsmedien werden einem regelmäßigen Test unterzogen. Von einem Jahr werden quartalsweise Gesamtsicherungen im Bankschließfach abgelegt. Jedes Jahr werden die Medien stichprobenweise überprüft, in dem eine Datenwiederherstellung versucht wird. Ist diese erfolgreich, kann eine korrekte Funktion des Mediums angenommen werden. Die Auswahl der Stichproben folgt einem festgelegten System: Beginnend mit einem Schaltjahr werden alle 1. Quartalssicherungen eines jeden gespeicherten Jahres überprüft. Im Folgejahr werden alle 2. Quartalssicherungen überprüft, ein Jahr später werden alle 3. Quartalssicherungen überprüft und wiederum ein Jahr später werden alle 4. Quartalssicherungen überprüft. So ergibt sich ein Überprüfungsintervall von 4 Jahren. Wird ein defektes Sicherungsmedium entdeckt, werden zusätzlich alle Sicherungsmedien dieses Jahres überprüft.

#### 5.2.2.5 Wiederherstellung alter Dateiformate

Es muss gewährleistet sein, dass alte Dateiformate gelesen werden können. Dies erfordert die notwendigen Programme und Rechner, die zu dieser Zeit im Einsatz waren. Um die Lagerung von alter Hardware und der Programme zu umgehen, werden Festplattenimages von PCs mit relevanter Software erstellt. Diese Images werden mit den Jahressicherungen mitgesichert und im Bankschließfach verwahrt.

Die Software zur Erstellung der Images (dzt. Acronis TrueImage) wird ebenfalls mitgesichert, so ist eine Wiederherstellung der Images möglich. Um nun auf die alten Dateien zugreifen zu können, werden diese Images in virtuellen Umgebungen geladen und verwendet.

### 5.2.3 Datenarchivierung

#### *5.2.3.1 Daten*

Bei der Datensicherung müssen die Anwendungen einbezogen werden, die im *Desaster Recovery Konzept* (Kapitel 3.6.1) angeführt sind, auszugsweise sind diese im Folgenden angeführt.

- EDV-System Logistik Pur, Axavia, …
- Daten der Abteilungen Entwicklung, Produktion, Verwaltung, etc.
- Emailverkehr – Exchange Postfächer
- Intranetdaten
- Eigene Dateien jedes Mitarbeiters
- Richtlinien der Firewall
- ADS-Datenbank
- Konfigurationsdatei der Telefonanlage

Die Sicherung erfolgt nach folgender Tabelle:

| | |
|---|---|
| Sicherungsdatenträger (DT) | Datenband (Streamertape), mit Sicherungsdatum versehen |
| Sicherungsart/-umfang | Vollständige Datensicherung |
| Sicherungsdatum | Täglich (jeden Arbeitstag) |
| Ausführung durch | IT-Mitarbeiter |
| Einlagerung DT in der EDV-Abteilung/Serverraum | 8 Tapes von Mo-Do (je 2fach) der letzen 8 Arbeitstage<br>Überspielungsrhythmus: 14-tägig |
| Einlagerung DT im gr. Tresor | 4 Tapes von jedem Fr der zurückliegenden 4 Wochen<br>Überspielungsrhythmus: monatlich |
| Einlagerung DT auf Bank | 8 Tapes von jedem letzten Fr der Monate Jan, Feb, Apr, Mai, Jul, Aug, Okt und Nov<br>Überspielungsrhythmus: jährlich<br>4 Tapes von jedem letzten Fr der Monate Mrz, Jun, Sep, Dez<br>Überspielungsrhythmus: keiner (dauerhafte Archivierung) |

**Tabelle 17: Sicherung von Daten**

### 5.2.3.2 Medien

Für die Ablage von Daten, die nicht produktionswichtig sind (Bilder, Präsentationen, Videos, etc.) wird ein Medienserver verwendet.

Die Sicherung erfolgt nach folgender Tabelle:

| | |
|---|---|
| Sicherungsdatenträger (DT) | Datenband (Streamertape), mit Sicherungsdatum versehen |
| Sicherungsart/-umfang | Vollständige Datensicherung |
| Sicherungsdatum | Täglich (jeden Arbeitstag) |
| Ausführung durch | IT-Mitarbeiter |
| Einlagerung DT im großen Tresor Chefsekretariat | 4 Tapes von jedem Fr der zurückliegenden 4 Wochen<br>Überspielungsrhythmus: monatlich |
| Einlagerung DT auf Bank | 8 Tapes von jedem letzten Fr der Monate Jan, Feb, Apr, Mai, Jul, Aug, Okt und Nov<br>Überspielungsrhythmus: jährlich<br>4 Tapes von jedem letzten Fr der Monate Mrz, Jun, Sep, Dez<br>Überspielungsrhythmus: keiner (dauerhafte Archivierung) |

**Tabelle 18: Sicherung von Medien**

### 5.2.3.3 Betriebssysteme und Systempartitionen

Betriebssysteme und darauf installierte Programme werden nicht in der regelmäßigen Datensicherung berücksichtigt. Die Datenmenge wäre dadurch sehr groß und die Durchführung kompliziert. Es besteht auch nicht die Notwendigkeit, diese Daten regelmäßig zu sichern, da sie sich nur wenig verändern. Weiters sind diese Datenträger alle durch ein RAID-System soweit abgesichert, dass der Ausfall einer einzelnen Festplatte noch keinen Datenverlust nach sich zieht.

Die einzelnen Systempartitionen werden nach der Installation durch Images gesichert. Die Erstellung der Images erfolgt durch „Acronis True Image“. Die Images werden auf dem Server selbst (auf einer 2. Festplatte) und auf einem zentralen Netzwerkspeicher abgelegt. Bei einer größeren Aktualisierung des Systems (Installation zusätzlicher Programme) wird das Image aktualisiert.

#### *5.2.3.4 Domaincontroller und Active Directory*

Ein wichtiges System für die IT-Infrastruktur ist der Domaincontroller und das damit verbundene Active Directory. Es verwaltet die Benutzeraccounts und die Gruppenzugehörigkeit aller Mitarbeiter und damit die Anmeldung der Benutzer. Es sind in der Firmeninfrastruktur zwei Domaincontroller im Einsatz. Alle DC replizieren ihre ADS-Datenbank und verfügen so über eine abgeglichene Datenbank. Die ADS-Datenbank wird mit der normalen Sicherung mitgesichert.

### 5.2.4 Workstations

Die Arbeitsstationen an werden grundsätzlich nicht gesichert, da keine wichtigen Daten darauf gespeichert werden. Wird von einem Mitarbeiter überhaupt auf dem lokalen Datenträger (Festplatte C:\, D:\, etc. in der Workstation) gearbeitet, müssen alle Daten nach eigenem Ermessen, aber mindestens einmal pro Woche, am Daten- bzw. Medienserver (je nach Wichtigkeit der Daten) gesichert werden.

## 5.3 Richtlinie Datenschutz

### 5.3.1 Kenndaten der Richtlinie

#### *5.3.1.1 Zweck/Ziel*

Diese Richtlinie dient dem Schutz von Daten. Es werden verschiedene Punkte angeführt, die Datenschutz gewährleisten. Unter diese Punkte fallen die Sicherheit des Internetzugangs, der Virenschutz, die Passwörter, die Konfiguration von Arbeitsplatzrechnern, der Umgang mit Wechselmedien, Software-Updates und die Ressourcenvergabe. Weiters wird die Vorgehensweise beim Ausscheiden von Mitarbeitern und dem Ausscheiden von Hardware dokumentiert. Die in dieser Richtlinie beschriebenen Maßnahmen dienen auch dem Schutz von IT-Systemen durch Serverraumsicherung und Absicherung der Stromversorgung.

#### *5.3.1.2 Geltungsbereich*

Die Richtlinie gilt verpflichtend für alle IT-Mitarbeiter, welche mit dem Datenschutz, also mit der Betreuung der obigen Ziele, beschäftigt sind. Natürlich sind indirekt alle Mitarbeiter betroffen, die ein PC-System nutzen, für diese gilt aber die *IT-Sicherheitsrichtlinie für Mitarbeiter* (Kapitel 5.1), in der die für sie relevanten Richtlinien zusammen gefasst sind.

#### *5.3.1.3 Verantwortlichkeit*

Die Erstellung und Änderung der Richtlinie obliegt dem IT-Prozesseigner. Für den Inhalt tragen der IT-Leiter und der Vorstand die Verantwortung.

#### *5.3.1.4 Überprüfung der Einhaltung*

Die Einhaltung der Richtlinie wird regelmäßig aber auch anlassbezogen überprüft. Die notwendigen Maßnahmen, die im Fehlerfall zu ergreifen sind, sind bereits in diesem Dokument angeführt.

### 5.3.2 Sicherheit des Internetzugangs

Der Internetzugang soll vor aktiven Inhalten auf Webseiten und vor Schadprogrammen wie Viren, Würmern, Spyware und Adware geschützt werden. Weiters ist jeder Mitarbeiter dazu angehalten, keine Datenträger aus dem Privatbereich in der Firma zu verwenden. (siehe Kapitel 4), da dies ein großes Risiko darstellt.

