Fachhochschule Köln
Cologne University of Applied Sciences

Diplomarbeit

zur Erlangung des Grades

Diplom Informatiker

"Studie zur Kompatibilität und Interoperabilität von Informationssicherheitsmanagementsystemen"

Erstprüfer:	Prof. Dr. Stefan Karsch
Zweitprüfer:	Prof. Dr. Hans Ludwig Stahl
Autor:	Daniel Jedecke
	Luisenweg 6
	D-53919 Weilerswist
E-Mail:	diplom@daniel-jedecke.de
Matrikelnr.:	11036816
Referenz:	Diplomarbeit.tex
Version:	v1.0
Datum:	12. August 2006

Vorwort

Ich möchte mich bei allen Personen bedanken, die mich in der Zeit der Erstellung dieser Arbeit so tatkräftig unterstützt und mir den Rücken freigehalten haben.

Danke an Prof. Dr. Karsch für die Unterstützung und Betreuung dieser Diplomarbeit.

Danke auch an Prof. Dr. Stahl für die hilfreichen Kommentare.

Ein besonderer Dank gebührt auch Randolf Skerka, Holger von Rhein und Manuel Atug, die mir in vielerlei Hinsicht sehr geholfen haben.

Für die Bereitstellung des GSTOOL möchte ich dem Bundesamt für Sicherheit in der Informationstechnik danken.

Zudem danke ich der Firma SRC Security Research & Consulting GmbH für die Einblicke in das interessante Umfeld von Informationssicherheitsmanagementsystemen.

Mein Dank gebührt vor allem Inga – Danke für Deine Unterstützung und den einen oder anderen kritischen Kommentar.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Kapitel 1

Einführung

In diesem Kapitel: Grundsätzliches über diese Diplomarbeit.

1.1 Einleitung

In der heutigen Zeit nutzen immer mehr Unternehmen IT-Systeme und die aus der tiefen Einbindung in existierende Unternehmensprozesse entstehenden Vorteile und Chancen. Der Informations- und Kommunikationstechnologie wird von Unternehmensseite zunehmend eine hohe bis sehr hohe Bedeutung für die eigene Tätigkeit zugeschrieben[1].

Unternehmerische Tätigkeiten, die von IT-Systemen unterstützt werden, müssen mannigfaltigen Sicherheitskriterien gerecht werden. Ein Ausfall oder eine Fehlfunktion eines IT-Systems kann diese Sicherheitsziele verletzen. Die Auswirkungen eines solchen Störfalls werden mit dem Begriff "Risiko"bezeichnet. "Risiken sind die aus der Unvorhersehbarkeit der Zukunft resultierenden, durch "zufällige" Störungen verursachten Möglichkeiten, andere Werte als die geplanten Zielwerte zu erreichen."[2] Das um Prävention und Krisenbewältigung bemühte Risikomanagement muss "auf viele Dinge bestmöglich vorbereitet

[1] vgl. [BB-IKT], Seite 12
[2] [RISK-MITTEL], Seite 12

sein, um auf schwierige Fragen immer bessere Antworten zu finden"[3].

Sicherheitsziele entstehen durch gesetzliche Anforderungen oder durch den Charakter der unternehmerischen Tätigkeit. In der Folge bedeutet dies, daß es darum geht, Risiken durch Maßnahmen zu minimieren. Ein wichtiger Aspekt in der Planung von risikomindernden Maßnahmen ist es, darauf zu achten, daß die Maßnahmen für das jeweilige Risiko angemessen sind. "Gerade wenig spektakuläre Maßnahmen wie Prozessoptimierung, Ausbildung und Motivation von Mitarbeitern oder das Anfertigen von verständlichen Dokumentationen verbessern das Sicherheitsniveau in der Praxis sehr deutlich."[4]

Das Spektrum von Risiken ist enorm. Die möglichen Gegenmaßnahmen sind ebenfalls zahlreich. Beide lassen sich jedoch nicht in einem 1:1-Verhältnis aufeinander abbilden. Meist mindert eine einzelne Maßnahme mehrere Risiken. Den Risiken kann hierbei "durch ein Zusammenspiel von technischen und organisatorischen Maßnahmen"[5] begegnet werden.

"Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich niemals wieder ändert."[6]. Vielmehr müssen durch technische oder organisatorische Veränderungen ständig neue Maßnahmen entwickelt werden, um neuen Risiken zu begegnen. Dies macht eine kontinuierliche Fortschreibung des Maßnahmenkataloges erforderlich.

Als Ergebnis dieser Erkenntnisse erhalten wir zwei komplexe Aufgaben:

- Entwicklung von Maßnahmen an gegebenen Unternehmensprozessen
- Fortschreibung des Maßnahmenkataloges

[3] vgl. [SZENARIO-RISK], Seite 5
[4] vgl. [BSI-100-1], Seite 16
[5] vgl. [BSI-100-1], Seite 17
[6] vgl. [BSI-100-1], Seite 13

Diese beiden Aufgaben vereinen sich im **Sicherheitsmanagement**[7]. Im Kontext von Informations- und Kommunikationstechnologien finden sie sich im Informationssicherheitsmanagementsystem (ISMS) wieder.

Das Angebot an ISMS ist groß. Eine Vielzahl verschiedener Systeme bieten unterschiedliche Lösungsansätze, basierend auf divergenten Annahmen und Voraussetzungen bezüglich der Unternehmensprozesse und der vorhandenen Risiken.

So unterscheidet sich zum Beispiel der Payment Card Industry Data Security Standard (PCI DSS) [PCIDSS] von anderen ISMS durch die Voraussetzung, daß das Unternehmen Kreditkartendaten verarbeitet, speichert oder weiterleitet. IT-Grundschutz [BSI-100-2] des Bundesamts für Sicherheit in der Informationstechnik (BSI) hingegen ist ein sehr umfassendes ISMS, welches keine konkreten Annahmen oder Voraussetzungen definiert.

Ebenso wenig formuliert auch der International Standards Organisation (ISO) Standard 27001:2005 [27001] ausdrückliche Vorraussetzungen. Im Unterschied zum PCI DSS oder zum IT-Grundschutz definiert dieser Standard auch keine grundlegenden Risiken. Vielmehr müssen diese durch eine umfassende Risikoanalyse definiert werden[8].

1.2 Über diese Arbeit

Die Motivation zur Wahl dieses Themengebietes liegt in meiner fachlichen Ausrichtung. Berufsbedingt habe ich mich neben meinem Studium viel mit dem ISMS Payment Card Industry Data Security Standard (PCI DSS)[PCIDSS] beschäftigt und auch einige Erfahrungen mit dem IT-Grundschutz [BSI-100-2] des Bundesamts für Sicherheit in der Informationstechnik (BSI) sammeln können. Da ich mich auf den Bereich des Sicherheitsmanagements spezialisieren möchte und dort auch mit beiden Systemen arbeiten werde, lag für mich diese Studie über die Kombinationsmöglichkeiten nahe.

[7] siehe auch [SICHERHEITSMAN]
[8] siehe auch [BSI-100-3]

Der IT-Grundschutz ist ein in Deutschland anerkannter IT-Sicherheitsmanagement-Standard, welcher in Kapitel 3.2.1 näher erläutert wird.

Der PCI DSS ist ein primär von den Kreditkartenanbietern MasterCard und Visa entwickelter Standard und richtet sich an die Sicherheit von kreditkartendatenverarbeitenden Unternehmen. Im Gegensatz zu anderen Standards definiert hierbei der Kreditkartenanbieter das zu erwartende Risiko, was eine unternehmensspezifische Risikoanalyse obsolet macht. Die Entstehungsgeschichte und den Aufbau dieses Standards kann in Kapitel 3.2.2 nachlesen werden.

In Hinblick auf die Migration von IT-Grundschutz und International Standards Organisation (ISO) Standard 27001:2005 [27001] wird dieses Arbeitsumfeld immer interessanter.

Kapitel 2

Analyse der Aufgabenstellung

In diesem Kapitel: Aufgabenstellung und Zielsetzung.

2.1 Aufgabenstellung

Die Kombination verschiedener ISMS gewinnt in der heutigen Zeit, gerade bei international tätigen Unternehmen, immer mehr an Bedeutung. Beispielsweise wird die Auftragsvergabe oft an das Vorhandensein eines bestimmten ISMS gekoppelt. So ist es in Deutschland häufig der Fall, daß Unternehmen, welche für Bundesbehörden arbeiten, nach IT-Grundschutz [BSI-100-2] zertifiziert sein müssen.

International tätige Unternehmen unterhalten oftmals schon ein funktionierendes ISMS nach ISO 27001 [27001]. In diesem Fall ist es sehr interessant, die Übereinstimmungen verschiedener Systeme sowie auch ihre Konflikte zu kennen. Diese Konflikte treten in Zusammenhang mit Maßnahmen auf, die durch das ISMS gefordert werden, jedoch nationalen Gesetzen widersprechen. Bei großen, weltweit operierenden Unternehmen treten solche rechtlichen Probleme auf, wenn ein länderübergreifendes ISMS eingesetzt werden soll, jedes Land jedoch eigene Gesetze hat, welche im gewählten Managementsystem berücksichtigt werden müssen. Aus diesem Grund muss die Maßnahmenebene sehr ge-

nau betrachtet werden und gegebenenfalls entsprechend den gesetzlichen Vorgaben des Landes angepasst werden.

Im Rahmen dieser Arbeit soll die Kompatibilität und Interoperabilität verschiedener ISMS evaluiert werden. Hierbei geht es speziell um den IT-Grundschutz des BSI, den ISO Standard 27001:2005 und 17799:2005 [17799] sowie den PCI DSS [PCIDSS].

Diese Systeme haben bereits eine große Schnittmenge in ihren Vorgehensweisen, jedoch tauchen in einigen Bereichen Konflikte auf, welche teils einfach, teils durch weitergehende Maßnahmen aufgelöst werden können. Speziell für Unternehmen, welche Kreditkarten verarbeiten, gibt der PCI DSS neue Richtlinien vor, die teilweise im deutschen Recht nicht umsetzbar sind, oder in Konflikt zu bereits existierenden ISMS stehen[1].

2.2 Zielsetzung

An diesem Punkt setzt diese Arbeit an und versucht Konflikte bei der Kombination verschiedener ISMS herauszuarbeiten und Lösungsansätze aufzuzeigen. Speziell sollen die Möglichkeiten der Interoperabilität und Kompatibilität zwischen PCI DSS und IT-Grundschutz getestet werden.

Ziel der Arbeit ist, eine Übersicht über die bei der Kombination auftretenden Probleme zu liefern, und entsprechende Lösungsansätze zu bieten. Dabei werden im Rahmen einer exemplarischen Kombination der Maßnahmen der IT-Grundschutz-Kataloge [GSHB] mit den Maßnahmen PCI DSS Probleme beschrieben sowie konkrete Lösungsvorschläge bereitgestellt. Hierzu bediene ich mich des mittleren Profils [MITTLERES], welches eine beispielhafte Umsetzung von IT-Grundschutz in einem mittelständischen Unternehmen aufzeigt. Das Profil wird im Rahmen dieser Arbeit zu einem Unternehmen erweitert, das Kreditkartendaten verarbeitet. An diesem neuen Profil soll dann die exemplarische Kombination vorgenommen werden.

[1] vgl. [PCIAUDIT], Requirement 12.7 und Bundesdatenschutzgesetz[BDSG]

Im Rahmen dieser Kombination werden neue Bausteine nach Vorlage der IT-Grundschutz-Kataloge erstellt, welche das Vorgehen zur Kombination verdeutlichen. Aufgrund der Menge an Anforderungen seitens des PCI DSS werden nicht alle Anforderungen in Bausteine abgebildet. Vielmehr dienen die hier betrachteten Bausteine als Vorlage für eine weitere Umsetzung, welche jedoch nicht Bestandteil dieser Arbeit ist.

Die Erstellung der Bausteine wird komplett mit dem Programm GSTOOL[2] in der Version 4.0 des BSI durchgeführt.

Bevor jedoch die Kombination der ISMS durchgeführt wird, werden in Kapitel 3 die Grundlagen dieser Arbeit näher erläutert. Dies schließt die Definition eines ISMS sowie der verschiedenen existierenden ISMS ein.

In Kapitel 4 wird dann eine Analyse der verschiedenen ISMS durchgeführt, sowie erste Kombinationsmöglichkeiten erläutert.

An dieses Kapitel schließt das Kapitel 5 an, in welchem das Vorgehen zur Kombination verschiedener ISMS beschrieben wird.

Anschließend findet in Kapitel 6 eine exemplarische Kombination von vier Anforderungen des PCI DSS mit den Maßnahmen der IT-Grundschutz-Kataloge statt.

In den beiden letzten Kapiteln 7 und 8 wird ein Ausblick auf weitere mögliche Projekte im Rahmen der Kombination von ISMS geben, sowie ein persönliches Fazit aus dieser Arbeit gegeben.

[2] http://www.bsi.de/gstool/index.htm

Kapitel 3

Grundlagen

In diesem Kapitel: Beschreibung der Grundlagen zu dieser Arbeit.

3.1 Informationssicherheitsmanagementsysteme

Ein Managementsystem ist "Führungs- und Organisationssystem zur optimalen Unternehmensführung im Rahmen der eigenen Unternehmenspolitik und der für einen bestimmten Bereich festgelegten, möglichst quantifizierten Unternehmenszielen"[1]. Hierzu wird ein Regelkreis genutzt, welcher in Abbildung 3.1 gezeigt wird. Er besteht aus den folgenden Komponenten[2]:

- Ist-Analyse der Organisation, der Technik, der Mitarbeiterkenntnisse, der Unternehmenskultur u.a.
- Unternehmenspolitik/-leitlinien/-philosophie festlegen
- Ziele festlegen
- Maßnahmenprogramm zur Erreichung der Ziele festlegen
- Ressourcen zur Durchführung des Programms bereitstellen

[1] vgl. [NACH-MS], Seite 33
[2] nach [NACH-MS]

- die richtigen Maßnahmen durchführen
- Zielerreichung bzw. Zielabweichungen festestellen, ggf. Korrekturmaßnahmen definieren und durchführen
- Durchführung von Audits
- Bewertung der Auditergebnisse und Berücksichtigung neuer Erkenntnisse durch die Unternehmensleitung
- Festlegung neuer Ziele

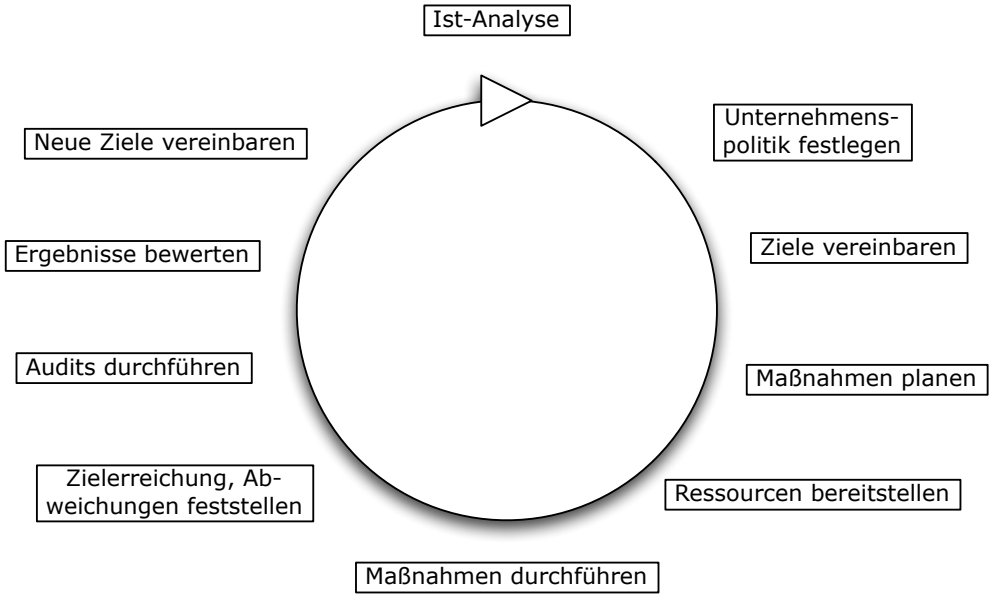

Abbildung 3.1: Managementsystem Regelkreis (vgl. [NACH-MS])

Ein ISMS ist ein spezielles Managementsystem und umfasst Regeln für die Steuerung, Lenkung und Kontrolle von IT-Sicherheitsprozessen. Das ISMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert)[3]". Zu den grundlegenden Komponenten zählen hierbei (siehe auch Abbildung 3.2):

[3] vgl. [BSI-100-1]

- **die Managementprinzipien**, welche die Steuerung, Lenkung und Kontrolle der Sicherheitsprozesse behandeln.
- **die Ressourcen**, welche finanzielle, personelle und zeitliche Ressourcen beinhalten.
- **die Mitarbeiter**, welche alle Mitarbeiter des Unternehmens umfassen.
- **der IT-Sicherheitsstrategie**, der im folgenden genauer beschrieben wird.

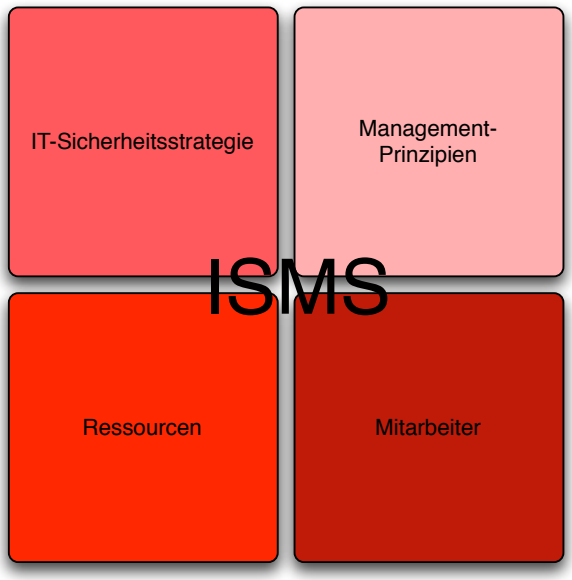

Abbildung 3.2: Bestandteile eines ISMS (vgl. [BSI-100-1])

Die zuvor genannte IT-Sicherheitsstrategie läßt sich wiederum in drei Unterpunkte gliedern:

- **IT-Sicherheitsleitlinie**

  In der Sicherheitsleitlinie werden Sicherheitsziele und Strategien zum Umsetzung von IT-Sicherheit definiert.

- **IT-Sicherheitskonzept**

  Das Sicherheitskonzept ist ein Hilfsmittel zur Umsetzung der Sicherheitsstrategie. Im Sicherheitskonzept werden zum Beispiel Maßnahmen, IT-Strukturen und Risiken beschrieben.

- **IT-Sicherheitsorganisation**

  Wie auch das Sicherheitskonzept ist auch die Sicherheitsorganisation ein Hilfsmittel zur Umsetzung der Sicherheitsstrategie. Jedoch werden in der Sicherheitsorganisation beispielsweise Prozesse, Strukturen, Abläufe und Regeln beschrieben.

Im Jahre 1995 wurde die erste Version des damals noch IT-Grundschutzhandbuch genannten ISMS im Bundesanzeiger[4] veröffentlicht. Zeitgleich wurde auch die erste Version von COBIT[5] herausgebracht. Im Laufe der Zeit entwickelten sich dann weitere ISMS, welche oft ähnliche Ansätze und gemeinsame Vorgehensweisen hatten. Bei näherer Betrachtung muss man jedoch feststellen, daß sich die verschiedenen Systeme nicht direkt kombinieren lassen. Es gibt Unterschiede im Umfang der Abdeckung, sowie in der Zielgruppe der Systeme. Einen Überblick über die verschiedenen ISMS findet sich in Kapitel 4.

Wie das oben genannte allgemeine Managementsystem, ist auch das ISMS ein fortlaufender Prozess. Dieses wird jedoch bei ISMS vielfach vereinfacht und folgt in vielen Fällen dem PDCA Modell nach Deming[6]. PDCA steht für "Plan, Do, Check and Act" und wird beispielsweise von ISO 27001 verwendet. Ziel von PDCA ist die Etablierung eines ständigen, das System verbessernden Prozesses. Das PDCA Modell lässt sich wie folgt beschreiben (siehe auch Abbildung 3.3):

Plan: Planung eines Vorhabens

Do: Umsetzung des geplanten Vorhabens

Check: Kontrolle der Umsetzung

Act: Optimierung und Verbesserung der erkannten Mängel

[4] http://http://www.bundesanzeiger.de
[5] vgl. [COBIT]
[6] vgl. [DEMING] und [BSI-100-1]

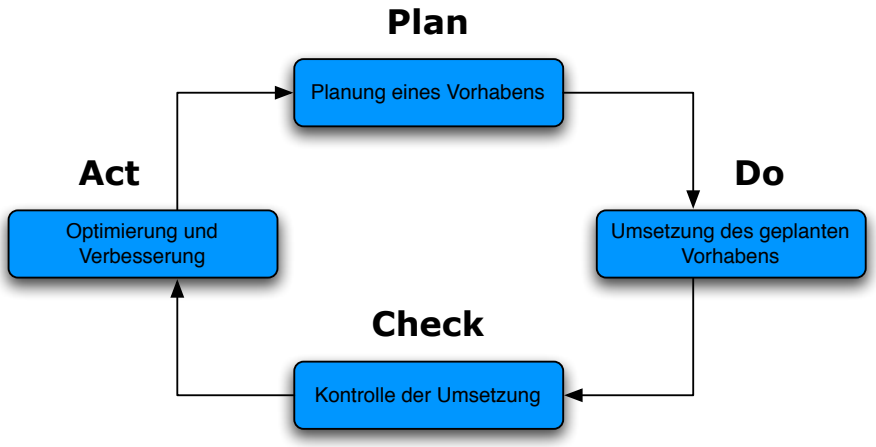

Abbildung 3.3: PDCA Model nach Deming [DEMING]

3.2 Beschreibung existierender ISMS

3.2.1 IT-Grundschutz

3.2.1.1 Einführung

Der IT-Grundschutz des BSI ist das in Deutschland bekannteste ISMS. Es ist als Leitfaden zu verstehen und gibt dem Anwender eine Schritt-für-Schritt-Vorgehensweise an die Hand. IT-Grundschutz hat gerade für kleinere und mittlere Unternehmen den Vorteil, daß nicht für alle Systeme eine Risikoanalyse durchgeführt werden muss, da schon sehr viele Gefährdungen und entsprechende Maßnahmen vorgegeben sind. Bei einem höheren Schutzbedarf, oder bei nicht abgedeckten Systemen, wie einem Windows 2003 Server muss jedoch eine Risikoanalyse durchgeführt werden. Eine anerkannte Methode ist unter [BSI-100-3] genauer beschrieben. Prinzipiell kann jedoch jede Risikoanalyse angewandt werden.

Der Leitfaden dient dazu, durch die Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau zu schaffen, welches für den normalen Schutzbedarf der IT-Systeme angemessen und ausreichend ist und als Basis für IT-Systeme mit höherem Schutzbedarf dient. Durch die

Anwendung des IT-Grundschutz lassen sich IT-Sicherheitskonzepte einfach und mit geringem Arbeitsaufwand erstellen. Es kann jedoch schon bei kleineren Unternehmen sechs Monate dauern, bis erste Ergebnisse sichtbar werden.

3.2.1.2 Entstehung

Der IT-Grundschutz wurde bis zum Jahr 2005 IT-Grundschutzhandbuch genannt. Die erste Version des IT-Grundschutzhandbuches wurde 1995 in Bundesanzeiger veröffentlicht und bestand damals aus 18 Bausteinen, 200 Maßnahmen und war 150 Seiten lang.

Der Umfang wuchs von Jahr zu Jahr, so daß allein die heutigen IT-Grundschutz-Kataloge über 3000 Seiten aufweisen. Der Aufbau von IT-Grundschutz hat sich im Laufe des letzen Jahres grundlegend verändert und wird im nächsten Kapitel genauer beschrieben.

3.2.1.3 Aufbau

IT-Grundschutz teilt sich in drei Standards zum Thema IT-Sicherheit sowie den IT-Grundschutz-Katalogen. Die drei Standards sind wie folgt gegliedert:

BSI-Standard 100-1: Managementsysteme für Informationssicherheit[BSI-100-1]
Dieser Standard befasst sich mit dem Aufbau von ISMS und gibt eine Übersicht über die Prozesse zur Umsetzung von IT-Sicherheit

BSI-Standard 100-2: Vorgehensweise nach IT-Grundschutz[BSI-100-2]
Der Standard beschreibt das Vorgehen nach IT-Grundschutz und bezieht sich dabei auf die Initiierung des IT-Sicherheitsprozesses, die Erstellung einer IT-Sicherheitskonzeption sowie die Aufrechterhaltung der IT-Sicherheit

BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz[BSI-100-3]
Dieser Standard beschreibt die Vorgehensweise für eine Risikoanalyse auf der Basis von IT-Grundschutz. Durch die starke Anlehnung an IT-Grundschutz eignet er sich beson-

ders gut für die Umsetzung einer Risikoanalyse im Rahmen von IT-Grundschutz.

Die IT-Grundschutz-Kataloge beginnen mit einer kurzen Einführung zum Thema IT-Grundschutz und fahren mit einer genaueren Beschreibung der Bausteine fort. "Die einzelnen Bausteine spiegeln typische Bereiche des IT-Einsatzes wieder, wie beispielsweise Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten"[7]. Jeder Baustein wird in den IT-Grundschutz-Katalogen kurz erläutert und gibt daraufhin Verweise auf die Gefährdungen und Maßnahmen welche im Rahmen des Bausteins betrachtet werden. Die Bausteine sind in fünf Abschnitte eingeteilt:

B 1: Übergeordnete Aspekte der IT-Sicherheit
In diesem Kapitel wird auf übergreifende Bausteine wie Personal, IT-Sicherheitsmanagement oder ein Datensicherheitskonzept eingegangen.

B 2: Sicherheit der Infrastruktur
Dieser Abschnitt befasst sich unter anderen mit den Bausteinen Gebäude, Serverraum und häuslicher Arbeitsplatz.

B 3: Sicherheit der IT-Systeme
Für weit verbreitete IT-Systeme wie Unix-Systeme, tragbare PCs und TK-Anlagen gibt es in diesem Abschnitt Bausteine.

B 4: Sicherheit im Netz
Dieser Abschnitt befasst sich mit der Vernetzung von IT-Systemen sowie deren Sicherheitsmanagement.

B 5: Sicherheit in Anwendungen
Größere IT-Anwendungen wie E-Mail, WWW-Server und Datenbanken werden in diesem

[7] vgl. [GSHB]

Abschnitt beschrieben.

3.2.1.4 Zielgruppe

Durch sein breites Spektrum richtet sich IT-Grundschutz an alle Unternehmen und hat für viele Gefährdungen passende Maßnahmen parat. Gerade bei kleinen und mittleren Unternehmen (KMU) empfiehlt sich aufgrund der Leitfäden und des klaren Vorgehens eine Umsetzung nach IT-Grundschutz.

3.2.1.5 Umsetzung und Zertifizierung

Im Gegensatz zu einer traditionellen Risikoanalyse[8], welche teuer und aufwendig sein kann, wird beim IT-Grundschutz zuerst nur ein Basis-Sicherheitscheck zwischen den empfohlenen und den bereits realisierten Maßnahmen durchgeführt. Fehlende oder nicht vollständig umgesetzte Maßnahmen zeigen Sicherheitsdefizite auf, welche durch die empfohlenen Maßnahmen zu beheben sind. Die Vorgehensweise beim IT-Grundschutz lässt sich in vier Bereiche einteilen.

1. IT-Strukturanalyse: Durch die IT-Strukturanalyse werden Informationen über den betrachteten Bereich gewonnen. Dieser Bereich wird auch "IT-Verbund" genannt. In diesem Schritt werden Anwendungen, IT-Systeme oder IT-Räume zu einem Verbund zusammengefasst und deren Abhängigkeit zueinander dargestellt. Wichtig dabei ist, daß alle verbundenen Zielobjekte erfasst werden, was diesen Prozess zu einem der Schwierigsten im Rahmen von IT-Grundschutz macht. Eine genaue und vollständige Abgrenzung des IT-Verbundes ist der zentrale Schritt für die weitere Vorgehensweise.