#### *5.3.2.1 Hardware – Firewall*

Dem EDV-Netzwerk ist eine Firewall vorgeschaltet. Sie besteht aus einem physikalischen Rechner mit installierter Checkpoint-Firewall unter der Verwaltung der Firma SecureGUARD. Jeglicher Datenverkehr von innen nach außen wird über die Firewall geführt. Es werden nur die unbedingt notwendigen und tatsächlich gebrauchten Verbindungen erlaubt, alle anderen Verbindungen werden blockiert (Ports, Protokolle). Die Firewall wird automatisch mit Sicherheitspatches und Updates versorgt. Die Überwachung der Updates, die Funktion sowie die Konfiguration und Administration der Firewall ist von innen (Passwortschutz) und außen (sichere VPN-Verbindung) möglich. Größere Konfigurationsänderungen werden von der Firma SecureGUARD durchgeführt. Die Firewall steuert auch die VPN-Verbindungen zu den Außenstellen. An den Außenstellen ist eine gleichwertige Firewall-Infrastruktur vorhanden. Die Firewall ist mit einem Servicevertrag gesichert, die eine Reaktion innert 4 Stunden ermöglicht.
Die Konfiguration der Firewall wird regelmäßig gesichert (siehe *Richtlinie Datensicherung*).

#### *5.3.2.2 Personal – Firewall*

Jeder Laptop ist mit einer Personal-Firewall von Kaspersky ausgestattet. Diese Firewall bekommt ihre Updates und Patches von zentraler Stelle im EDV-Netzwerk. Die Firewall ist nur aktiv, wenn der Laptop nicht mit dem EDV-Netzwerk verbunden ist, da dann kein Schutz durch die Hardware-Firewall besteht.

#### *5.3.2.3 Virenschutz – global*

Dem EDV-Netzwerk ist eine Contentwall von Ikarus (physikalischer Server mit spezieller Software) vorgeschaltet. Die Contentwall überprüft den eingehenden Datenverkehr auf Schadprogramme und Emails. Emails werden zuerst auf einen

sogenannten Greylister weitergeleitet. Dieser blockt generell den ersten Empfang eines Emails und wartet auf den zweiten Sendeversuch. So werden die meisten Spammails erfolgreich abgewehrt.
Die Contentwall hat einen Spamfilter und einen Filter für gefährdende Anhänge (ausführbare Dateien, Skripte,...). Emails mit Spamverdacht werden im Betreff gekennzeichnet („possible spam“ oder „spam“) und in eigene Postfächer umgeleitet und dort 1 Woche lang aufbewahrt. Diese Postfächer werden wöchentlich durch einen Mitarbeiter überprüft, ob sich wichtige Emails darin befinden. Bei Emails mit gefährdenden Anhängen werden die Anhänge entfernt und das Email mit einem Vermerk an das normale Postfach weitergeleitet. Der Anhang wird im Quarantäne-Ordner der Contentwall gespeichert. Nach Unbedenklichkeitsprüfung kann dieser Anhang durch einen IT-Mitarbeiter wiederhergestellt werden.
Die Contentwall wird ebenfalls von der Firma SecureGUARD verwaltet und ist durch einen Servicevertrag gesichert, der eine Reaktion innert 4 Stunden ermöglicht.

#### *5.3.2.4 Virenschutz – lokal*

Jede Workstation, Laptop und jeder Server werden zusätzlich durch einen lokalen Virenscanner Kaspersky geschützt. Dieser wird zentral verwaltet und vollautomatisch mit Updates versorgt, wenn neue Virensignaturen erscheinen. Er kann auch nicht deaktiviert werden. Die funktionelle Überwachung dieser Vorgänge obliegt der IT Abteilung.

#### *5.3.2.5 Wireless LANs*

Derzeit ist ein WLAN-Access-Point im Einsatz. Er wird für Handscanner in der Lagerverwaltung benutzt. Für die Verschlüsselung wird WPA-PSK (Pre-Shared-Key) über das TKIP-Protokoll verwendet (Handscanner unterstützt WPA2 nicht). Der PSK wurde dabei möglichst lang gewählt. Weiters ist der WLAN-Zugriff auf den WLAN-Access-Point auf die MAC-Adresse des Handscanners beschränkt. Der Remotezugriff ist durch ein 10-stelliges Passwort gesichert. Der DHCP-Server am WLAN-Access-Point wurde deaktiviert.

#### *5.3.2.6 Sicherheit der Internet Browser*

Für den Zugang zum Internet benötigt man einen Internet Browser. Schwachstellen in den eingesetzten Internet-Browsern können durch Fehlbedienungen und falsches Benutzerverhalten, unzureichende Konfiguration der benutzten Browser und

Sicherheitslücken in den Browsern auftreten. Mitarbeiter werden in der *IT-Sicherheitsrichtlinie für Mitarbeiter* auf die Verwendung hingewiesen.

Weitere notwendige Punkte sind:

- Die Browser werden so konfiguriert, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann. Im Internet Explorer ist für das Internet zumindest die Stufe „Mittel“ auszuwählen. Der Internet Explorer ab Version 7.0 beinhaltet zudem Schutzvorkehrungen gegen Phishing-Angriffe.
- Internet-Browser werden immer auf dem neuesten Stand gehalten. Die Verteilung erfolgt über die automatischen Updates.
- Das Ausführen von aktiven Inhalten (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script) sollte durch entsprechende Optionen unterbunden werden.
- Die Anzeige der Dateiendungen sollte aktiviert werden, um potenzielle Schadprogramme, die als E-Mail-Attachment geschickt werden, leichter zu erkennen. In MS Office soll der Makro-Virenschutz aktiviert und auf entsprechende Warnmeldungen geachtet werden.
- E-Mail-Clients sollten so eingestellt werden, dass Dateianhänge nicht automatisch geöffnet werden.

### 5.3.3 Passwörter

Passwörter haben grundlegende Bedeutung beim Schutz der IT-Systeme und Daten. Passwörter müssen ausreichend komplex sein, um nicht erraten werden zu können. Andererseits dürfen sie aber nicht so kompliziert sein, dass sie vergessen werden oder schriftlich notiert werden müssen. Dieser Kompromiss ist letztlich vom jeweiligen Benutzer abhängig, einige Grundregeln sollten dabei aber unbedingt beachtet werden:

- Namen, Vornamen, Geburtsdaten, tel. Durchwahlen, KFZ-Kennzeichen etc. dürfen nicht verwendet werden, da sie sind leicht ausfindig zu machen sind.
- Passwörter sollten nicht aus Begriffen bestehen, die in einem Wörterbuch stehen.
- Trivialpasswörter (aaaaaa, qwertz, 4711 ...) dürfen nicht verwendet werden.
- Das Passwort muss ausreichend lang sein (mind. 8 Zeichen).
- Passwörter sollten in regelmäßigen Abständen geändert werden (z.B. alle 90 Tage). Sie sollten aber auch immer dann geändert werden, wenn der Verdacht besteht, dass sie von einem Unbefugten ausfindig gemacht wurden. Jeder Mitarbeiter sollte wissen, auf welche Weise er sein Passwort ändern kann.

Die Passwort-Regeln für die Mitarbeiter sind in der *IT-Sicherheitsrichtlinie für Mitarbeiter* festgehalten.

### 5.3.4 Konfiguration der Arbeitsplatzrechner

Die folgende Konfiguration betrifft die IT-Mitarbeiter, die die Arbeitsplatzrechner zur Verfügung stellen. Verhaltensregeln für den Umgang mit Arbeitsplatzrechnern für die Mitarbeiter sind in der *IT-Sicherheitsrichtlinie für Mitarbeiter* festgehalten.

#### *5.3.4.1 Rechtestruktur*

Auf den Arbeitsplatzrechnern haben alle Benutzer Hauptbenutzerrechte. Eine Programminstallation durch den Benutzer ist nicht vorgesehen. Eine Ausnahme bilden die Mitarbeiter der Entwicklungsabteilung, die über Administrationsrechte verfügen. Dies ist erforderlich, da sie selbst regelmäßig Programmupdates (Compiler,…) durchführen müssen. Diese Updates sind mit der IT-Abteilung abgesprochen.
Die „Eigenen Dateien“ sind auf ein Serverlaufwerk umgeleitet und werden dadurch bei der Sicherung berücksichtigt. Es dürfen keine firmenrelevanten Daten lokal auf dem Arbeitsplatzrechner gespeichert werden.

#### *5.3.4.2 Email-Programm*

Als Email-Programm wird Microsoft Outlook eingesetzt. Das Email-Programm ist aus Performancegründen bei einem Standgerät (Arbeitsstation) so konfiguriert, dass die Emails lokal gespeichert werden.

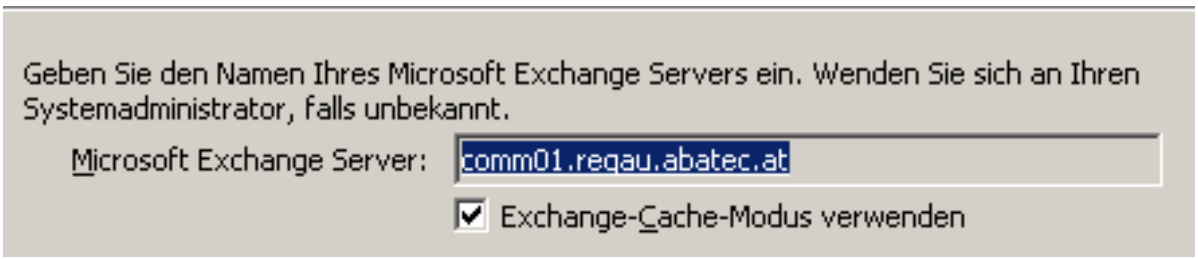



**Abbildung 19: Microsoft Outlook-Cache**

Bei einer mobilen Arbeitsstation (Laptop) wird dieser Cache-Modus nicht verwendet. Es bleiben dadurch nach der Trennung mit dem Exchange-Server keine Emails lokal gespeichert.

#### 5.3.4.3 Wechselmedien

Wechselmedien, wie z.B. Disketten, CD-ROMs, USB-Sticks oder externe Festplatten, ermöglichen den raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich.

Derartige Risiken sind unter anderem:

- Booten von Betriebssystemen, durch die Schutzmechanismen umgangen werden können
- unbefugte Installation unerwünschter Software oder Schadsoftware
- unberechtigtes Kopieren von Unternehmensdaten (Datendiebstahl)

Wechselmedien sollten völlig gesperrt werden, dies ist aber sehr schwer durchsetzbar. Es wird daher auf die *IT-Sicherheitsrichtlinie für Mitarbeiter* (Kapitel 5.1) verwiesen, in der die Verwendung von Wechselmedien eindeutig geregelt ist.

#### 5.3.4.4 Verschlüsselung

Verschlüsselung wird für die mobilen Arbeitsstationen (Laptops) angewendet, da hier ein Diebstahl am Wahrscheinlichsten ist. Als Verschlüsselungssystem wird eine transparente Verschlüsselung gewählt. Dabei wird die gesamte Festplatte des Rechners verschlüsselt, alle Dateien sind geschützt. Der Benutzer bemerkt davon nichts, er muss nur beim Rechnerstart ein Verschlüsselungspasswort eingeben. Um zu vermeiden, dass auf wichtige Daten nicht mehr zugegriffen werden kann, weil das Passwort zu ihrer Entschlüsselung verloren gegangen ist, werden Verschlüsselungspasswörter in verschlossenen Kuverts im Firmensafe deponiert.

### 5.3.5 Ressourcenvergabe

In diesem Bereich wird die Aufteilung der Ressourcen für die einzelnen Mitarbeiter behandelt. Als Ressourcen werden Datenzugriffe, Programmberechtigungen, Software und Hardware behandelt.

#### *5.3.5.1 Datenzugangsberechtigungen*

##### *(1) Allgemeine Berechtigungen*

Jeder Mitarbeiter erhält für seinen Bereich alle zur Erfüllung seiner Funktion erforderlichen Datenzugriffe bzw. Programmberechtigungen, in allen anderen Bereichen nicht. Freischalten von Berechtigungen erfolgt durch die IT Abteilung oder durch Mitarbeiter, die von der IT Abteilung oder vom Vorstand dazu ermächtigt wurden. Bei Unklarheiten betreffend Funktion oder Tätigkeit erfolgt die Einrichtung der Berechtigungen erst nach Rücksprache mit dem jeweiligen Bereichsleiter bzw. Projektleiter.

##### *(2) Neue Mitarbeiter*

Jeder neue Mitarbeiter erhält aufgrund seiner Funktion eine passende Basisausstattung in den verschiedenen Softwaresystemen und Datenbereichen. Die Funktion wird von der HR-Abteilung oder vom Bereichsleiter rechtzeitig bekannt gegeben und mittels des Abstimmungsgespräches der IT mit dem zuständigen Bereichsleiter endgültig fixiert. In den Softwaresystemen und Datenbereichen selber sind dafür unterschiedliche Standardrollen vorgesehen, die dem Mitarbeiter dann zugeschrieben werden.

##### *(3) Erweiterung von bestehenden Berechtigungen*

Erweitert sich der Funktionsbereich eines Mitarbeiters, kann seitens des Mitarbeiters eine Ausweitung seiner Datenzugangsberechtigung schriftlich (z.B. per Email) bei der IT-Leitung beantragt werden. Falls bei der IT-Leitung Unklarheit besteht, ob die Ausweitung berechtigt ist, wird beim zuständigen Bereichsleiter ebenfalls schriftlich rückgefragt und bei positivem Ergebnis die Erweiterung durchgeführt.

#### 5.3.5.2 Hardware

##### (1) Neue Mitarbeiter

Jeder neue Mitarbeiter erhält aufgrund seiner Funktion eine passende Basisausstattung an Hardware. Unmittelbar nach Einstellung des neuen Mitarbeiters bekommt die IT eine Information von der HR-Abteilung. Die HR-Abteilung beauftragt den für den neuen Mitarbeiter zuständigen Bereichsleiter damit, eine Abstimmung mit der IT über die benötigten Ressourcen herbeizuführen. Um der IT die nötige Beschaffungsvorlaufzeit zu ermöglichen, hat diese Abstimmung bei „Standardmitarbeitern“ mindestens 2 Wochen vor Arbeitsbeginn, bei Verkäufern (Notebooks) u. CAD-Mitarbeitern oder anderen, mit speziellen Anforderungen an Hardware oder Software, mindestens 4 Wochen vor Arbeitsbeginn zu erfolgen. Nach dem Abstimmungsgespräch ist vom zuständigen Bereichsleiter noch eine Bedarfsanzeige zu generieren und an die IT zu senden. Die IT kümmert sich dann um die rechtzeitige Beschaffung der Hardware für den neuen Mitarbeiter. Ebenfalls ist vom zuständigen Bereichsleiter rechtzeitig der künftige Arbeitsplatz des neuen Mitarbeiters anzugeben.

##### (2) Erweiterung und Erneuerung

Eine Erweiterung oder Erneuerung von Hardware erfolgt grundsätzlich über Bedarfsanzeigen.

#### 5.3.5.3 Software

##### (1) Allgemeine Bestimmungen

Die Verteilung von Software basiert auf der Funktion und Tätigkeit des einzelnen Mitarbeiters. Da Software durchwegs kostenpflichtig ist, werden hierbei die Kosten und der Nutzen gegenübergestellt und aufgrund dieser Analyse Rollout-Entscheidungen für die einzelnen Funktionen getroffen. Es kann hierbei auch sein, dass innerhalb der gleichen Funktionsgruppe nur für einen Mitarbeiter die Software verfügbar gemacht wird. Dieser wird dann dazu bestimmt, die mit der Software zusammenhängenden Vorgänge auch für die anderen zu erledigen.

*(2) Neue Mitarbeiter*

Jeder neue Mitarbeiter erhält aufgrund seiner Funktion eine passende Basisausstattung an Software. Unmittelbar nach Einstellung des neuen Mitarbeiters bekommt die IT eine Information von der HR-Abteilung. Die HR-Abteilung beauftragt den für den neuen Mitarbeiter zuständigen Bereichsleiter damit, eine Abstimmung mit der IT über die benötigten Ressourcen herbeizuführen. Die benötigte, der Funktion entsprechende, Standardsoftware wird nach einem Abstimmungsgespräch von der IT installiert. Ergibt sich beim Abstimmungsgespräch eine über die Standardsoftware hinausgehende Softwareanforderung, ist vom zuständigen Bereichsleiter noch eine Bedarfsanzeige zu generieren und an die IT zu senden. Die IT kümmert sich dann um die rechtzeitige Beschaffung der Software für den neuen Mitarbeiter.

*(3) Erweiterung und Erneuerung*

Eine Erweiterung oder Erneuerung von Software erfolgt grundsätzlich über Bedarfsanzeigen.

### 5.3.6 Softwareverteilung

#### *5.3.6.1 Updates*

Als Updates werden z.B. Patches, Virenupdates, Applikationsupdates, Servicepacks bezeichnet. Die Verteilung ist in den folgenden Punkten geregelt.

*(1) Updates auf Servern*

Die für den sicheren Betrieb von Servern notwendigen Updates werden von der IT Abteilung, unbemerkt von den Usern, regelmäßig eingespielt. Es handelt sich dabei meist um Sicherheitspatches des Betriebssystems und der installierten Programme.