2. Schutzbedarfsfeststellung: Die darauf folgende Schutzbedarfsfeststellung betrachtet die Gefährdungen, welche zu Beeinträchtigungen der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit[9] innerhalb von IT-Anwendungen, IT-Systemen, Kom-

[8] vgl. [RISK-MITTEL]

[9] siehe auch Wahlpflichtfach IT-Sicherheit, Dozent: Prof. Dr. Karsch, FH Köln

munikationssystemen und Räumen führen könnten. Durch diesen Schritt lässt sich ein ausreichendes Schutzniveau mit möglichst geringen Kosten erreichen.

3. Modellierung: Einer der zentralen Schritte bei der Anwendung von IT-Grundschutz ist die Modellierung. Bei der Modellierung werden den existierenden Prozessen und Komponenten (Ziel-Objekte), welche im vorangegangenen Schritt definiert worden sind, Bausteine zugeordnet. Hierzu bietet IT-Grundschutz eine detaillierte Anleitung, wie mit Hilfe der vorhandenen Bausteine der IT-Verbund möglichst realistisch nachgebildet werden kann.

   Jeder Baustein beschreibt die relevanten Gefährdungen des konkreten Zielobjektes und bietet entsprechende Maßnahmen an. Durch die Modellierung entsteht daraus eine umfangreiche Liste mit allen umzusetzenden Maßnahmen.

4. Basis-Sicherheitscheck: Der letzte Schritt bezieht sich auf den ermittelten IT-Verbund. In diesem Schritt werden die Maßnahmen, welche in der Modellierung als erforderlich identifiziert worden sind, überprüft. Dabei sollen, zum Beispiel durch Interviews und stichprobenartige Kontrollen, Defizite herauskristalisiert werden. Der Basis-Sicherheitscheck ist ein Soll-Ist Vergleich, welcher den derzeitigen Stand mit dem geforderten Stand laut Modellierung vergleicht.

Das BSI stellt unter [BSI-100-2] ein umfassendes Dokument zur Verfügung, indem die Vorgehensweise nach IT-Grundschutz beschrieben wird. Je nach Wunsch des Anwenders kann man einen IT-Verbund zertifizieren lassen. Dies muss beispielsweise geschehen, um an manchen Ausschreibungen öffentlicher Stellen teilnehmen zu können. Ein Schema zur Zertifizierung ist unter [27001-GS] beschrieben

3.2.1.6 Besonderheiten

Um eine praxisnahe Hilfestellung bei der Umsetzung nach IT-Grundschutz zu geben, hat das BSI drei exemplarische Umsetzungen ("Ein IT-Grundschutzprofil für eine kleine Insti-

tution[10]", "Ein IT-Grundschutzprofil für den Mittelstand[11]", "Ein IT-Grundschutzprofil für eine große Institution[12]") erstellt, welche den Anwendern Einblicke in die Umsetzung in fiktiven Unternehmen oder Institutionen gewähren. Hierdurch erhält der Anwender einen Überblick über ein gradliniges Vorgehen beim IT-Grundschutz. Das BSI hat zu diesem Zweck eine Umsetzung in einem kleinen Unternehmen simuliert, in dem IT-Grundschutz noch nicht betrachtet wurde. Dies soll zur Sensibilisierung für IT-Sicherheitsfragen beitragen. Des weiteren gibt es eine Umsetzung in einem mittelgroßen Unternehmen, dessen Mitarbeiter bereits mit dem Thema IT-Sicherheit vertraut sind. Das dritte und letze Profil zeigt eine Umsetzung in einem großen Unternehmen. Hier steht nicht die Umsetzung von IT-Grundschutz im Vordergrund. Vielmehr sollen potentielle Probleme bei großen Unternehmen besprochen werden.

Ein IT-Grundschutzprofil für eine kleine Institution

Das kleine Profil soll kleineren Firmen helfen, IT-Grundschutz erstmalig aufzubauen. Gerade kleine Unternehmen haben oftmals nicht genug Geld, um sich einen Sicherheitsbeauftragten leisten zu können. Demnach richtet sich das Dokument primär an Geschäftsführer, da diese in kleinen Betrieben nur selten die Verantwortlichkeiten weiter delegieren können. Dies trifft zum Beispiel bei Arztpraxen, Rechtsanwaltskanzleien, Steuerberatern, kleineren Handwerksbetrieben, kleineren Behörden, Ämtern, Reisebüros oder Hotels zu. Oft schreibt der Gesetzgeber die Benutzung von Informationstechnologie vor, sei es für die Steuerabwicklung (Elster[13]) oder bei Arztpraxen durch die kommende elektronische Gesundheitskarte. Viele Unternehmen haben nicht genügend Ressourcen oder technisches Verständnis, sich mit den daraus resultierenden Sicherheitsproblemen ausreichend auseinanderzusetzen. Das kleine Profil zeigt Ansätze für einen IT-Grundschutz, welcher ein klares Vorgehen ausweist und den Anwender für das Thema IT-Sicherheit sensibilisiert. Eine grafische Übersicht über den Musterbetrieb im kleinen Profil sehen

[10] siehe [KLEINES]
[11] siehe [MITTLERES]
[12] siehe [GROSSES]
[13] https://www.elster.de

Sie in Abbildung 3.4.

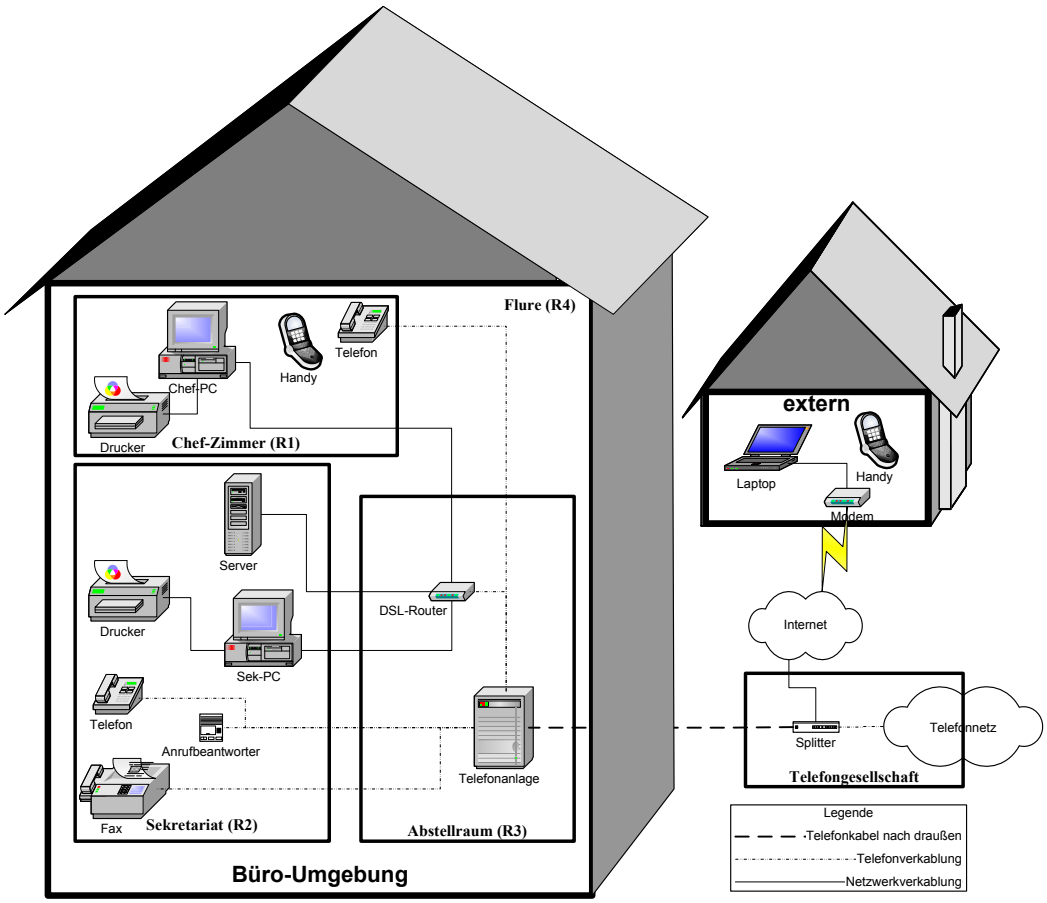

Abbildung 3.4: Kleines Profil - Quelle: BSI[KLEINES]

Ein IT-Grundschutzprofil für den Mittelstand

Beim mittleren Profil liegt der Fokus auf einem mittelgroßen Unternehmen. Es verfügt meist über eine IT-Abteilung und hat schon Erfahrung mit der Sicherheit der eingesetzten IT Systeme. Das mittlere Profil zeigt einen systematischen Ansatz zur Einführung von IT-Grundschutz und nutzt dabei das Werkzeug "GSTOOL" vom BSI.

Im Fokus der Untersuchung der Kompatibilität eignet sich das mittlere Profil sehr gut

für eine spätere Untersuchung, da es ein authentisches Unternehmen darstellt und einen starken Praxisbezug hat. In Kapitel 6 wird mit Hilfe der später gewonnen Erkenntnisse Teile des PCI DSS in das mittlere Profil integriert.

Eine grafische Übersicht über das Musterunternehmen im mittleren Profil sehen Sie in Abbildung 3.5.

Ein IT-Grundschutzprofil für eine große Institution
Bei großen Unternehmen muss meist eine große Anzahl von IT-Systemen betrachtet werden. Dies ist meist mit einem großen personellen und finanziellen Aufwand verbunden und erfordert ein striktes Projektmanagement, um die Wirtschaftlichkeit zu wahren. Das große Profil befasst sich mit den Problemen, die speziell bei der Umsetzung in einem Rechenzentrum auftreten und gibt Hinweise zur korrekten Vorgehensweise.

Dieses Profil eignet sich jedoch nicht für eine weitere Betrachtung im Rahmen der Kombination von ISMS, da in diesem Profil primär Probleme behandelt werden.

Eine grafische Übersicht über das Musterunternehmen im großen Profil sehen Sie in Abbildung 3.6.

3.2.2 Payment Card Industry - Data Security Standard (PCI DSS)

3.2.2.1 Einführung

Die Unternehmen MasterCard Worldwide[14] und Visa[15] reagieren mit den PCI DSS auf den zunehmenden Diebstahl von Kreditkartendaten. Der PCI DSS ist aus zwei einzelnen Vorgehensweisen der beiden Kreditkartenanbieter hervorgegangen (das "Site Data Protection" [SDP] Programm von MasterCard Worldwide und das "Account Information

[14] http://www.mastercard.com
[15] http://www.visa.com

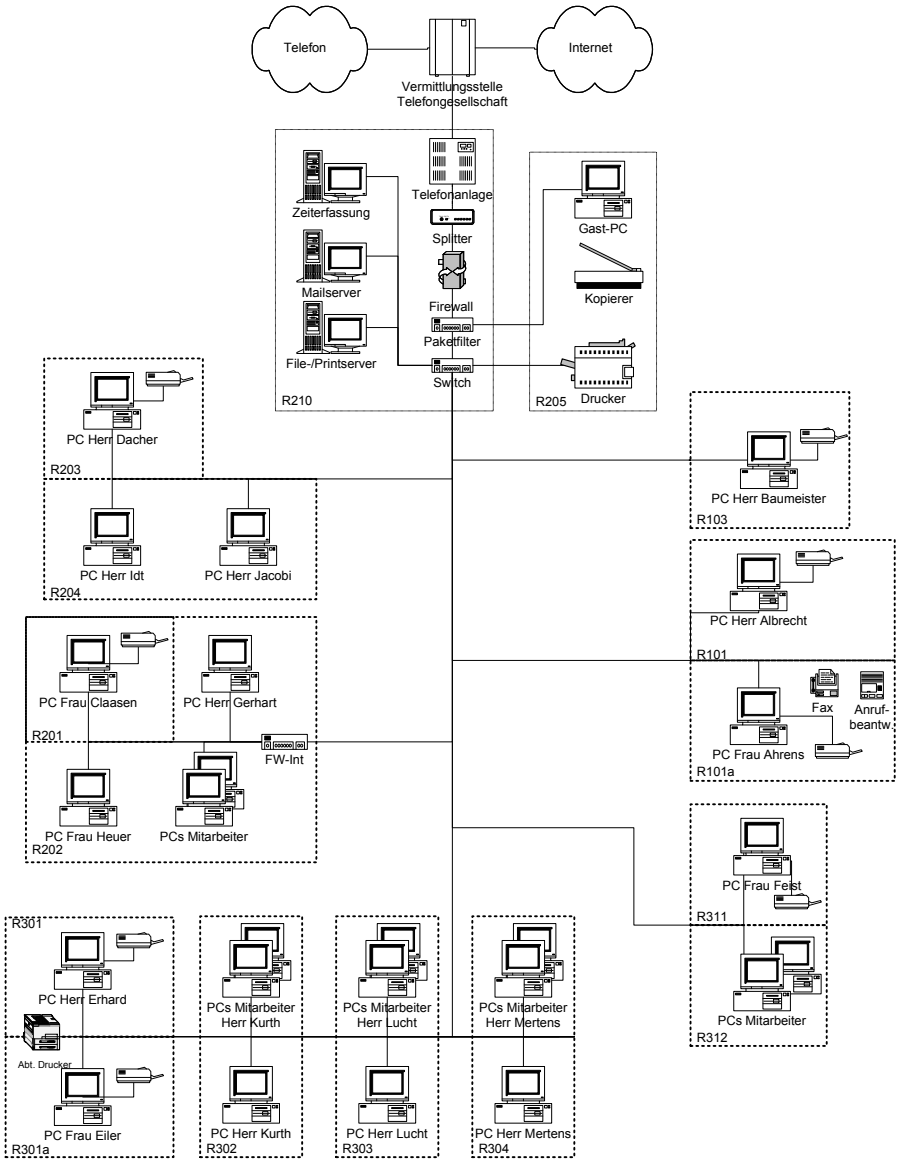

Abbildung 3.5: Mittleres Profil - Quelle: BSI[MITTLERES]