*(2) Updates auf Clients*

Die Updates der Clients werden durch WSUS unterstützt. Bei den Windows Server Update Services (WSUS) handelt es sich um eine Patch- und Updatesoftware von Microsoft, bestehend aus einer Server- und einer Clientkomponente. WSUS lädt Updatepakete aus dem Internet (Microsoft Update) und bietet sie den Windows-

Clients zur Installation an. Die IT-Mitarbeiter legen am Server fest, welche Computer welche Updates installieren sollen. Die Updates werden zuerst getestet und dann schrittweise an die Clients verteilt.

#### *5.3.6.2 Upgrades*

Als Upgrade wird der Umstieg auf neuere Software-Version von Betriebssystemen, Applikationen und Firmware von Hardware bezeichnet.

##### *(1) Upgrades auf Servern*

Die für den sicheren Betrieb von Servern notwendigen Updates werden von der IT Abteilung, meist unbemerkt von den Usern, regelmäßig eingespielt. Als notwendig erachtet werden Upgrades dann, wenn sich daraus klare Vorteile (Beseitigung von Bugs, Handling od. Performance Vorteile) bei der Softwarenutzung ergeben.

##### *(2) Upgrades auf Clients*

Upgrades auf Clients werden von der IT Abteilung, wenn notwendig, ausgerollt. Die User werden vorher über den Vorgang informiert und teilweise aktiv mit einbezogen. Als notwendig erachtet werden Upgrades dann, wenn sich daraus klare Vorteile (Beseitigung von Bugs, Handling od. Performance Vorteile) bei der Softwarenutzung ergeben.

#### *5.3.6.3 Verteilung bestehender Software*

Die Verteilung bestehender Software basiert im Einklang mit der Funktion und Tätigkeit des einzelnen Users. Da Software durchwegs kostenpflichtig ist, werden hierbei die Kosten und der Nutzen gegenübergestellt und aufgrund dieser Analyse Rollout-Entscheidungen für die einzelnen Funktionen getroffen. Es kann hierbei auch sein, dass innerhalb der gleichen Funktionsgruppe nur für einen Mitarbeiter die Software verfügbar gemacht wird. Dieser wird dann dazu bestimmt, die mit der Software zusammenhängenden Vorgänge auch für die anderen zu erledigen.

#### *5.3.6.4 Einführung neuer Software*

##### *(1) Kleine Softwareprojekte*

Kleine Softwareprojekte betreffen meist nur einen oder wenige Benutzer. Die Auswahl einer neuen Software erfolgt nach folgendem Ablauf:

- Projektteam bilden, bestehend aus dem Spezialisten zum Thema und IT
- Software-Auswahlprozess starten (Marktanalyse, Testinstallation, Integrationsprüfung, Analyse Outputweiterverarbeitung)
- Erwerb und Installation der Software
- Anpassung und Einsetzen der neuen Software

##### *(2) Große Softwareprojekte*

Große Softwareprojekte betreffen große Teile oder die gesamte Firma. Die Auswahl einer neuen Software erfolgt nach folgendem Ablauf:

- Projektleiter ist hier die IT-Abteilung
- Projektteam bilden, bestehend aus dem Spezialisten zum Thema und IT
- Software-Auswahlprozess starten (Marktanalyse, Testinstallation, Integrationsprüfung)
- Softwaretest und Anpassung (Testinstallation, mind. 2 Testprojekte anlegen, Software anpassen, Fehler beseitigen)
- Schulung der künftigen Teilnehmer (fallweise Testinstallation)
- Systemweites Rollout → Arbeit mit der neuen Software
- Software Verbesserungen (Anpassung u. Beseitigung von Problemen, die sich erst während der praktischen systemweiten Anwendung zeigen)
- Einsetzen der neuen Software

### 5.3.7 Mitarbeiterabgänge

Beim Ausscheiden von Mitarbeitern aus dem Unternehmen sollten folgende grundlegende Punkte beachtet werden:

- Sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. Notebook, Handy, Blackberry, Speichermedien, Dokumentationen) sind zurückzufordern.
- Datenbestände des abgehenden Mitarbeiters müssen konsolidiert und übergeben werden.
- Der Abgang ist von der HR-Abteilung der IT-Abteilung bekannt zu geben und eliminiert in Absprache mit dem Vorgesetzten sämtliche Zugangsberechtigungen und Zugriffsrechte.
- Wenn eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt wurde (z.B. mittels eines gemeinsamen Passwortes), muss nach Ausscheiden einer der Personen die Zugangsberechtigung sofort geändert werden.

- Wenn Administratoren oder andere Schlüsselpersonen ausscheiden, müssen auch alle anderen Passwörter geändert werden, die ihnen bekannt waren.
- Das bestehende Benutzerkontos darf nicht an einen anderen Mitarbeiter weitergegeben werden.
- Das Benutzerkonto wird im Active Directory deaktiviert, damit eine Anmeldung nicht mehr möglich ist und nach Maßgabe gelöscht.
- Das Emailkonto wird an den neuen Verantwortlichen zuerst weitergeleitet und später dann gelöscht, dies ist im Microsoft Exchange Server einzustellen.
- Wenn es sich bei dem Abgang um einen Bereichsleiter oder Business-Unit-Leiter handelt, übernimmt in diesem Fall der bereits bestimmte Nachfolger oder, wenn nicht vorhanden, der IT Leiter die Rolle des Vorgesetzten.

Der unmittelbare Vorgesetzte ist für die Durchführung dieser Handlungen verantwortlich.

### 5.3.8 Auszuscheidende Hardware

#### *5.3.8.1 Computer*

Vor dem Weggeben von Computern (Entsorgung, Flohmark, Schenkung), werden die Festplatten mit einer speziellen Software überschrieben. Dies ist notwendig, damit eine spätere Wiederherstellung der Daten vermieden wird. Wenn ein sicheres Löschen nicht möglich ist, weil es sich z.B. um ein spezielles Raidsystem handelt, müssen die Festplatten mechanisch irreparabel zerstört werden. Werden die Computer einer weiteren Verwendung in der Firma zugeführt, ist diese Maßnahme nicht notwendig.

#### *5.3.8.2 Wechseldatenträger*

Wechseldatenträger (CDs, DVDs, Disketten, USB-Sticks) müssen vor der Entsorgung mechanisch zerstört werden (Schredder,…).

#### *5.3.8.3 Schriftliche Aufzeichnungen*

Schriftliche Aufzeichnungen, die sensible Daten enthalten (Verzeichnisstruktur, Zugangskennungen, Netzwerkpläne,…) müssen vor der Entsorgung mechanisch zerstört werden (Schredder,…) und dürfen nicht im Papiercontainer entsorgt werden.

### 5.3.9 Serverraumsicherung

#### *5.3.9.1 Zugangssicherung*

Die Serverräume im Altbau und im Neubau werden täglich verschlossen. Schlüssel mit der entsprechenden Kodierung stehen ausschließlich befugten Personen zur Verfügung (IT Abteilung, Vorstand, Gebäudemanager)

#### *5.3.9.2 Klimaanlage*

Um die Server vor Überhitzung zu schützen, sind die Serverräume mit zwei unabhängig versorgten Klimaanlagen bestückt. Zusätzlich sind die Server temperaturüberwacht und werden bei Übertemperatur automatisch niedergefahren.

#### *5.3.9.3 Brandmeldeanlage*

Im Serverraum an der Decke und im Zwischenboden sind Rauchmelder installiert. Diese Melder lösen bei einem Überschreiten einer gewissen Rauchgaskonzentration einen Brandalarm aus.

### 5.3.10 Stromversorgung

#### *5.3.10.1 Stromversorgung*

Die Stromversorgung der beiden Serverräume und der darin befindlichen IT-Infrastruktur ist durch zwei unabhängig voneinander abgesicherte Stromkreise gewährleistet.

#### *5.3.10.2 USV*

Die Server sind durch eine USV-Anlage geschützt. Die Server werden bei Stromausfall nach wenigen Minuten herunter gefahren. Die beiden Domaincontroller werden als letzte abgeschaltet. Wird der Strom wieder eingeschaltet, fahren die Server nicht mehr automatisch hoch – dies muss per Hand erledigt werden, da die Reihenfolge des Hochfahrens wichtig ist (DC zuerst). Es ist während der Arbeitszeit immer ein IT-Mitarbeiter verfügbar, der diese Aufgabe übernimmt. Die USV-Anlage ist so ausgelegt, dass ein sicheres Herunterfahren der Server gewährleistet wird, ein erhaltender Betrieb (Notstrom) ist nicht vorgesehen.

## 5.4 Notfallplan Datenwiederherstellung

Im Notfallplan Datenwiederherstellung sind konkrete Maßnahmen beschrieben, die bei einer Datenwiederherstellung notwendig sind. Der Notfallplan enthält Kontaktadressen und Wiederherstellungsabläufe. Da diese Masterarbeit anonymisiert ist, fehlen konkrete Kontaktadressen und Wiederherstellungsmaßnahmen. Dieser Notfallplan ist eine Vorlage, um im konkreten Fall einen vollständigen Notfallplan erstellen zu können.

### 5.4.1 Kenndaten des Notfallplans

#### *5.4.1.1 Zweck/Ziel*

Dieser Notfallplan ist im Falle des Datenverlustes ein Leitfaden, um eine rasche Wiederherstellung der Daten ermöglichen.

#### *5.4.1.2 Geltungsbereich*

Dieser Notfallplan ist für alle Mitarbeiter, welche mit der Datenwiederherstellung betraut sind.

#### *5.4.1.3 Verantwortlichkeit*

Die Erstellung und Änderung dieses Plans obliegt der IT-Leitung.

#### *5.4.1.4 Überprüfung der Aktualität*

Die Einsatzfähigkeit soll einmal jährlich überprüft werden und im Anlassfall aktualisiert werden.

### 5.4.2 Beschaffung der Datenbänder

#### *5.4.2.1 Standort der Sicherungsbänder*

Die Lagerungsorte, die zu speichernden Daten und die dazugehörigen Sicherungsintervalle sind in der *Richtlinie Datensicherung* (Kapitel 5.3) angeführt. Hier werden die Standorte der Sicherungsbänder aufgezählt, damit ein rascher Zugriff auf die Sicherungsbänder möglich ist. Die Daten des Bankschließfaches werden hier anonymisiert.

*(1) Bänder der EDV-Abteilung*

| | |
|---|---|
| Standort | Büro der IT-Leitung, versperrbarer Wandschrank |
| Zugriff | alle IT-Mitarbeiter (Schlüssel) |
| Rücksicherung | alle berechtigten IT-Mitarbeiter |

*(2) Tresor Chefsekretariat*

| | |
|---|---|
| Standort | Tresor im Neubau, 1.Stock, Raum der Chefsekretärin |
| Zugriff | IT-Mitarbeiter, Chefsekretärin |
| Rücksicherung | alle berechtigten IT-Mitarbeiter |

*(3) Bankschließfach*

| | |
|---|---|
| Standort | Bank (anonym), Adresse, Telefonnummer |
| Öffnungszeiten | Montag 8 - 12 und 14 - 15:30 Uhr, Dienstag 8 - 12 und 14 - 15:30 Uhr, Mittwoch 8 - 12 Uhr, Donnerstag 8 - 12 und 14 - 17 Uhr, Freitag 8 - 15 Uhr durchgehend |
| Zugriff | der Bank als berechtigt gemeldete IT-Mitarbeiter, Buchhaltung, Authentifizierung erfolgt durch Ausweis und Mitnahme des Schließfachschlüssels |
| Rücksicherung | alle berechtigten IT-Mitarbeiter |

#### *5.4.2.2 Ansprechpersonen*

Hier werden die wichtigsten Ansprechpersonen angeführt, die für eine Beschaffung der Datenbänder notwendig sein können. Es sollten e-Mail Adressen und Telefonnummern der einzelnen Ansprechpartner angeführt sein.

| | |
|---|---|
| Kontaktperson1 | IT-Leiter, Name, Telefonnummer, email |
| Kontaktperson2 | IT-Mitarbeiter, Name, Telefonnummer, email |
| Kontaktperson3 | Chefsekretärin, Name, Telefonnummer, email |

#### *5.4.2.3 Auswahl des aktuellsten Sicherungsbandes*

Um das aktuellste Band auszuwählen, muss die Sicherungsart berücksichtigt werden. Bei der vollständigen Sicherung werden sowieso alle Dateien gesichert, d.h. es kann das letztmögliche Band zur Wiederherstellung verwendet werden. Bei der inkrementellen Sicherung (z.B. wöchentlich) benötigt man immer alle Sicherungsbänder der ganzen Woche.
Ist das aktuellste Band nicht mehr verfügbar (Brand, Defekt, Diebstahl,…) muss auf die Wochen- Monats- oder Jahresbänder im Tresor oder auf der Bank zurückgegriffen werden. Die Reihenfolge ist in der *Richtlinie Datensicherung* (Kapitel 5.2) angeführt.

### 5.4.3 Wiederherstellung

Die Wiederherstellung selbst unterscheidet zwischen dem Verlust einer oder mehrerer Dateien, dem Verlust von Emails, der Wiederherstellung nach einem Datenbankfehler, einem Totalausfall eines Servers oder eines Datenträgers oder der Wiederherstellung eines Domaincontrollers.

#### *5.4.3.1 Dateien*

Ausgewähltes Sicherungsband einlegen, Wiederherstellung starten und Datei wiederherstellen. Hier sollte einmal eine erfolgreiche Wiederherstellung einer Datei mit Hilfe von Screenshots beschrieben werden, damit man einen Musterablauf hat, wie eine Datei rückgesichert werden kann.

#### *5.4.3.2 Emails*

Ausgewähltes Sicherungsband einlegen, Wiederherstellung starten und Email wiederherstellen. Hier sollte einmal eine erfolgreiche Wiederherstellung einer Email mit Hilfe von Screenshots beschrieben werden, damit man einen Musterablauf hat, wie eine Email rückgesichert werden kann.

#### *5.4.3.3 SQL-Datenbank*

Ausgewähltes Sicherungsband einlegen, Wiederherstellung starten und SQL-Datenbank wiederherstellen. Hier sollte einmal eine erfolgreiche Wiederherstellung

einer Datenbank mit Hilfe von Screenshots beschrieben werden, damit man einen Musterablauf hat, wie eine Datenbank rückgesichert werden kann.

#### *5.4.3.4 Datenträger*

Bei dieser Wiederherstellung muss unterschieden werden, ob sich um einen Systemdatenträger oder um Datenträger mit reinem Speicherplatz handelt (Datenfestplatte). Da alle Serverdatenträger durch ein RAID-System gespiegelt werden, kommt es bei einem Ausfall einer Festplatte noch zu keinem Datenverlust sondern nur zu einem Geschwindigkeitsverlust. Nach dem Einbau des neuen Datenträgers synchronisiert RAID die Information wieder und der Betrieb sollte weiterlaufen. Alle anderen Fälle (Wiederherstellung) werden im Folgenden behandelt.

##### *(1) Datenfestplatte*

An dieser Stelle sollte die Kontaktadresse des Händlers notiert sein, damit ein rascher Neukauf einer Festplatte möglich ist. Idealerweise verfügt man über einen Hardware-Servicevertrag, dann sollte man hier die Kontaktdaten des Servicevertragshändlers notieren. Nach der Neubeschaffung der Festplatte wird diese eingebaut und die Wiederherstellung gestartet.

##### *(2) Systemdatenträger*

An dieser Stelle sollte die Kontaktadresse des Händlers notiert sein, damit ein rascher Neukauf einer Festplatte möglich ist. Idealerweise verfügt man über einen Hardware-Servicevertrag, dann sollte man hier die Kontaktdaten des Servicevertragshändlers notieren. Nach der Neubeschaffung der Festplatte wird diese eingebaut und das Image der Systempartition mit der Software „Acronis True Image“ zurückgespielt, es folgt die Wiederherstellung der Daten nach obiger Anleitung.
Ist das Systemimage nicht mehr verfügbar (durch Brand im Serverraum), muss die Systempartition durch Neuinstallation des Betriebssystems und der notwendigen Programme durchgeführt werden. Die Installationsdatenträger sind im Büro der IT-Abteilung gelagert. Notfalls sind diese Installationsdatenträger auch im EDV-Shop käuflich zu erwerben (Windows Server, SQL-Server,…).
Eine Lagerung der Systemimages in einem Bankschließfach ist nicht vorgesehen.

#### 5.4.3.5 Server und Hardware

An dieser Stelle sollte die Kontaktadresse des Händlers notiert sein, damit ein rascher Neukauf der ausgefallenen Hardware möglich ist. Idealerweise verfügt man über einen Hardware-Servicevertrag, dann sollte man hier die Kontaktdaten des Servicevertragshändlers notieren. Nach der Neubeschaffung der ausgefallenen Hardware (Server, Netzteil, Switch,…) ist diese wieder in Betrieb zu nehmen. Auf eine genaue Unterscheidung von möglichen Fehlerfällen wird hier verzichtet, da dies nicht primäres Ziel dieser Masterarbeit ist.
Nach Wiederherstellung der Infrastruktur (neuer Server…) können die Daten, wie oben beschrieben, wiederhergestellt werden.

#### 5.4.3.6 Domaincontroller

Bei der Wiederherstellung eines Domaincontrollers sind zwei Fälle zu unterscheiden:

- Wiederherstellung eines DC mit vorhandenem 2. DC (ADS noch vorhanden)
- Wiederherstellung eines DC ohne vorhandenem 2.DC (ADS nicht mehr aktiv)

Durch die Aufteilung der Domaincontroller auf zwei Standorte ist ein Totalausfall der ADS-Datenbank sehr unwahrscheinlich. Sie kann aber durch Fehlkonfiguration (löschen von Organisationseinheiten,…) unbrauchbar werden, daher ist auch dieser Fall beschrieben. Ist der Server selbst defekt, muss dieser zuerst ausgetauscht werden, die Vorgangsweise ist weiter oben beschrieben.