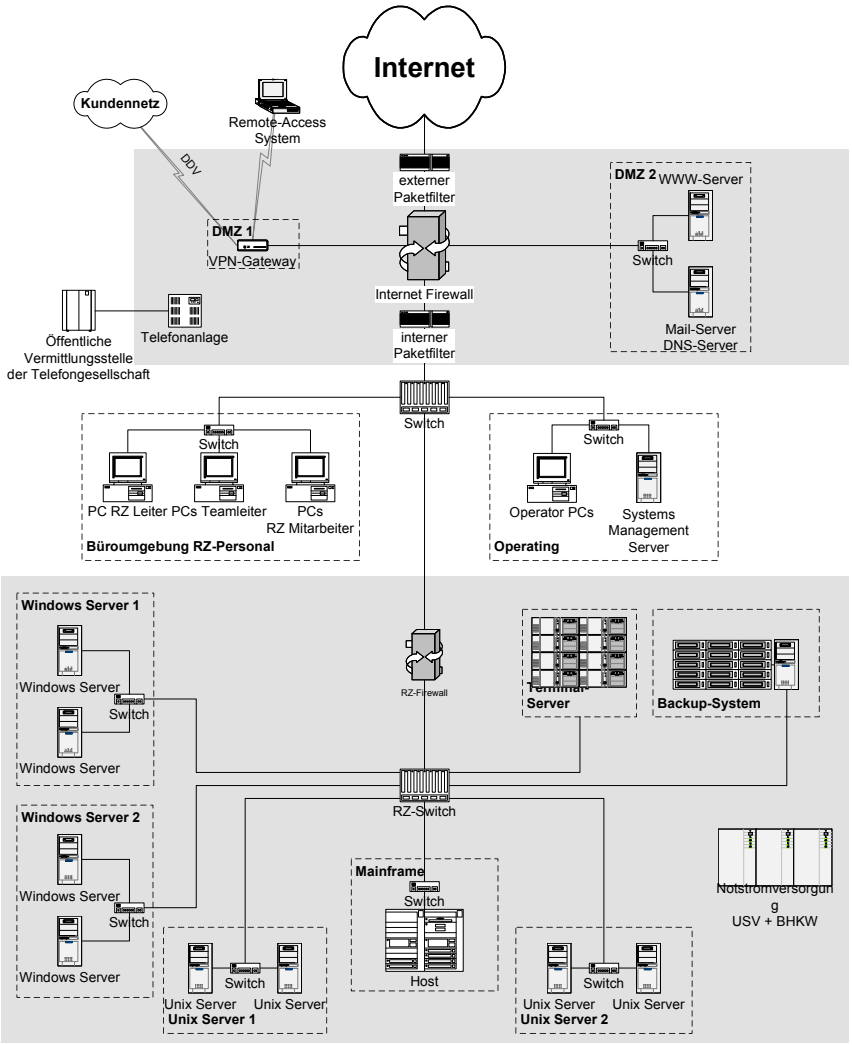

Abbildung 3.6: Grosses Profil - Quelle: BSI[GROSSES]

Sercurity" [AIS] Programm von Visa). Beide Vorgehensweisen verfolgen das selbe Ziel, die Sicherheit von Kreditkartenzahlungen über das Internet sicher zu machen, und so entstand der gemeinsame Standard PCI DSS.

3.2.2.2 Entstehung

Die ersten Ansätze zur Verbesserung der Sicherheit bei Kreditkartentransaktionen über das Internet, das SDP und AIS Programm, entstanden in den Jahren 2000 und 2001. Die Umsetzung auf Seiten der Unternehmen, welche Kreditkarten verarbeiten, wurde jedoch erst Ende 2003 forciert. Durch die gemeinsamen Anstrengungen von MasterCard Wordwide und Visa enstand Ende 2004 der PCI DSS. Dieser bot nun eine gemeinsame Zertifizierungsbasis an.

3.2.2.3 Aufbau

Der PCI DSS beschränkt sich größtenteils auf konkrete Verfahrensanweisungen, welche zwingend umzusetzen sind. Eine Risikoanalyse entfällt bei diesem ISMS, da das Risiko, der Diebstahl von Kreditkartendaten, fest vorgegeben ist. Diese Vorgaben haben den Nachteil, daß alle Maßnahmen umgesetzt werden müssen und nicht zwingend in Abhängigkeit zum tatsächlichem Risiko stehen.

Die Verfahrensanweisungen sind in 12 Gruppen unterteilt, welche sich wiederum in 6 Methodengruppen einteilen lassen. Diese Einteilung trägt zum einen der eingesetzten Hardware, der Software, der Sicherheit der Kreditkartendaten, sowie einigen Managementansätzen Rechnung. Die Methodengruppen[16] lauten wie folgt:

- build and maintain a secure network

  Aufbau und Sicherung des Netzwerkes

[16] vgl. [PCIDSS]

- protect cardholder data
  Schutz der Kartendaten
- maintain a vulnerability management program
  Aufbau eines Managementsystems zur Beseitigung von Schwachstellen
- implement strong access control measures
  Einbai von starken Zugriffkontrollmethoden
- regularly monitor and test networks
  Regelmäßige Überwachung und Tests des Netzwerkes
- maintain an information security policy
  Verwalten einer Sicherheitsrichtlinie

3.2.2.4 Zielgruppe

Zielgruppe dieses ISMS sind Händler und Dienstleister, welche Kreditkartendaten verarbeiten, speichern oder weiterleiten. Je nach Anzahl der Kreditkarten-Transaktionen werden Händler und Dienstleister in verschiedene Stufen eingeteilt. Zum besseren Verständnis wird im folgenden die Einteilung bei Händlern gezeigt.

- Level 1:
  - alle Händler, unabhängig vom Vertriebsweg, die mehr als 6 Millionen Transaktionen mit MasterCard oder Visa pro Jahr abwickeln;
  - alle Händler, die Opfer eines Angriffs und einer Kompromittierung geworden sind;
  - alle Händler, die mit einer anderen Kreditkartenmarke in die Kategorie Level 1 fallen;
  - alle Händler, die nach dem Ermessen von MasterCard oder Visa zur Minderung des Risikos für die Zahlungssysteme in diese Kategorie eingestuft werden.

- Level 2:
  - alle Händler, die zwischen 150.000 und 6 Millionen E-Commerce Transaktionen mit MasterCard- oder Visa-Karten pro Jahr abwickeln;
  - alle Händler, die mit einer anderen Kreditkartenmarke in die Kategorie Level 2 fallen.
- Level 3:
  - alle Händler, die zwischen 20.000 und 150.000 E-Commerce Transaktionen mit MasterCard- oder Visa-Karten pro Jahr abwickeln;
  - alle Händler, die mit einer anderen Kreditkartenmarke in die Kategorie Level 3 fallen.
- Level 4:
  - alle Händler, die nicht in eine der Kategorien Level 1, 2 oder 3 eingestuft sind.

Weitere Informationen, wie auch die Einteilung der Dienstleister, findet sich unter [AIS] und [SDP].

3.2.2.5 Umsetzung und Zertifizierung

Die Umsetzung des PCI DSS beginnt mit der Eingrenzung der IT-Systeme auf jene, die Kreditkartendaten verarbeiten, speichern oder weiterleiten.

Die Maßnahmen des PCI DSS richten sich primär auf die Sicherung von Kreditkartendaten. Dabei werden unter anderem IT-Systeme gehärtet, Verfahrensanweisungen erstellt und organisatorische Vorgaben spezifiziert.

Die Umsetzung der Maßnahmen im PCI DSS wird sich mittels eines umfassenden Fragebogens [PCIQUEST], ein bis vier Security Scans pro Jahr[PCISCAN], sowie eines jährlichen Audits [PCIAUDIT] für große Händler und Dienstleistern überprüfen und

schließt mit einer Zertifizierung ab. Abbildung 3.7 verdeutlicht das Prüfverfahren des Standards.

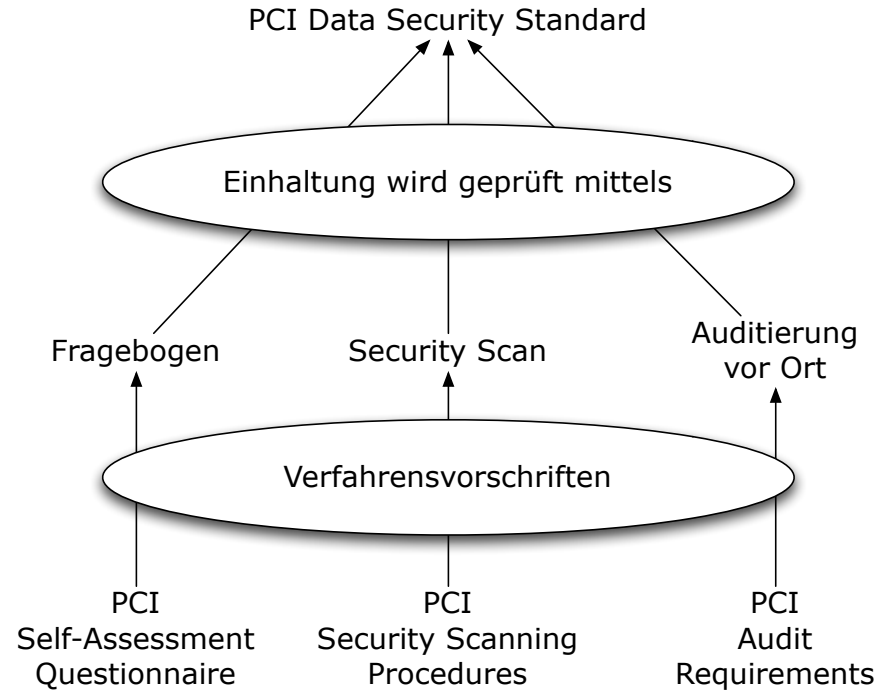

Abbildung 3.7: Prüfschema PCI DSS

Die erste Prüfung ist ein Fragebogen, welcher vom Händler oder Dienstleistern selbst auszufüllen ist. Dieser fragt anhand einer Ja/Nein Liste den jeweiligen Umsetzungsgrad der verschiedenen Maßnahmen ab. Hierdurch erhält das Unternehmen einen ersten Überblick über den Umsetzungsgrad von PCI DSS. Ohne eine positive Überprüfung des Fragebogens, bei dem alle mit "Nein" angekreuzten Fragen Sicherheitsdefizite darstellen, kann keine Zertifizierung gegeben werden.

Die zweite Prüfung ist ein sog. Security Scan der "Internet facing IP-Adresses"[17], also den aus dem Internet erreichbaren IP-Adressen. Bei einem Security Scan werden mit Hilfe von automatisierten Schwachstellen-Scannern potenzielle Probleme auf den zu überprüfenden

[17] vgl. [PCISCAN]

Systemen gesucht und dann mittels einer manuellen Überprüfung von einem Spezialisten bewertet. Der Security Scan darf keine kritischen Schwachstellen aufweisen. Je nach Anzahl der verarbeiteten Kreditkartendaten sind pro Jahr ein bis vier Scans notwendig. Die Scans müssen von zertifizierten Auditoren durchgeführt werden.

Der letzte Schritt ist ein sog. Onsite-Audit. Dieser ist nur für Dienstleister und sehr große Händler notwendig. Händler können diesen Audit selber durchführen, Dienstleister müssen den Audit von einem zertifizierten Auditor durchführen lassen. Der Auditor prüft anhand einer Checkliste die Umsetzung der verschiedenen Maßnahmen vor Ort. Hierzu werden Befragungen durchgeführt, Logeinträge überprüft, verschiedene Policies angesehen, sowie die physikalische Sicherheit der Systeme überprüft. Der Auditor erstellt anschließend einen Bericht, welcher von Visa geprüft wird. Fällt die Entscheidung von Visa positiv aus, ist das Unternehmen nach PCI DSS zertifiziert.

Zur Vervollständigung sei die Vorgehensmatrix zur Erlangung einer Zertifizierung gegeben.

Kategorie Händler	**Self Assessment**	**Security Scan**	**Security Audit**
Stufe 1	-	4 x pro Jahr	
Stufe 2	1 x pro Jahr	4 x pro Jahr	-
Stufe 3	1 x pro Jahr	4 x pro Jahr	-
Stufe 4	1 x pro Jahr	1 x pro Jahr	-

Tabelle 3.1: Einstufung Händler

3.2.3 ISO 27001 / ISO 17799

3.2.3.1 Einführung

ISO 27001 [27001] und ISO 17799 [17799] sind zwei international anerkannte Standards und beschreiben die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines ISMS. Hierbei werden auch speziell die Risiken der Gesamtorganisation betrachtet. Im Gegensatz zum IT-Grundschutz muss beim ISO 27001 immer eine Risikoanalyse durchgeführt werden.

3.2.3.2 Entstehung

Der ISO 27001 Standart ist aus dem britischen Standard BS7799-2 entstanden. Das britische Department of Trade and Industry (DTI) hat im Jahr 1992 eine Kommission gebildet, welche die damaligen "Best Practices" im Bereich Informationssicherheit niederschrieb. Sie wurden 1993 veröffentlicht und 1995 vom British Standard Institute adaptiert als BS 7799:1995. Der Standard wurde aber aufgrund seiner mangelnde Flexibilität von der Industrie abgelehnt.

Er wurde daher 1998 grundlegend überarbeitet und in zwei verschiedene Teile aufgeteilt. Ein Jahr später übernahm die ISO den ersten Teil als ISO 17799:2000. Der zweite Teil erfuhr in Jahr 2002 eine grundlegende Überarbeitung, welche im Standard BS 7799-2:2002 resultiert. Aus diesem entstand der heutige ISO 27001 Standard ("Information technology - Security techniques - Information security management systems - Requierements").

ISO 17799 ist im Jahr 2000 durch die Übernahme von BS 7799-1 in den ISO-Normenkatalog entstanden. Im Jahre 2005 wurde der Standard überarbeitet und unter der Bezeichnung ISO 17799:2005 veröffentlicht.

3.2.3.3 Aufbau

Der Standard besteht aus 2 Teilen, welche sich auf der einen Seite durch den ISO 27001 und seiner allgemeinen Vorgehensweise für ein ISMS definiert und auf der anderen Seite durch den ISO 17799 Standard. Letztgenannter gibt dem Benutzer Maßnahmen zur Hand, um die in ISO 27001 erstellten Anforderungen umzusetzen. Die einzelnen Maßnahmen sind nicht so detailliert wie im IT-Grundschutz, sondern eher allgemein gehalten. Dies erfordert mehr Aufwand bei der Umsetzung, kann jedoch auch vorteilhaft sein, da die Maßnahmen selber konkretisiert und besser an die eigene Unternehmung angepasst werden können.

Der Standard findet in vielen Bereichen Anwendung, beispielsweise

- zur Definition von neuen ISMS Prozessen,
- zur Definition von Forderungen und Zielen zur IT-Sicherheit,
- zur Gewährleistung der Einhaltung von Gesetzen,
- zur Identifikation und Definition von bestehenden Informationssicherheits Managementprozessen,
- zur Definition von Informationssicherheits-Managementtätigkeiten,
- zum wirtschaftlichen Management von Sicherheitsrisiken und
- zum Gebrauch durch interne und externen Auditoren zur Feststellung des Umsetzungsgrades von Richtlinien und Standards.

3.2.3.4 Zielgruppe

Der Standard richtet sich aufgrund seiner internationalen Anerkennung primär an. Sein erheblicher Umfang und der Bedarf einer Risikoanalyse eignen ihn besonders für mittlere bis große Unternehmen, da diese häufig im Rahmen anderes Managementsysteme bereits Risikoanalysen durchführen. ISO 27001 erlangt zunehmend Bedeutung, da nun auch das BSI eine Zertifizierung nach diesem Standard auf Basis von IT-Grundschutz vorsieht.

3.2.3.5 Umsetzung und Zertifizierung

Eine Zertifizierung ist grundsätzlich nur nach ISO 27001 und nicht nach ISO 17799 möglich. Hierzu wird ein externer Auditor beauftragt, eine Prüfung der umgesetzten Maßnahmen durchzuführen. Nach einem positiven Audit, welcher sich mit den verschiedenen Anforderungen befasst, erhält das Unternehmen das ISO 27001 Zertifikat. ISO 27001 und ISO 17799 zusammen ergeben ein abgerundetes ISMS.

3.3 Kleinere ISMS

3.3.1 ISO 13335

ISO 13335 "Guidelines for the management of It security" [13335] "gibt Handreichungen für das IT-Sicherheitsmanagement, ohne bestimmte Lösungen zu erzwingen. Der Standard stellt ein Basiswerk dar und ist Ausgang- oder Referenzpunkt für eine Reihe von Dokumenten zum IT-Sicherheitsmanagement."[18]

3.3.2 IT Infrastructure Library

Im Rahmen der IT Infrastructure Library (ITIL) [ITIL-SF], welche einen Rahmen für ein Service Management bildet, welches sich mit dem Thema "Security Management" befasst. Das Modul ist sehr allgemein gehalten und für meine Untersuchung nicht geeignet, da es keine Maßnahmen definiert. Weitere Informationen zu ITIL finden Sie auf der Homepage[19] des Office of Government Commerce (OGC) sowie in einer Studie des BSI [ITIL].

3.3.3 Cobit

Die Control Objectives for Information and Related Technology (CobiT) [COBIT] wurden ursprünglich im Jahre 1993 von der Information Systems Audit and Control As-

[18] vgl. [13335-TR]
[19] http://www.itil.org/

sociation (ISACA)[20] entwickelt. Der Standart wurde im Jahr 2000 vom IT Governance Institute übernommen und wird seitdem von diesem gepflegt. CobiT definiert keine konkreten Maßnahmen, sondern gibt nur eine Grobe Richtung vor.

3.4 Eingrenzung der ISMS für diese Arbeit

Aufgrund der Bekanntheit von IT-Grundschutz und des PCI DSS sowie ISO 27001/17799 werden im Rahmen dieser Arbeit nur diese ISMS im folgenden näher beschrieben, um einen Überblick und ein Verständnis für die Systeme zu erhalten. Weiterführende Informationen zur Definition und Prozessbeschreibung eines ISMS finden Sie unter [BSI-100-1]

[20] http://www.isaca.org/

Kapitel 4

Analyse verschiedener ISMS

In diesem Kapitel: Analyse der verschiedenen ISMS, sowie erste Ansätze zur Kombination.

Nach der Einführung in die Grundlagen der unterschiedlichen ISMS (siehe Kapitel 3) wird klar, daß die unterschiedlichen ISMS in der Regel auf verschiedenen Abstraktionsstufen arbeiten. Diese gilt es nun zu analysieren und zu beschreiben, um Gemeinsamkeiten der Systeme zu finden.

Die verschiedenen Herangehensweisen der ISMS lassen sich in Abstraktionsebenen einordnen. Die Einteilung geschieht hier anhand des Grades der Tiefe, der in den jeweiligen Systemen angesprochen wird. Die Ebenen lassen sich wie folgt definieren:

Policies

Policies sind allgemein gehaltene Vorgaben. Sie lassen viel Spielraum bei der Umsetzung, da in der Regel keine technischen Vorgaben getroffen werden. Als Beispiel sei hier die Policy "User-Management" erwähnt, welche auch den Passwortschutz beinhaltet.

Konzepte

Konzepte sind genauer als Policies. Um das Beispiel aus dem Punkt "Policies" zu über-

nehmen, wäre ein Konzept eine Passwortrichtlinie.

Verfahrensanweisungen / Maßnahmen / technische Dokumente
Dies ist die unterste Schicht. Die Angaben sind hier sehr konkret und lassen kaum Spielraum bei der Umsetzung. Bezogen auf die beiden vorangegangenen Beispiele sei hier die Maßnahme "Passwörter müssen nach 90 Tagen geändert werden" genannt. Unter anderen werden konkrete technische Maßnahmen genannt.

Wie man am Beispiel des Passwortgebrauches sehen kann, steigt der Grad der Genauigkeit von Stufe zu Stufe. Am oberen Ende werden nur grobe Richtungen und Ziele vorgegeben, während am unteren Ende konkret umzusetzende Maßnahmen genannt werden.

Da nicht alle ISMS das gesamte Spektrum abdecken, sollte man zuerst versuchen, die einzelnen ISMS von einander abzugrenzen.

Hierbei wird klar, daß sich nicht jedes ISMS bezüglich der Maßnahmen auf alle drei Ebenen bezieht. Um Gemeinsamkeiten der Systeme herauszufinden gilt es, die Systeme zuerst einmal einzuordnen. Wie bereits in den Grundlagen erwähnt, ist ISO 27001 sehr abstrakt gehalten und ignoriert Maßnahmen. Es behandelt die grundlegenden Aufgaben zur Erstellung eines ISMS und wird deshalb auf in das Ebene "Policies" eingeordnet.

ISO 17799 beinhaltet viele Maßnahmen und Konzepte. Als Erweiterung von ISO 27001 geht es nicht auf das Thema "Policy" ein. Es ist daher zwischen den Ebene "Konzepte" und "Maßnahmen, etc" eingeordnet.

IT-Grundschutz hingegen bietet von Policies bis hinunter zu den Maßnahmen ein durchgängiges Vorgehen an. Durch die Einteilung in "Bausteinen", "Gefährdungen" und "Maßnahmen" wird eine gute Trennung der Abstraktionsebenen erreicht.

PCI DSS hingegen bezieht sich fast nur auf konkrete Maßnahmen. Es verfolgt zwar auch Policies und abstraktere Gedanken, jedoch läßt der Standard hier viel Luft zur Umsetzung. Lediglich einige konkrete Anforderungen an die Umsetzung sind genannt.

Abbildung 4.1 stellt den Zusammenhang noch einmal grafisch dar.

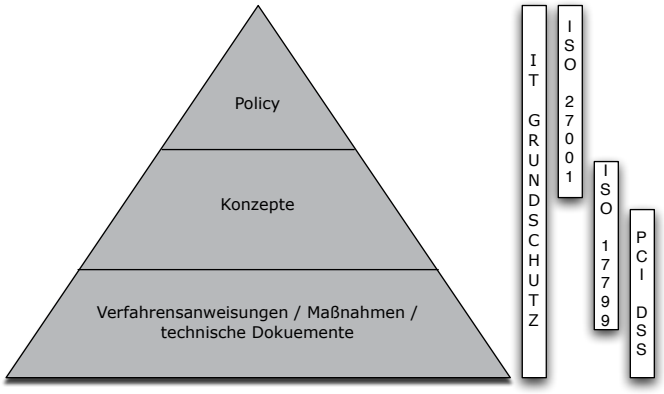

Abbildung 4.1: Einordnung verschiedener ISMS

4.1 Gemeinsamkeiten der verschiedenen Systeme

Um Gemeinsamkeiten der verschiedenen ISMS zu finden, muß zunächst einmal betrachtet werden, welche ISMS kombiniert werden sollen. So macht eine Kombination auf der Ebene der Policies bei PCI DSS keinen Sinn, da dieser Punkt nur sehr rudimentär abgebildet ist.

Prinzipiell lassen sich ISMS an den drei genannten Ebenen "Policies", "Konzepte" und "Methoden", wobei dies stark von den betrachteten Systemen abhängt. So lassen sich Systeme unterscheiden, bei denen die Umsetzung der Maßnahmen angepaßt an die jeweilige Umgebung gewählt werden kann (zum Beispiel ISO 27001) und Systeme wie zum Beispiel PCI DSS, bei denen die Umsetzung der Maßnahmen zwingend erforderlich ist. Systeme, bei denen die Maßnahmen nicht fest sind, lassen sich besser auf der Ebene der Policies vereinen, während Systeme, welche die Einhaltung von Maßnahmen zwingend

vorschreiben, sich besser auf der Ebene der Maßnahmen kombinieren lassen.

Nachdem wir nun Gemeinsamkeiten bei den ISMS gefunden und diese auch benannt haben, müssen wir im nächsten Schritt Möglichkeiten finden, diese systematisch zu nutzen, um die ISMS zu vereinen.

4.2 Möglichkeiten der Kombination von ISMS

Ein systematischer Ansatz, welcher die Systeme auf der Ebene der Policies vereint, besteht darin, von oben herab immer weiter in den Ebenen hinab zu steigen. Dieser Ansatz ist bei Systemen empfehlenswert, welche ihren Fokus auf Policies legen. Hierzu zählt ISO 27001 wie auch IT-Grundschutz. Der Ansatz, von oberster Schicht nach unten absteigend sich an das Problem heran zuarbeiten, wird als "Top-down" Methode bezeichnet.

Eine andere Möglichkeit besteht darin, von der Ebene der Methoden an die Sache heranzugehen. Dies lohnt sich bei ISMS, welche einen starken Methodenbezug haben und bei denen diese Maßnahmen zwingend umgesetzt werden müssen. Dies ist teilweise beim IT-Grundschutz wie auch beim PCI DSS der Fall. Da wir bei diesem Ansatz am untersten Ende der ISMS Hierarchie anfangen, wird hier diese Methode auch "Bottom-up" Methode bezeichnet. Abbildung 4.2 zeigt diesen Zusammenhang noch einmal grafisch.

4.2.1 Top-down Ansatz

Beim "Top-down" Ansatz vergleicht man zuerst die abstrakten Ansätze der verschiedenen ISMS. Hierzu werden die Policies der ISMS beleuchtet und auf Gemeinsamkeiten hin überprüft. Durch den abstrakten Charakter der Policies ist eine Kombination meist einfacher. Abstrakte Ansätze lassen sich leichter in die gewünschte Richtung ändern. Auch sind die Policies bei vielen ISMS größtenteils ähnlich.

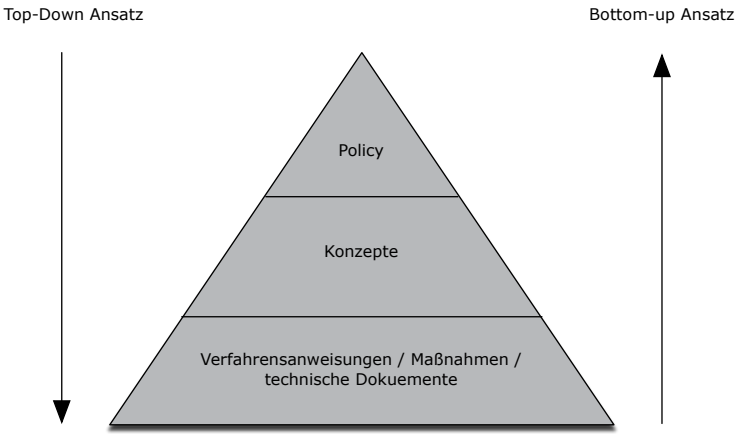

Abbildung 4.2: Vergleich Top-down und Bottom-up Ansatz

Durch die weitreichenden abstrakten Ansätze von ISO 27001/17799 und IT-Grundschutz lassen diese sich durch den "Top-down"-Ansatz gut zusammen führen. Bei stark methodenlastigen Ansätzen, wie zum Beispiel dem PCI DSS, ist dieser Ansatz schwierig.

Das BSI nutzt diesen Ansatz, um ISO 27001 und IT-Grundschutz zu kombinieren. Weitere Informationen findet man unter [27001-GS]

4.2.2 Bottom-up Ansatz

Einen anderen Ansatz verspricht das "Bottom-up"-Vorgehen. Hierbei wird versucht, einzelne Maßnahmen miteinander zu vereinen. Die verschiedenen Maßnahmen der ISMS werden hier auf Gemeinsamkeiten geprüft. Oft kommt es zu Überschneidungen bei den einzelnen Maßnahmen. Nachdem die unterste Ebene kombiniert ist, wird versucht, die nächst höhere Ebene zu kombinieren. Dieser Ansatz erscheint zunächst komplizierter, verspricht jedoch gerade bei PCI DSS einen guten Ansatz zur Kombination.

4.2.3 Vor - und Nachteile

Zusammenfassend lassen sich für beide Ansätze Vor- und Nachteile erkennen, anhand derer man die Wahl des richtigen Ansatzes treffen sollte.

Top-down Ansatz

Vorteile	**Nachteile**
Gut geeignet für abstraktere ISMS	Oft komplizierter durch abstrakten Ansatz
Schnell erste Ergebnisse	Ergebnisse nicht sehr aussagekräftig

Tabelle 4.1: Vor- und Nachteile beim Top-down Ansatz

Bottom-up Ansatz

Vorteile	**Nachteile**
Gut geeignet für methodenlastige Systeme	Langwierig in der Anfangsphase
Guter systematischer Ansatz möglich	Gute Kenntnisse der Maßnahmen nötig

Tabelle 4.2: Vor- und Nachteile beim Bottom-up Ansatz

Anhand dieser Erkenntnisse kann man nun die passende Methodik wählen. Im Fall von IT-Grundschutz und des PCI DSS wird in der exemplarischen Umsetzung die "Bottom-up" Methode benutzt, da methodenlastige ISMS kombiniert werden.

Nicht betrachtet wurden bisher die Kombination auf der mittleren Ebene. Man kann zwar theoretisch an diesem Punkt ansetzen, jedoch ist dies in der Praxis nicht praktikabel, da man in zwei Richtungen arbeiten müßte, was nicht wirtschaftlich ist.