##### *(3) Aufwertung eines Servers zu einem Domaincontroller*

Nach der Wiederherstellung muss der Server zu einem Domaincontroller aufgewertet werden. Eine Aufwertung zu einem DC wird mit dem Programm „dcpromo“ durchgeführt. Das Programm wird auf der Kommandozeile des Servers gestartet.

##### *(4) Wiederherstellung eines DC mit vorhandenem 2.DC*

Die ADS-Datenbank muss von einem bestehenden DC repliziert werden.

##### *(5) Wiederherstellung eines DC ohne vorhandenen 2.DC*

Die ADS-Datenbank muss von einem Sicherungsdatenträger wiederhergestellt werden. Dazu wird das aktuellste Sicherungsband ausgewählt und die ADS-Datenbank von diesem Band wiederhergestellt.

## 5.5 Geheimhaltungs- und Abtretungserklärung

### 5.5.1 Allgemeines

Die Geheimhaltungs- und Abtretungserklärung schützt die Firma und deren Kunden vor der Weitergabe von Informationen und Werten. Sie sollte jedem neuen Mitarbeiter vorgelegt werden und nach einer einführenden Erklärung auch von diesem unterschrieben werden. Das Original verbleibt in der Personalakte und eine Kopie bekommt der jeweilige Mitarbeiter. Die vorliegende Erklärung musste der Ersteller dieser Masterarbeit am Beginn seiner Recherche bei der Firma unterzeichnen. Diese Erklärung sollte von ausnahmslos allen Mitarbeitern und Fremdarbeitern unterschrieben werden. Die folgende Mustererklärung wurde von der Personalabteilung der Firma erstellt und kann als Mustererklärung verwendet werden. Der Schriftzug „die Firma“ muss dann durch den aktuellen Firmennamen ersetzt werden.

### 5.5.2 Mustererklärung

Die Unterzeichneten verpflichten sich, über alle Geschäfts- und Betriebsgeheimnisse dieser Firma, Geschäftsgeheimnisse Dritter, die ihnen aufgrund ihrer Tätigkeit in Verbindung mit dem Projekt zugänglich gemacht werden, Stillschweigen zu bewahren, diese an niemanden, auch nicht andere Betriebsangehörige oder Mitarbeiter weiterzugeben und/oder nicht für sich selbst zu verwenden, soweit nicht im Rahmen der erteilten Aufträge ausdrücklich etwas anderes angeordnet wird. Als Geschäfts- und Betriebsgeheimnisse gelten alle nicht offenkundigen Vorkommnisse, im Zweifelsfall alles, was nicht schon anderweitig bekannt ist. Dies gilt auch für Informationen, welche üblicherweise als belanglos angesehen werden. Zu den Geschäfts- und Betriebsgeheimnissen gehören z.B. Arbeitsmethoden, Arbeitsprogramme, Daten über Kunden, Lieferanten und Bezugsquellen, Korrespondenz, Zeichnungen, Stücklisten, Musterteile, Mustergeräte, usw.
Die Unterzeichneten verpflichten sich, bei Beendigung des Auftragsverhältnisses alle in ihrem Besitz befindlichen Arbeitsunterlagen, Schriften sowie Bücher zurück zu geben. Sie sind nicht berechtigt, Abschriften von Unterlagen aller Art für sich anzufertigen und zu behalten. Schließlich verpflichten sie sich, diese Geschäfts- und Betriebsgeheimnisse auch nach der Beendigung der Mitarbeit am Projekt weder für

sich selbst, noch für Dritte zu verwerten oder derartige Produkte für sich selbst, oder für Dritte herzustellen oder herstellen zu lassen.

Die Unterzeichneten treten unentgeltlich sämtliche Rechte an Erfindungen, Verbesserungsvorschlägen und allen „Werken“, die sie bei der Mitarbeit am Projekt schaffen, an die Firma bzw. deren Kunden ab, bzw. räumen die Unterzeichneten ein übertragbares Werknutzungsrecht an allen Werken, insbesondere an den für die Firma bzw. deren Kunden erstellten technischen Beschreibungen und Zeichnungen, wie z.B. an Programmen, Verbesserungsvorschlägen und Erfindungen ein, gleichgültig ob die Erstellung im Auftrag der Firma erfolgt, oder ob die Erfindung, der Verbesserungsvorschlag oder das Werk für einen Kunden von der Firma erstellt wird.

Die Unterzeichneten verpflichten sich, alle in Verbindung mit dieser Abtretung notwendigen Formulare innerhalb von 14 Tagen nach Aufforderung zu unterzeichnen.

Die Firma und deren Kunde sind berechtigt, diese Entwicklungen, Erfindungen, Verbesserungsvorschläge oder Werke nach eigenem Ermessen unentgeltlich, zur Gänze oder teilweise, oder gar nicht zu nutzen.

Datum…….. Unterschrift ……

## 5.6 Checkliste

Die Fragen in diesem Kapitel fassen den Inhalt von empfohlenen Sicherheitsmaßnahmen kurz zusammen und ermöglichen einen schnellen Überblick über die Schwachstellen im eigenen Unternehmen. [BSILF, Kapitel 10.1]

### 5.6.1 Informationssicherheitsmanagement

| | |
|---|---|
| | *Hat die Unternehmens- bzw. Behördenleitung die Informationssicherheitsziele festgelegt und sich zu ihrer Verantwortung für die Informationssicherheit bekannt?<br>Sind alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt worden?* |
| | *Gibt es einen IT-Sicherheitsbeauftragten?* |
| | *Werden Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?* |
| | *Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?* |
| | *Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen Sicherheitsmaßnahmen regelt?* |
| | *Ist bei allen Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z. B. Update des Viren-Schutzprogramms)?* |
| | *Sind für alle Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?* |
| | *Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?* |
| | *Sind die bestehenden Richtlinien und Zuständigkeiten allen Zielpersonen bekannt?* |
| | *Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.)?* |
| | *Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?* |
| | *Gibt es ein dokumentiertes Sicherheitskonzept?* |

### 5.6.2 Sicherheit von IT-Systemen

| | |
|---|---|
| | *Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt?* |
| | *Werden flächendeckend Viren-Schutzprogramme eingesetzt?* |
| | *Sind allen Systembenutzern Rollen und Profile zugeordnet worden?* |
| | *Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf? Gibt es sinnvolle Beschränkungen?* |
| | *Gibt es verschiedene Rollen und Profile für Administratoren oder darf jeder Administrator alles?* |
| | *Ist bekannt und geregelt, welche Privilegien und Rechte Programme haben?* |
| | *Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst oder wird der Auslieferungszustand beibehalten?* |
| | *Werden nicht benötigte sicherheitsrelevante Programme und Funktionen konsequent deinstalliert bzw. deaktiviert?* |
| | *Werden Handbücher und Produktdokumentationen frühzeitig gelesen?* |
| | *Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?* |

### 5.6.3 Vernetzung und Internet-Anbindung

| | |
|---|---|
| | *Gibt es eine Firewall?* |
| | *Werden Konfiguration und Funktionsfähigkeit der Firewall regelmäßig kritisch überprüft und kontrolliert?* |
| | *Gibt es ein Konzept, welche Daten nach außen angeboten werden müssen?* |
| | *Ist festgelegt, wie mit gefährlichen Zusatzprogrammen (PlugIns) und aktiven Inhalten umgegangen wird?* |
| | *Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?* |
| | *Sind Web-Browser und E-Mail-Programm sicher konfiguriert?* |
| | *Sind die Mitarbeiter ausreichend geschult?* |

### 5.6.4 Beachtung von Sicherheitserfordernissen

| | |
|---|---|
| | *Werden vertrauliche Informationen und Datenträger sorgfältig aufbewahrt?* |
| | *Werden vertrauliche Informationen vor Wartungs- oder Reparaturarbeiten von Datenträgern oder IT-Systemen gelöscht?* |
| | *Werden Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?* |
| | *Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?* |
| | *Werden bestehende Sicherheitsvorgaben kontrolliert und Verstöße geahndet?* |

### 5.6.5 Wartung von IT-Systemen: Umgang mit Updates

| | |
|---|---|
| | *Werden Sicherheits-Updates regelmäßig eingespielt?* |
| | *Gibt es einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informiert?* |
| | *Gibt es ein Testkonzept für Softwareänderungen?* |

### 5.6.6 Passwörter und Verschlüsselung

| | |
|---|---|
| | *Bieten Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung? Sind die Sicherheitsmechanismen aktiviert?* |
| | *Wurden voreingestellte oder leere Passwörter geändert?* |
| | *Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?* |
| | *Werden Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert?* |
| | *Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?* |

### 5.6.7 Notfallvorsorge

| | |
|---|---|
| | *Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?* |
| | *Werden alle notwendigen Notfallsituationen behandelt?* |
| | *Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?* |

### 5.6.8 Datensicherung

| | |
|---|---|
| | *Gibt es eine Backupstrategie?* |
| | *Ist festgelegt, welche Daten wie lange gesichert werden?* |
| | *Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?* |
| | *Werden die Sicherungsbänder regelmäßig kontrolliert?* |
| | *Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?* |