Kapitel 5

Vorgehen zur Kombination verschiedener ISMS

In diesem Kapitel: Erläuterungen zum Vorgehen bei einer Kombination von ISMS.

Wie bereits in Kapitel 4.2 betrachtet, lassen sich zwei Vorgehensweisen anwenden, um verschiedene Systeme zu Kombinieren. In dem später betrachteten Beispiel-Fall wird das "Bottom-up"-Prinzip benutzt, da mindestens eins der betrachteten ISMS fast ausschließlich auf der Ebene der Richtlinien arbeitet. Der "Top-Down" Ansatz würde auch zum Ziel führen, jedoch gäbe es sehr viele Probleme, welche sich schwerer lösen lassen. Diese können zum Beispiel die fehlenden Policies des PCI DSS sein, durch deren Wegfall der Einstieg in die Kombination erschwert werden würde. Im Sinne einer kosteneffizienten Umsetzung scheidet dieses Vorgehen daher aus.

Durch die Verwendung des "Bottom-up" Ansatzes werden im Rahmen einer Kombination die verschiedenen Maßnahmen verknüpft. Da oft nicht alle Maßnahmen 1:1 in ein anderes System übernommen werden können, muss ein Vorgehen definiert werden, durch welches sich die Maßnahmen anpassen oder erweitern lassen. Die nachfolgende Auflistung gibt einen ersten Einblick in die vier möglichen Lösungsansätze. Eine Übersicht über das allgemeine Vorgehen findet sich in Abbildung 5.2.

Zur Vereinfachung werden in den folgenden Fällen die Begriffe ISMS1 und ISMS2 verwendet, bei welchen es sich um zwei verschiedene ISMS handelt.

Möglichkeit 1: Richtlinie/Maßnahme kann übernommen werden

In diesem einfachen Fall ist keine weitere Nachbearbeitung der Maßnahmen nötig. Er beinhaltet auch eine verteilte Ansicht der Maßnahmen. So kann beispielsweise eine Maßnahme aus ISMS1 in drei Maßnahmen des ISMS2 abgebildet werden.

Möglichkeit 2: Richtlinie/Maßnahme muss erweitert werden

In diesem Fall ist eine Richtlinie/Maßnahme unvollständig implementiert. Sie muss zur vollständigen Kombination der Systeme ergänzt werden.

Möglichkeit 3: Richtlinie/Maßnahme steht im Konflikt

Dieser Fall ist komplizierter. Es muss geprüft werden, ob sich diese Maßnahme so umändern läßt, daß die Anforderungen beider Systeme erfüllt werden oder ob man andere Möglichkeiten sieht, dieses Kriterium zu erfüllen.

Möglichkeit 4: Richlinie/Maßnahme ist nicht vorhanden

In manchen Fällen kann die Richtlinie in das andere ISMS übertragen werden werden. Dieser Fall grenzt sich zum Fall "Richtlinie/Maßnahme kann übernommen werden" dahin gehend ab, daß die Maßnahme im anderen ISMS noch nicht definiert ist. Durch die Übernahme kann es aber auch zu Problemen kommen, falls diese Methode aus einem bestimmten Grund nicht vorhanden ist.

Im folgenden wird zur Vereinfachung nur noch der Begriff der Maßnahme gewählt. Aus dieser Auflistung wird deutlich, das es ausser der einfachen 1:1-Übernahme von Maßnahmen auch die Möglichkeit gibt, eine Maßnahme zu ergänzen oder eine nicht vorhandene Maßnahme hinzuzufügen. Im Falle einer Konfliktsituation müssen mehrere Faktoren betrachtet werden. Näheres zur Lösung von Konflikten findet sich in Kapitel 5.3.

5.1 Maßnahme kann übernommen werden

Bei der Übernahme werden inhaltlich gleiche Maßnahmen gesucht. Ein Großteil der betrachteten Maßnahmen kann durch dieses Vorgehen kombiniert werden.

Um zwei Maßnahmen miteinander zu vergleichen, betrachtet man deren Inhalt. Man sucht Stichpunkte und versucht, diese in der Maßnahme des anderen ISMS wiederzufinden. Bei genauerer Betrachtung lassen sich wiederum drei Arten von möglichen Fällen unterscheiden:

- Einseitige Übereinstimmung
- Beidseitige Übereinstimmung
- Abbildung durch mehrere Maßnahmen/Richtlinien

Von der **einseitigen Übereinstimmung** spricht man, wenn die Maßnahme aus ISMS2 nur einen Teil von ISMS1 abbildet, jedoch die Kernaussage von ISMS1 trifft. In diesem Fall muss keine Erweiterung durchgeführt werden, da der Kernpunkt schon komplett abgebildet worden ist. Folgendes Beispiel soll diese "einseitige Übereinstimmung" verdeutlichen:

Eine Maßnahme aus ISMS1 beschreibt konkrete Maßnahmen zur Umsetzung der Passwortsicherheit. ISMS1 schreibt in diesem Falle vor, daß das Passwort mindestens 8 Zeichen lang ist, mindestens einen Großbuchstaben hat und nicht im Wörterbuch steht.

Die Maßnahme in ISMS2 sieht aber nur eine Passwortlänge von mindestens 8 Zeichen, ohne weitere Anforderungen vor. Falls nun die Maßnahme von ISMS1 umgesetzt worden ist, erfüllt diese automatisch die Anforderungen von ISMS2.

Beim zweiten Fall, der **beidseitigen Übereinstimmung**, stimmen die Maßnahmen von ISMS1 und ISMS2 genau überein. Eine weitere Betrachtung ist somit nicht mehr nötig.

Wichtig in diesem Zusammenhang ist eine eindeutige Auslegung der Begrifflichkeiten. Oft gibt es für die selbe Maßnahme mehrere Ausdrücke in der Fachsprache. Auch die Abbildung eines internationalen Systems in ein nationales System kann Probleme bereiten, da möglicherweise Probleme bei der Übersetzung der Begriffe auftreten können.

Folgendes Beispiel soll den Fall der "beidseitigen Übereinstimmung" verdeutlichen:

Wie auch im ersten Beispiel nehmen wir eine Maßnahme, welche die Passwortsicherheit definiert. In ISMS1 muss das Passwort nach 90 Tagen gewechselt werden. Dies ist auch bei ISMS2 der Fall.

Der letzte Fall ist komplexer. Bei der **Abbildung durch mehrere Maßnahmen** ist eine umfangreiche Überprüfung der verschiedenen Maßnahmen notwendig. Eine Maßnahme aus ISMS2 teilt sich hierbei in zwei oder mehr Maßnahmen aus ISMS1 auf. Alle Maßnahmen aus ISMS1 zusammen ergeben somit den Inhalt der Maßnahmen aus ISMS2. Bei diesem Ansatz ist ein genaues Wissen über die einzelnen Maßnahmen notwendig, um Übereinstimmungen zu finden.

Das folgende Beispiel gibt einen Überblick über die Abbildung durch mehrere Maßnahmen:

Im ISMS2 besagt die Maßnahme zum Passwortschutz, daß Passwörter mindestens 8 Zeichen lang sein und nach 90 Tagen gewechselt werden müssen. In ISMS1 ist diese Maßnahme in 2 verschiedene Maßnahmen aufgeteilt. Maßnahme 1 besagt daß Passwörter mindestens 8 Zeichen haben und Maßnahme 2 besagt daß Passwörter nach 90 Tagen gewechselt werden müssen. Jedoch stehen diese beiden Maßnahmen im Maßnahmenkatalog nicht direkt hintereinander, so daß man die verschiedenen Maßnahmenkataloge sehr gut kennen muss um übereinstimmungen zu finden.

In Abbildung 5.1 finden Sie eine grafische Übersicht über die verschiedenen Übereinstimmungs-Varianten.

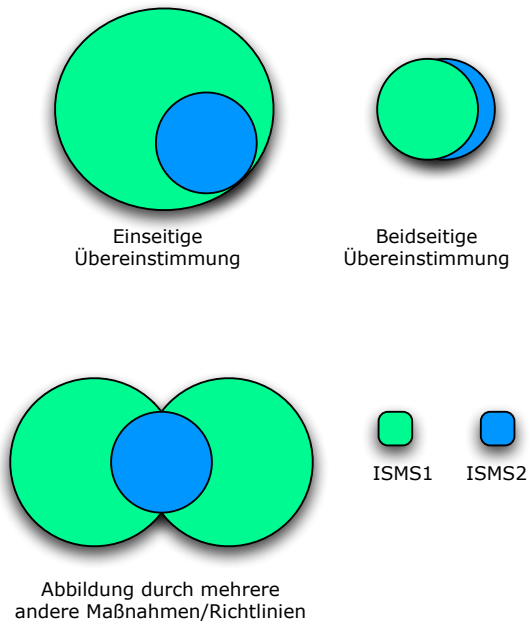

Abbildung 5.1: Übersicht über verschiedene Übereinstimmungsvarianten

5.2 Maßnahme muss erweitert werden

Oft existiert der Fall, daß eine Maßnahme eines ISMS nur einen Teil der Maßnahme des zweiten ISMS abbildet. Wenn sich nicht, wie im vorangegangenen Kapitel beschrieben, weitere Maßnahmen finden lassen, welche den fehlenden Teil der Maßnahme abbilden, kann es von Nöten sein, die Maßnahme zu erweitern. Ob eine Erweiterung sinnvoll ist hängt von den Gegebenheiten ab. Beispielweise läßt der PCI DSS Standard keine Erweiterung des Standards zu. Bei anderen System kann jedoch eine Erweiterung vorgenommen werden, wenn die Kernaussage nicht berührt wird. Dies gilt es vor einer Erweiterung zu prüfen. Beim IT-Grundschutz wird hierzu eine neue Maßnahme erstellt, welche zusätzlich zur alten, nicht vollständigen Maßnahme genutzt wird. Bei der exemplarischen Umsetzung der Maßnahmen des IT-Grundschutz im Kapitel 6 werden nur einseitige Erweite-

rungen auf Seite von IT-Grundschutz vorgenommen werden, da eine Erweiterung des PCI DSS nicht vorgesehen ist. Hierzu werden neue Bausteine erstellt, welche in Kapitel 6 näher erläutert wird.

Zur Verdeutlichung sei folgende Ausgangssituation gegeben:

Eine Maßnahme aus ISMS 1 beschreibt detailiert das Passwortmanagement in einer Unternehmung. Diese besagt, daß alle Passwörter mindestens 8 Zeichen lang sein müssen, aus Buchstaben und Nummern bestehen müssen und alle 90 Tage gewechselt werden müssen. Die Maßnahme aus ISMS2 schreibt das selbe vor, jedoch mit dem Unterschied, daß zusätzlich alle Passwörter auch mindestens einen Großbuchstaben enthalten.

Im beschriebenen Fall tritt das Problem auf, daß die Maßnahme des ISMS2 einen höheren Schutz fordert. Prinzipiell ist dies kein Problem, da ein höherer Schutz immer von Vorteil ist. Jedoch muss diese höhere Forderung auch in der Maßnahme von ISMS1 erscheinen. Hierzu muss diese erweitert werden. Im Falle von IT-Grundschutz würde man dies folgendermaßen lösen: Man definiert eine neue Maßnahme, welche als Erweiterung der alten Maßnahme dient. In ihr ist die Benutzung eines großgeschriebenen Buchstaben im Passwort definiert. Diese neue Maßnahme wird zusätzlich zur alten Maßnahme genutzt.

5.3 Richtlinie/Maßnahme steht im Konflikt

Eines der größten Probleme stellen Konflikte innerhalb der Maßnahmen der verschiedenen ISMS dar. Diese können rechtlicher, organisatorischer oder technischer Natur sein. Die Auflösung dieser Konflikte erfordert oft detailliertes Wissen über die einzelnen ISMS sowie ihrer Sonderregelungen. Beispielsweise gibt es bei dem PCI DSS eine Ausnahmeregelung, welche besagt, daß nationales Recht vor dem ISMS steht. Diese logische Regel kann jedoch auch zu Problemen führen. So muss zum Beispiel bei international tätigen Unternehmen jede Maßnahme einzeln geprüft werden, ob diese nicht gegen gültiges Recht verstößt. Eine einheitliche Umsetzung wird somit schwieriger.

5.3.1 Rechtlicher Konflikt

Beim rechtlichen Konflikt verstößt die Maßnahme gegen eine nationale Rechtsprechung. Dies kann dadurch passieren, daß die verschiedenen ISMS, ausser dem IT-Grundschutz, länderübergreifend arbeiten. So kann es zum Beispiel geschehen, daß eine Maßnahme vorschreibt, verschiedene Daten zu speichern, dies jedoch in Deutschland durch das Bundesdatenschutzgesetz [BDSG] nicht erlaubt ist.

PCI DSS sieht in einem solchen Fall vor, daß die entsprechende Maßnahme nicht oder nur zum Teil umgesetzt werden muss. Betrachten wir exemplarisch folgende Maßnahme aus den PCI DSS:

12.7 Screen potential employees to minimise the risk from internal sources.

In den USA würde diese Maßnahme bedeuten, daß der neue Mitarbeiter mehrere Sicherheitsprüfungen über sich ergehen lassen muss. Eine solche Vorgehensweise könnte die Überprüfung der Kreditwürdigkeit, des potentiellen kriminellen Hintergrundes und weitere Maßnahmen beinhalten. In Deutschland sind nicht alle Maßnahmen rechtlich zulässig. Das strenge Datenschutzgesetz verbietet hier zum Beispiel die Schufa-Auskunft.

Falls rechtliche Problemfälle auftauchen, sollten diese durch die eigene Rechtsabteilung (sofern existent) oder von einem externen Rechtsanwalt geprüft werden. Dies beugt Klagen durch die beteiligten Parteien vor (zum Beispiel durch Mitarbeiter).

5.3.2 Organisatorischer Konflikt

Organisatorische Mängel ergeben sich oft im Zusammenspiel von verschiedenen ISMS. Solche Mängel hängen mit der Unternehmensstruktur zusammen oder entstehen durch Konflikte in den Abläufen des Unternehmens. Betrachten wir folgende Maßnahmen:

"9.7.1 Label the media so it can be identified as confidential. (PCI DSS)"

"M 2.3 Datenträgerverwaltung
... Die äußerliche Kennzeichnung von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z. B. die Kennzeichnung eines Magnetbandes mit dem Stichwort "Telefongebühren"), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen. ...(IT-Grundschutz)"

Die Maßnahme des PCI DSS sieht vor, daß die Backup-Bänder klar als vertraulich zu kennzeichnen sind. Dies wiederspricht jedoch dem Ansatz von IT-Grundschutz, welcher zwar eine Kennzeichnung vorsieht, jedoch darf diese keine Rückschlüsse auf den Inhalt der Bänder geben. Ein als "vertraulich" definiertes Band regt nach IT-Grundschutz das Interesse eines Unbefugten.