### 5.6.9 Infrastruktursicherheit

| | |
|---|---|
| | *Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?* |
| | *Ist der Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden?* |
| | *Besteht ein ausreichender Schutz vor Einbrechern?* |
| | *Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?* |

# 6 SCHLUSSBEMERKUNG

Die Umsetzung von Sicherheitsstandards bei einem Elektronikunternehmen hat gezeigt, dass es Handlungsbedarf gibt. Es sind bei dieser Analyse viele kleinere und größere Mängel aufgetreten. Man darf nur nicht behaupten, es wäre die Sicherheit in diesem Unternehmen bewusst vernachlässigt worden. Die Wahrung der IT-Sicherheit ist zu einer sehr komplexen Aufgabe geworden und die Analyse erfordert sehr viel Zeit. Zeit ist Geld und daher wird meist für die Wahrung der IT-Sicherheit und die stete Kontrolle nur sehr eingeschränkt Zeit zur Verfügung gestellt. Alleine die Recherche der IT-Sicherheitsmängel in diesem Elektronikunternehmen dauerte ungefähr 150 Stunden. Diese Zeit stand für die IT-Abteilung dieser Firma nicht zur Verfügung, man konnte hier nur auf Aufgaben und Probleme reagieren, nicht aber den Ursachen auf den Grund gehen.

Spätestens seit dieser Masterarbeit sollte aber klar sein, dass es sich auszahlt, Zeit und Geld in ein durchdachtes Sicherheitsmanagement zu stecken. Es gibt auch für Unternehmen dieser Größe eine rechtliche Verpflichtung, ein gewisses Maß an IT-Sicherheit zu gewährleisten. Für potentielle Kunden wiederum ist es eine vertrauensbildende Maßnahme, mit der das Unternehmen gegenüber Mitbewerbern punkten kann. Das bringt Gewinne, die dann wieder in das IT-Sicherheitsmanagement einfließen können und der Kreis beginnt sich zu schließen.

Die gesetzten Maßnahmen und Richtlinien können eine dauerhafte Sicherung der IT-Sicherheit gewährleisten, aber die Arbeit an der IT-Sicherheit sollte ein ständiger Prozess sein.

Ein wichtiger Punkt, der für die Zukunft berücksichtigt werden soll, ist die Virtualisierung. Diese Technik vereinfacht die Administration und spart Energie- und Hardwarekosten. Natürlich erfordert Virtualisierung eine sorgfältige Planung.

Abschliessend darf angenommen werden, dass es sich bei dem Elektronikunternehmen um keinen Einzelfall handelt, sondern dass eine Analyse eines ähnlichen Unternehmens auch einen ähnlichen Mängel- und Maßnahmenkatalog ergeben würde.

# 7 LITERATUR UND LINKS


| | |
|---|---|
| [ASIT01] | A-SIT Statuten<br>http://www.a-sit.at/de/allgemein/asit_statuten.php |
| [ASIT02] | A-SIT Informationssicherheitshandbuch, Übersicht<br>http://www.a-sit.at/de/sicherheitsbegleitung/sicherheitshandbuch/index.php |
| [ASIT03] | A-SIT Informationssicherheitshandbuch Version 2.3, April 2007<br>http://www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf |
| [BELLE] | BellEquip, Serverraum- und Schranküberwachung, Juli 2010<br>http://www.bellequip.at/akcp-monitoring.htm |
| [BITCOM01] | BITCOM, Kompass der IT-Sicherheitsstandards, 4.Auflage, August 2009<br>http://www.bitkom.org/de/publikationen/38337_40496.aspx |
| [BÖNI08] | Dr. Michael Böni, Aussagen zur IT-Sicherheit, Firma shiftTHINK<br>http://www.lehrer-online.de/426104.php |
| [BSI100-1] | BSI-Standard 100-1, Managementsysteme für Informationssicherheit<br>https://www.bsi.bund.de/cae/servlet/contentblob/471450/publicationFile/30759/standard_1001.pdf |
| [BSI100-2] | BSI-Standard 100-2, IT-Grundschutz Vorgehensweise<br>https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30758/standard_1002.pdf |
| [BSI100-3] | BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz<br>https://www.bsi.bund.de/cae/servlet/contentblob/471454/publicationFile/30757/standard_1003.pdf |
| [BSI100-4] | BSI-Standard 100-4, Notfallmanagement<br>https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30756/standard_1004.pdf |
| [BSI-CC] | BSI, Leitfaden zur IT-Sicherheit auf Basis der Common Criteria<br>https://www.bsi.bund.de/cae/servlet/contentblob/487910/publicationFile/30515/cc_leitf_pdf.pdf |
| [BSI-ITGS] | BSI IT-Grundschutz, Startseite<br>http://www.it-grundschutz.de/ |
| [BSI-LF] | BSI, Leitfaden Informationssicherheit, Jänner 2009<br>https://www.bsi.bund.de/cln_165/DE/Themen/ITGrundschutz/LeitfadenInformationssicherheit/leitfaden_node.html |
| [COMP01] | CE Infosys – Free CompuSec<br>http://www.ce-infosys.com/deutsch/free_compusec/german_free_compusec.aspx |
| [ECKE08] | Eckert Claudia, IT-Sicherheit: Konzepte-Verfahren-Protokolle, 5.Auflage<br>ISBN 978-3-486-58270-3, Oldenburg Verlag |
| [FERMA] | ferma – Federation of European Risk Management Associations, “Der Risikomanagement-Standard”, 2003, http://www.ferma.eu/Portals/2/documents/RMS/RMS-German(2).pdf |
| [GFI-SC] | Glasfaserinfo, SC-Stecker<br>http://www.glasfaserinfo.de/sc.html |

| | |
|---|---|
| [GSTOOL] | BSI Grundschutz-Tool GSTOOL<br>https://www.bsi.bund.de/cln_165/ContentBSI/gstool/gstool.html |
| [GUG01] | Gebauer&Griller, LWL-Außenkabel Datenblatt<br>http://www.griller.at/images/pdf/DB_A-DQ(ZN)_ZB.pdf |
| [GUG02] | Gebauer&Griller, LWL-Faserspezifikation G50/125<br>http://www.ggriller.co.at/images/pdf/DB_Fasern%20G50.pdf |
| [HP4121] | Beschreibung HP ProCurve 4000M – J4121A<br>http://www.hp.com/rnd/support/manuals/8000_4000_2424.htm |
| [HP4858] | Beschreibung HP ProCurve Gigabit SX-LC Mini-GBIC – J4858C<br>http://www.hp.com/rnd/support/faqs/mini-GBICs.htm |
| [HP8699] | Beschreibung HP ProCurve 5406zl-48G – J8699A<br>http://h10144.www1.hp.com/products/switches/HP_ProCurve_Switch_5400zl_Series/overview.htm#J8699A |
| [HP9008] | Beschreibung HP ProCurve 2-Port 10-GbE SFP+ al Modul – J9008A<br>http://www.procurve.com/customercare/support/faqs/2910al.htm?jumpid=reg_R1002_USEN |
| [HP9064] | Beschreibung HP ProCurve 4204vl – J9064A<br>http://h10144.www1.hp.com/products/switches/HP_ProCurve_Switch_4200vl_Series/overview.htm#J9064A |
| [HP9147] | Beschreibung HP ProCurve 2910al – J9147A<br>http://h10144.www1.hp.com/products/switches/HP_ProCurve_2910al_Switch_Series/overview.htm#J9147A |
| [HP9150] | Beschreibung HP ProCurve 10-GbE SFP+ SR Transceiver – J9150A<br>http://www.procurve.com/products/accessories/J9150A/accessory.htm?jumpid=reg_R1002_USEN |
| [ISO27003] | International Organisation for Standardisation, ISO/IEC27003:2010<br>http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42105 |
| [ISO27004] | International Organisation for Standardisation, ISO/IEC27004:2009<br>http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42106 |
| [ISOITTF1] | ISO/IEC27000 IT Overview, Jan.2009, first edition<br>http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip |
| [ITS01] | IT Sicherheitshandbuch der WKO, 4.Auflage, September 2009<br>http://www.it-safe.at/DE/Handbuch/Sicherheitshandbuch/Online-Handbuch.aspx |
| [ITS02] | IT Mitarbeiterhandbuch der WKO, 3.Auflage, September 2009<br>http://www.it-safe.at/DE/Handbuch/Mitarbeiter-Handbuch/Mitarbeiter-Handbuch.aspx |
| [ITSM08] | IT-Sicherheitsmanagement nach ISO27001 und Grundschutz,<br>Auszug aus Google-Books, Kersten-Reuter-Schröder<br>http://books.google.at/books?id=ByulXmYu_RMC&printsec=frontcover&dq=IT-Sicherheitsmanagement+nach+ISO+27001&cd=1#v=onepage&q&f=false |
| [ITW-SX] | ITWissen Lexikon, 1000Base-SX, Jänner 2010<br>http://www.itwissen.info/definition/lexikon/IEEE-802-3-1000Base-SX-1000Base-SX.html |
| [JENZER04] | Dominik Jenzer, Risk Office, Risiko – Eine Begriffsdefinition, 2004<br>http://www.risk-office.ch/typo/uploads/tx_pdforder/Begriffsdefinition_Risiko.pdf |