Dies ist nur eines von vielen Beispielen für organisatorische Konflikte bei der Kombination verschiedener ISMS. Das Lösen dieser Konflikte erfordert mitunter einen engen Kontakt zu Beratern oder sachkundigen Mitarbeitern. Einige Konflikte lassen sich durch kleinere Anpassungen lösen, andere wiederum müssen durch die Wahl der richtigen Maßnahme gelöst werden. Hier hilft oft auch der Kontakt zu den Entwicklern des ISMS, welche oft eine Hilfestellung liefern können. Im Falle von IT-Grundschutz ist hierfür das BSI zuständig.

5.3.3 Technischer Konflikt

Die letzte Art von Konflikten ist technischer Natur. Beispielsweise werden in den Maßnahmen zweier ISMS verschiedene technische Lösungen zur Umsetzung gefordert. Anhand des PCI DSS läßt sich folgendes Beispiel kreieren:

4.1 Use strong cryptography and encryption techniques (at least 128 bit) such as Se-

cure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) to safeguard sensitive cardholder data during transmission over public networks. (PCI DSS)

M 5.66 Verwendung von SSL (IT-Grundschutz)

Die Maßnahme besagt, daß die Übertragung von Kreditkartendaten nur mit Hilfe starker Krypthografie geschehen darf. Andere ISMS Systeme schreiben nur vor, daß SSL Verschlüsselung genutzt werden sollte. Normalerweise würde man die Verwendung von starker Kryptographie im Rahmen einer Erweiterung der Maßnahme (vgl. Kapitel 5.2) für beide Systeme vorschlagen. Jedoch ist starke Kryptografie in einigen Ländern verboten.

Aus diesen Grund kann die Maßnahme nicht erweitert werden. SSL kann zwar genutzt werden, jedoch nur mit den genannten Einschränkungen. Im Falle von PCI DSS müßte die Verwendung von schwacher Kryptographie akzeptiert werden, da hier sonst gegen geltendes Recht verstoßen wird.

5.4 Richtlinie/Maßnahme ist nicht vorhanden

Falls es durch die vorangegangenen Schritte nicht geglückt ist, eine Maßnahme im anderen System abzubilden, muss diese neu erstellt werden. So ist zum Beispiel im IT-Grundschutz vorgesehen, daß der Anwender eigene Maßnahmen, Gefährdungen und Bausteine hinzufügen kann.

Wichtig bei der Erstellung neuer Maßnahmen ist eine abschließende Kontrolle. Oft werden Maßnahmen bewußt nicht aufgeführt, da sie zu Konflikten oder Problemen führen könnten. Sobald eine neue Maßnahme erstellt worden ist, muss sie auf die angesprochenen Konflikte aus Kapitel 5.3 hin untersucht werden.

Im Rahmen dieser Diplomarbeit werden in Kapitel 6 beispielhaft vier neue Bausteine entwickelt, welche auf vier ausgewählten Anforderungen des PCI DSS basieren. Hierbei werden die passenden Gefährdungen und Maßnahmen entwickelt und zahlreiche Beispiele für die Kombination gegeben.

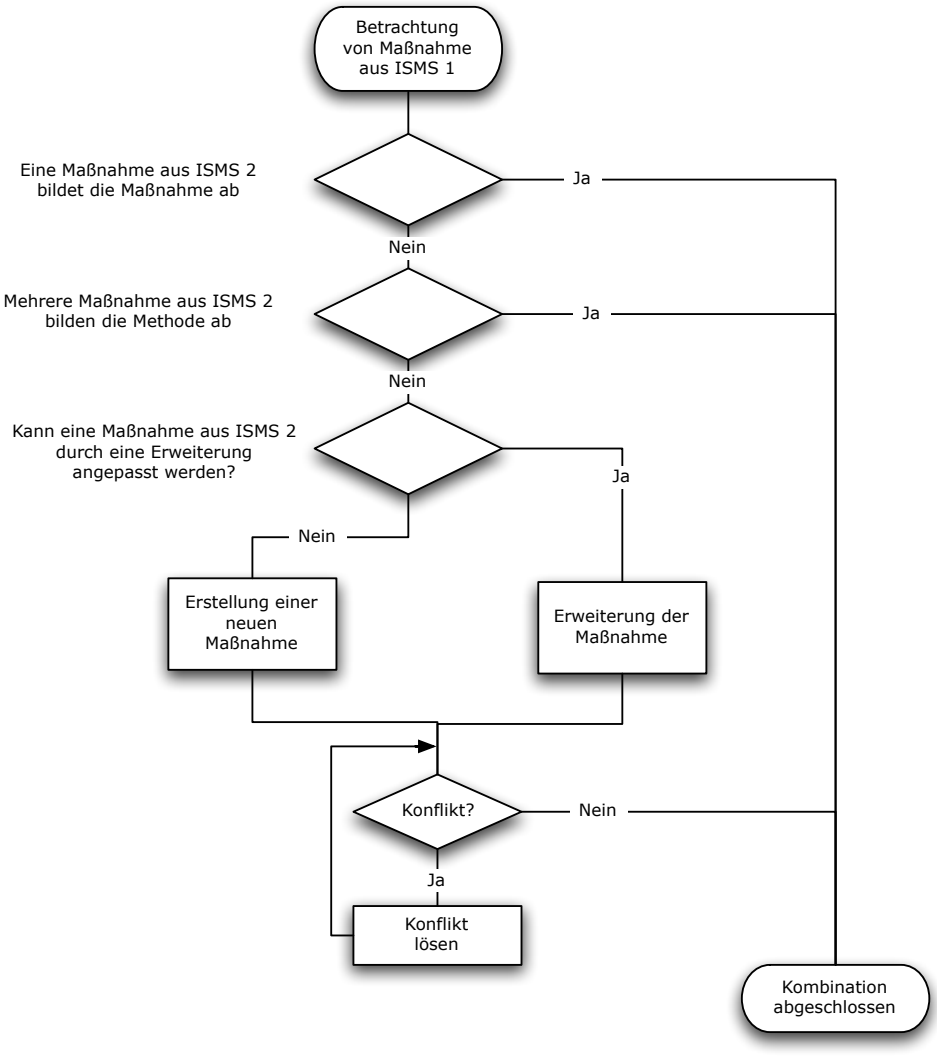

Abbildung 5.2: Vorgehensweise zur Kombination von Maßnahmen

Kapitel 6

Exemplarische Umsetzung der Kombination von PCI DSS und dem IT-Grundschutz

Im folgenden Kapitel sollen nun die Erkenntnisse aus Kapitel 5 genutzt werden, um eine exemplarische Umsetzung des PCI DSS in den IT-Grundschutz durchzuführen. Hierzu wird im folgenden kurz

- das allgemeine Vorgehen,
- die notwendigen Anpassungen am mittleren Profil, da der bisherige Betrieb keine Kreditkartenzahlungen verarbeitet,
- die Erstellung eines neuen Bausteins,
- sowie Ansätze zur Behebung von Konflikten erläutert.

Dieses Beispiel soll das Vorgehen zur Migration von PCI DSS und IT-Grundschutz verdeutlichen, sowie Probleme bei der Umsetzung darstellen. Hierdurch läßt sich eine weiterführende Umsetzung weiterer Bausteine schneller durchführen, da Probleme in der exemplarischen Umsetzung detailliert erläutert werden.

6.1 Vorgehen zur Umsetzung

In der folgenden Umsetzung wird die Kombination von PCI DSS und dem IT-Grundschutz anhand des mittleren Profils des IT-Grundschutz dargestellt. Das mittlere Profil des BSI geht nicht von einem Kreditkartendaten verarbeitenden Unternehmen aus, welches jedoch die Grundlage für die Umsetzung des PCI DSS ist. Aus diesem Grund wird der IT-Verbund des mittleren Profils um einige Punkte erweitert, um die nötigen Voraussetzungen für PCI DSS zu schaffen.

Nach der Anpassung des Profils sind die notwendigen Voraussetzungen für eine Kombination, unter Zuhilfenahme der in Kapitel 5 genannten Vorgehensweisen, gegeben. Im folgenden Schritt werden Maßnahmen entwickelt, welche zu den Anforderungen von PCI DSS passen. Anders als bei IT-Grundschutz werden jedoch keine Maßnahmen aus den Gefährdungen heraus entwickelt, da diese durch PCI DSS bereits fest vorgegeben sind. Vielmehr werden die entsprechenden Maßnahmen der beiden ISMS auf mögliche Kombinationsmöglichkeiten verglichen. Die durch die Kombination entstandenen Bausteine sollen dann später auf den IT-Verbund angewandt werden. Dies wird jedoch im Rahmen dieser Arbeit nicht durchgeführt.

6.2 Nötige Anpassungen am IT-Verbund

Das Unternehmen des mittleren Profils erfüllt nicht die benötigten Voraussetzungen für eine PCI DSS Zertifizierung. Um in das Raster von PCI DSS zu fallen, müssen Unternehmen Kreditkartendaten speichern, bearbeiten oder übertragen. Im Beispiel des mittleren Profils ist dies nicht gegeben. Aus diesem Grund wird das Unternehmen unter Zuhilfenahme des Werkzeugs GSTOOL dahingehend erweitert, daß ein typisches Kreditkartendaten verarbeitendes Unternehmen abgebildet wird. Im folgenden werden die nötigen Änderungen angesprochen, um in das Raster von PCI DSS zu passen. Eine ausführliche Liste des Änderungen mit weiteren Beschreibungen findet sich im Anhang A.

Das neue Unternehmen trägt nun die Firmenbezeichnung "Beratungs- und Entwicklungsunternehmen Albrecht" und produziert spezialisierte Software für andere Unternehmen. Die Software bietet das Unternehmen über das Internet an. Die eigenen Webseiten, auf denen die Produkte beworben werden, sowie der Online-Shop, welcher auch Kreditkartenzahlungen akzeptiert, stehen im eigenen Unternehmen. Die zu verkaufende Software und der Online-Shop werden durch die eigene Softwareentwicklungsabteilung entwickelt. Die beim Verkauf anfallenden Daten werden im Archiv für 10 Jahre gespeichert.

Ausgehend von diesen neuen Aufgaben des Unternehmens wird der IT-Verbund des mittleren Profils bearbeitet und neue Komponenten hinzugefügt, bestimmte Komponenten gelöscht sowie bereits vorhandene Komponenten angepasst. Im folgenden werden die benötigten Änderungen genauer darstellt. Den Netzplan des neuen Unternehmens kann in Abbildung 6.1 betrachtet werden.

6.2.1 Gebäude

Diese Komponente bedarf keiner Anpassung. Das Unternehmen ist weiterhin in einem Bürogebaude auf der dritten Etage. In dem Bürogebäude gibt es noch weitere Unternehmen, welche hier aber nicht weiter betrachtet werden.

6.2.2 Raum

Das neue Unternehmen hat eine neue Räumlichkeit, den Archivraum. In diesem Raum befindet sich zusätzlich ein Safe, welcher im IT-Verbund als eigenständiger Raum geführt wird. Die Räume werden in der folgenden Tabelle näher beschrieben. Die Räume 301 bis 304 werden zu einem Raum zusammengefasst. In diesem neuen Raum befindet sich nun der Vertrieb. Das alte Labor wurde zum Entwicklerbüro.

Name	Büro Entwickler	**Kurzname**	R-ENT
Anzahl	1	**Schutzbedarf**	hoch
Name	Archiv	**Kurzname**	AR
Anzahl	1	**Schutzbedarf**	normal

Name	Safe	**Kurzname**	SAFE
Anzahl	1	**Schutzbedarf**	hoch

Tabelle 6.1: Räume

6.2.3 IT-System

Es werden in diesem Beispiel fünf neue IT-Systeme benötigt. Es gibt einen neuen Mitarbeiter-PC für die Entwickler, sowie vier neue Server mit verschiedenen Funktionalitäten.

Name	PC Entwickler	**Kurzname**	PCENT
Anzahl	1	**Schutzbedarf**	normal
Name	Server Entwicklung	**Kurzname**	SRV ENT
Anzahl	1	**Schutzbedarf**	hoch
Name	Server Web (Kreditkartenverarbeitung)	**Kurzname**	SRV WEB
Anzahl	1	**Schutzbedarf**	hoch
Name	Server DB	**Kurzname**	SRV DB
Anzahl	1	**Schutzbedarf**	hoch
Name	Server Loging	**Kurzname**	SRV LOG
Anzahl	1	**Schutzbedarf**	hoch

Tabelle 6.2: IT-Systeme

6.2.4 Netz

Die neue Unternehmung braucht zwei neue Netze zur Anbindung von Webserver und Datenbank.

Name	NET DMZ WEB	**Kurzname**	DMZ WEB
Anzahl	1		
Name	NET DMZ DB	**Kurzname**	DMZ DB

Anzahl	1		

Tabelle 6.3: Netze

6.2.5 Anwendung

Im Rahmen der Erweiterung des mittleren Profils werden verschiedene neue Anwendungen benötigt, um die geforderten Dienste anzubieten.

Name	ANW Datenbank	**Kurzname**	DB
Anzahl	1	**Schutzbedarf**	hoch
Name	ANW Entwicklungs-umgebung	**Kurzname**	ENT
Anzahl	1	**Schutzbedarf**	normal
Name	ANW Loging	**Kurzname**	LOG
Anzahl	1	**Schutzbedarf**	hoch
Name	ANW Webserver	**Kurzname**	WEB
Anzahl	1	**Schutzbedarf**	hoch

Tabelle 6.4: Anwendungen

6.2.6 Mitarbeiter

Das neue Unternehmen verfügt über ein eigenes Entwicklerteam. Aus diesem Grund wird eine neue Mitarbeiterklasse eingeführt. Näheres hierzu finden Sie im Anhang A.