| | |
|---|---|
| [KSI01] | Fachbegriffe der Lichtwellenleitertechnik<br>http://www.ksi.at/LWL/lwl-begriffe.htm |
| [KSI02] | Lichtwellenleiter Fasertypenübersicht<br>http://www.ksi.at/LWL/lwl-faseruebersicht.htm |
| [MCSE07] | DHCP-Server installieren, konfigurieren, authorisieren, 05.01.1997<br>http://www.mcse-certification.de/archives/131-DHCP-Server-installieren,-konfigurieren-und-autorisieren.html |
| [MIC01] | Microsoft Office Online, Exchange Cache-Modus<br>http://office.microsoft.com/de-at/outlook/HP012329351031.aspx |
| [MÜHL07] | Prof. Jörg R. Mühlbacher, Vorlesung „Einführung IT-Sicherheit“ WS2007,<br>JKU Linz, Vorlesungsskript „IT_Sicherheit: Themenstellung“ |
| [PETRI01] | Petri IT, Problems with Exchange 2003 Installed on Domain Controllers<br>http://www.petri.co.il/problems_with_exchange_2003_installed_on_domain_controllers.htm |
| [PNC01] | PNC Newsletter, Email Signatur im Gesetz geregelt, 15.Juni 2008<br>http://www.pnc.at/newsletter/2008.06.15 |
| [PRESS07] | Pressetext Austria, IT-Challenge Unternehmensstrafrecht, 09.10.2007<br>http://www.pressetext.at/news/071009005/it-challenge-unternehmensstrafrecht-ausweg-aus-der-haftung/ |
| [PUTTY] | PuTTY, Simon Tatham, SSH- und Telnet-Client, Jänner 2010<br>http://www.putty.org/ |
| [QUAL01] | Qualys – On Demand Security<br>http://www.qualys.com/ |
| [RFC1519] | IETF.org, Classless Interdomain Routing (CIDR), September 1993<br>http://www.ietf.org/rfc/rfc1519.txt |
| [RFC1878] | IETF.org, Variable Length Subnet Table For IPv4. Dezember 1995<br>http://www.ietf.org/rfc/rfc1878.txt |
| [RFC1918] | IETF.org, Address Allocation for Private Internets, Februar 1996<br>http://www.ietf.org/rfc/rfc1918.txt |
| [RFC2131] | IETF.org, Dynamic Host Configuration Protocol (DHCP), März 1997<br>http://www.ietf.org/rfc/rfc2131.txt |
| [SCHBI07] | Univ.Doz. Dr. Ingrid Schaumüller-Bichl, Vorlesung „Einführung IT-Sicherheit“ WS2007<br>JKU Linz, Vorlesungsskript „Sicherheitshandbuch_2007-12-12“ |
| [SCHBI08] | Univ.Doz. Dr. Ingrid Schaumüller-Bichl, Vorlesung „Einführung IT-Sicherheit“ WS2007<br>JKU Linz, Vorlesungsskript „IT-Grundschutz_2008-01-16“ |
| [SCHBI081] | Univ.Doz. Dr. Ingrid Schaumüller-Bichl, Vorlesung „Einführung IT-Sicherheit“ WS2007<br>JKU Linz, Vorlesungsskript „ISO27000-Familie_2008-01-09“ |
| [SCHR01] | Schrack, Datenblatt Universal LWL-Kabel<br>http://shop.schrack.at/b2b_schrack/pages/FileTransfer.jsp?file=Online/datenblaetter/h_hseaibhxxxx_xx_01_at_de.pdf |
| [SICK01] | Sicherheitskultur und Informationssicherheit, Philipp Schaumann<br>http://www.sicherheitskultur.at/ |

| | |
|---|---|
| [SICK02] | Informationssicherheit und das Eisbergprinzip, Philipp Schaumann<br>http://www.sicherheitskultur.at/Eisbergprinzip.htm |
| [SICK03] | Sicherheitstipps IT-Security, Heinz Wachmann<br>http://www.sicherheitskultur.at/Eisberg_titanic.htm#tipps |
| [SICK04] | Informationssicherheit und Recht, Michael Pilz<br>http://www.sicherheitskultur.at/Eisberg_jus.htm#einfuehrung |
| [SICK05] | Was ist Social Engineering, Philipp Schaumann, Dez.2009<br>http://sicherheitskultur.at/social_engineering.htm |
| [STAT09] | Statistik Austria – IKT Einsatz in Unternehmen 2009<br>http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_unternehmen_e-commerce/index.html |
| [STE01] | Security in Safety Critical Systems, David Sternberger<br>http://www.vmars.tuwien.ac.at/courses/akti12/journal/03ss/article_03ss_Sternberger.pdf |
| [TEIA1] | Teialehrbuch, Risikoidentifikation, Juli2010,<br>http://www.teialehrbuch.de/Kostenlose-Kurse/Unternehmensfuehrung/23183-Risikoidentifikation.html |
| [TEIA2] | Teialehrbuch, Risikobeurteilung, Juli2010,<br>http://www.teialehrbuch.de/Kostenlose-Kurse/Unternehmensfuehrung/23184-Risikobewertung.html |
| [UNIFR01] | Universität Freiburg, Definition der IT-Sicherheit, Mai2010<br>https://www.unifr.ch/it-security/de/definition |
| [VERINICE] | verinice, OpenSource ISMS-Tool für Management der IS, 2008<br>http://www.verinice.org/Home.36.0.html |
| [WIKI-IEC] | Wikipedia, International Elektrotechnical Commission, Juli 2010<br>http://de.wikipedia.org/wiki/International_Electrotechnical_Commission |
| [WIKI-ISO] | Wikipedia, International Organisation for Standardization, Juli 2010<br>http://de.wikipedia.org/wiki/International_Organization_for_Standardization |


Alle angegebenen Links wurden am 20.August 2010 überprüft.

# 8 TABELLEN- UND ABBILDUNGSVERZEICHNIS

## 8.1 Abbildungsverzeichnis

## 8.2 Tabellenverzeichnis

# 9 LEBENSLAUF

| | |
|---|---|
| Name | **Roland Pachinger, Ing. Bakk.techn.** |
| Geburt | 1973 in Vöcklabruck |
| Anschrift | 4863 Seewalchen, Steindorf 148 |
| Staatsbürgerschaft | Österreich |
| Telefon | +43/7662/29372 |
| e-Mail | r.pachinger@gmx.at |
| Familienstand | verheiratet, 3 Kinder |

## Ausbildung:

| | |
|---|---|
| 1979 – 1983 | Volksschule Seewalchen |
| 1983 – 1987 | Hauptschule Seewalchen |
| 1987 – 1988 | HTL Vöcklabruck, Betriebstechnik |
| 1988 – 1992 | Berufschule I Gmunden<br>22.06.1992 – Lehrabschlußprüfung Meß- und Regelmechaniker<br>30.06.1992 – Lehrabschlußprüfung Betriebselektriker |
| 1992 – 1996 | Abendschule HTL Linz, Paul-Hahn, Elektrotechnik<br>28.06.1996 – Reifeprüfung HTL-Linz Elektrotechnik |
| Seit Okt. 2003 | Studium der techn. Informatik, JKU Linz<br>30.03.2007 – Bachelorprüfung Bakk.techn. |

## Berufserfahrung:

| | |
|---|---|
| 23.10.1988 – 30.06.1992 | Meß- und Regelmechaniker und Betriebselektriker<br>Lehrzeit in der Lenzing AG |
| 01.07.1992 – 28.02.1993 | Präsenzdienst Militärkommando OÖ |
| 01.03.1993 – 29.02.1996 | Zeitsoldat bei der Militärmusik OÖ am Instrument Flügelhorn, Militärkommando ÖO |
| 21.10.1996 – 31.10.2000 | EDV Administrator + Hardware Entwickler<br>ABATEC Electronic GmbH., 4844 Regau |
| 01.11.2000 – 31.07.2001 | EDV-Administrator bei der Stadtgemeinde<br>4840 Vöcklabruck |
| seit 10.09.2001 | Lehrer für Computerwerkstatt und Netzwerklabor<br>HTL Vöcklabruck, 4840 Vöcklabruck |

## Interessen:

| | |
|---|---|
| seit 1997 | Kapellmeister der Marktmusikkapelle Seewalchen |

# 10 EIDESTATTLICHE ERKLÄRUNG

Ich erkläre an Eides statt, dass ich die vorliegende Masterarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.
Des weiteren versichere ich, dass ich diese Masterarbeit weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Seewalchen, August 2010 ……

Roland Pachinger