6.3 Erstellung neuer Bausteine

Nachdem nun das Unternehmen des mittleren Profils für eine Zertifizierung nach PCI DSS umgebaut worden ist, beginnen wir nun mit der Abbildung der 12 Anforderungen in Bausteine der IT-Grundschutz-Kataloge. Wie schon in Kapitel 3.2.1 erläutert, teilen sich die Bausteine in fünf Abschnitte auf. Zur Vereinfachung werden alle neuen Bausteine

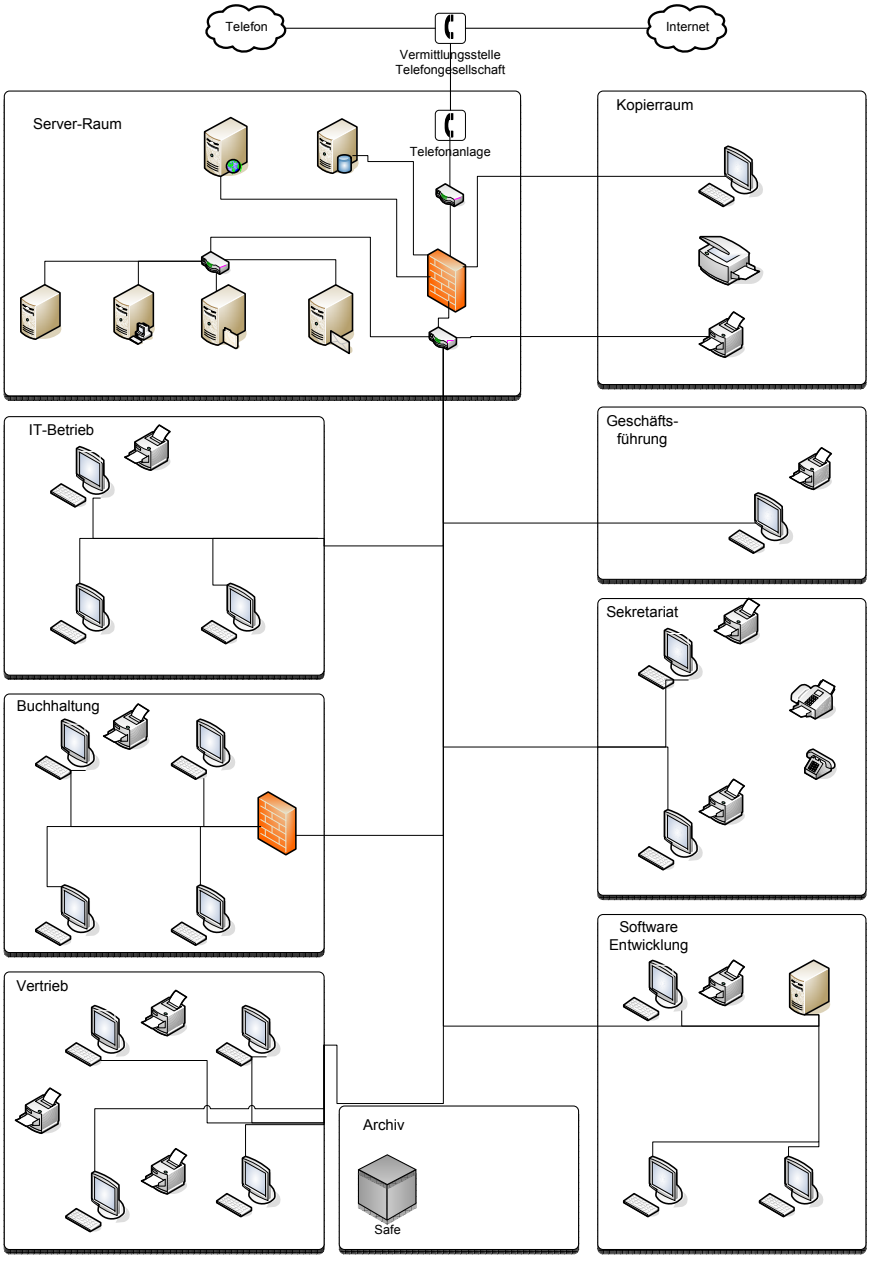

Abbildung 6.1: Mittleres Profil nach Änderungen

unter dem Abschnitt "Übergreifende IT-Sicherheitsaspekte" angelegt.

Folgende neue Bausteine werden für eine Umsetzung von PCI DSS benötigt:

- bB 1 - Installieren und verwalten Sie eine Firewall Konfiguration um Daten zu schützen (Original: Install and maintain a firewall configuration to protect data)
- bB 2 - Verwenden Sie keine Standardpasswörter und Standardsicherheitseinstellungen (Original: Do not use vendor-supplied defaults for system passwords and other security parameters)
- bB 3 - Schützen Sie gespeicherte Daten (Original: Protect stored data)
- bB 4 - Verschlüsseln Sie Verbindungen bei denen Kartendaten und sensiblen Information über öffentliche Netze übermittelt werden (Original: Encrypt transmission of cardholder data and sensitive information across public networks)
- bB 5 - Verwenden Sie eine Anti-Virus Software und aktualisieren Sie diese regelmäßig (Original: Use and regularly update anti-virus software)
- bB 6 - Entwicklen und verwalten Sie Systeme und Anwendungen sicher (Original: Develop and maintain secure systems and applications)
- bB 7 - Beschränken Sie den Zugriff auf Daten nach dem 'need-to-know' Prinzip (Original: Restrict access to data by business need-to-know)
- bB 8 - Jeder Benutzer muss einen eindeutigen Zugang haben (Original: Assign a unique ID to each person with computer access)
- bB 9 - Schränken Sie den physikalischen Zugriff auf Kartendaten ein (Original: Restrict physical access to cardholder data)
- bB 10 - Verfolgen und kontrollieren Sie den Zugriff auf Netzwerkkomponenten und Kartendaten (Original: Track and monitor all access to network resources and cardholder data)

- bB 11 - Testen Sie regelmäßig die Sicherheitssysteme und Prozesse (Original: Regularly test security systems and processes)
- bB 12 - Verwalten Sie eine Informationssicherheitsrichtlinie (Original: Maintain a policy that addresses information security)

Diese 12 Bausteine werden nun mit Gefährdungen und Maßnahmen gefüllt. Ein Baustein enthält jeweils eine kurze Beschreibung, welche üblicherweise Komponenten, Vorgehensweisen und IT-Systeme erläutert. Nach dieser Beschreibung werden ein Überblick über die Gefährdungslage sowie Maßnahmenempfehlungen gegeben.

Im folgenden werden beispielhaft die Bausteine bB2, bB5, bB7 und bB 11 erstellt. Die restlichen Bausteine lassen sich in gleicher Weise erstellen, dies würde jedoch aufgrund des Umfangs diese Arbeit sprengen.

6.3.1 Baustein bB 5

Um einen leichten Einstieg zu finden, wird mit dem Baustein “bB 5” begonnen. Dieser ist die kleinste Anforderung innerhalb von PCI DSS. Lediglich zwei Maßnahmen sind definiert:

- 5.1 Deploy anti-virus mechanisms on all systems commonly affected by viruses (e.g., PCs and servers).
- 5.2 Ensure that all anti-virus mechanisms current, and actively running, and capable of generating audit logs.

Die Betrachtung von Viren wird auch im IT-Grundschutz vorgenommen. Der Baustein ”B 1.6 Computer-Viren-Schutzkonzept” liefert hierfür sehr detaillierte Gefährdungen und Maßnahmen. Zuerst wird nun versucht, entsprechende Maßnahmen in den IT-Grundschutz-Katalogen zu finden, welche beide Anforderungen abbilden. Nach Durchsicht der Maßnahmen der IT-Grundschutz-Kataloge wurden folgende Maßnahmen ausgewählt:

- M 2.154 (A) Erstellung eines Computer-Virenschutzkonzepts

- M 2.155 (A) Identifikation potentiell von Computer-Viren betroffener IT-Systeme
- M 2.156 (A) Auswahl einer geeigneten Computer-Virenschutz-Strategie
- M 2.157 (A) Auswahl eines geeigneten Computer-Viren-Suchprogramms
- M 2.159 (A) Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
- M 4.3 (A) Regelmäßiger Einsatz eines Anti-Viren-Programms

Zur Vereinfachung werden im folgenden nur noch die Maßnahmennummern verwendet. Weiterführende Informationen zu den Maßnahmen und den später genannten Gefährdungen finden sich in den IT-Grundschutz-Katalogen unter [GSHB].

Wie in diesem Beispiel zu sehen ist, handelt es sich hierbei um eine "Abbildung durch mehrere Maßnahmen/Richtlinien" (siehe Kapitel 5.1). Dabei bilden mehrere Maßnahmen des IT-Grundschutz eine Maßnahme des PCI DSS ab. Im konkreten Fall handelt es sich dabei um die Maßnahmen M 2.154, M 2.155 und M 2.156, welche die Maßnahme 5.1 des PCI DSS abbilden.

Es fällt jedoch bei der Betrachtung der einzelnen Maßnahmen ein organisatorisches Problem auf. Maßnahme M 2.156 der IT-Grundschutz-Kataloge läßt dem Anwender die Wahl zwischen verschiedenen Virenschutz-Strategien. So kann der Anwender zwischen den Strategien "Computer-Viren-Suchprogramme auf jedem Endgerät", "Computer-Viren-Suchprovgramme auf allen Endgeräten mit externen Schnittstellen", "Computer-Viren-Suchprogramme auf allen Servern", "Computer-Viren-Suchprogramme auf allen Servern und Endgeräten", "Computer-Viren-Suchprogramme auf den Kommunikationsservern" und "Datenhygiene und zentrale Prüfung von Dateien" auswählen. Diese Auswahl widerspricht jedoch der Maßnahme 5.1 des PCI DSS. Diese besagt, daß Anti-Virus Programme auf **allen** Systemen eingesetzt werden, welche primär von Viren bedroht werden. Somit kann nur eine einzige Strategie gewählt werden, nämlich die Installation von "Computer-Viren-Suchprogramme auf allen Servern und Endgeräten".

Daher wurde die neue Maßnahme bM 2.156 erstellt, welche nur noch eine Strategie erlaubt. Der Konflikt ist somit gelöst. Die neue Maßnahme ist zugleich für den IT-Grundschutz als auch für den PCI DSS gültig ist. Die vollständige Maßnahme finden Sie in Anhang C.2.

Die zweite genannte Maßnahme des PCI DSS wird durch die Maßnahmen 2.159 und 4.3 des IT-Grundschutz abgedeckt. Auch hierbei handelt es sich um eine "Abbildung durch mehrere Maßnahmen/Richtlinien". Bei weiterer Betrachtung fällt jedoch auf, daß eine Anforderung fehlt. So wird in keiner Maßnahme Bezug auf das Generieren von Audit-Logs genommen. Dieser Punkt muss hinzugefügt werden. Der IT-Grundschutz sieht zwar im Falle eines Virenbefalls vor, daß die zuständigen Personen verständigt werden, jedoch wird in dieser Maßnahme nicht das Anlegen von Log-Files der Anti-Viren-Software erwähnt. Man hätte nun die Möglichkeit, die Maßnahme zu erweitern, oder die Anforderung in eine neue Maßnahme zu schreiben. Ich habe mich zu letzterer Vorgehensweise entschlossen, so daß die Maßnahmen des IT-Grundschutz nicht geändert werden müssen. Hierdurch erhält man besseren Überblick über die Änderungen. Da die Maßnahme M 1.158 des IT-Grundschutz thematisch in die selbe Richtung wie die gewünschte Maßnahme des PCI DSS geht, erhält die neue Maßnahme die Bezeichnung "bM 2.158 Logging von Computer-Virusinfektionen". Die Maßnahme läßt sich hierbei wie folgt definieren:

"bM 2.158 Logging von Computer-Virusinfektionen"

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement
Verantwortlich für Umsetzung: Leiter IT

Nach PCI DSS ist es vorgeschrieben, Meldungen von der Anti-Viren-Software zu protokolieren. Das Protokoll muss nach den unternehmensinternen Aufbewahrungs-Policy gespeichert werden.

Ergänzende Kontrollfragen:
Werden alle Meldungen der Anti-Viren-Software protokolliert?
Werden die Log-Files gemäß der Aufbewahrungspolicy gespeichert?"

Da zu einem Baustein des IT-Grundschutz auch Gefährdungen gehören, müssen diese noch nachgepflegt werden. Normalerweise werden im IT-Grundschutz aus den Gefährdungen die passenden Maßnahmen entwickelt. Mein Ansatz spielt diesem Vorgehen bewußt zu wieder, da die Gefährdungen in beiden Systemen schon definiert sind. Bei PCI DSS sind diese jedoch nicht niedergeschrieben, sondern ergeben sich implizit aus den Maßnahmen. Im Falle des Bausteins bB 5 sind folgende Gefährdungen geben:

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.8 Unkontrollierter Einsatz von Betriebsmitteln
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren

Menschliche Fehlhandlungen:

- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.44 Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:

- G 4.22 Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.80 Hoax

Auf die einzelnen Gefährdungen wird im Rahmen dieser Arbeit nicht eingegangen, da diese den Rahmen sprengen würden. Die komplette Beschreibung des Bausteins findet sich in Anhang B.2.

6.3.2 Baustein bB 7

Der zweite betrachtete Baustein lautet "bB 7 - Beschränken Sie den Zugriff auf Daten nach dem 'need-to-know' Prinzip". Auch dieser ist wie das erste Beispiel aus zwei Maßnahmen aufgebaut:

- 7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.
- 7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Ähnliche Regelungen nutzt auch der IT-Grundschutz im Baustein B 1.1, welcher jedoch noch viele andere Maßnahmen enthält. Nach erneuter Durchsicht aller Methoden des IT-Grundschutz bleiben drei Maßnahmen übrig, welche zu den Maßnahmen der ausgewählten Anforderungen passen. Diese lauten wie folgt:

- M 2.7 (A) Vergabe von Zugangsberechtigungen
- M 2.8 (A) Vergabe von Zugriffsrechten
- M 2.220 (A) Richtlinien für die Zugriffs- bzw. Zugangskontrolle

Eine genaue Aufteilung der Maßnahmen des IT-Grundschutz auf die Maßnahmen des PCI DSS ist kaum möglich. Vielmehr werden die beiden Maßnahmen des PCI DSS in den drei genannten Maßnahmen des IT-Grundschutz umgesetzt. Eine Erweiterung ist nicht mehr notwendig, da alle geforderten Maßnahmen erfüllt sind.

Es läßt sich jedoch feststellen, daß man leicht zu der Annahme kommen kann, daß nicht alle Forderungen des PCI DSS in den drei Maßnahmen abgebildet sind. So findet sich in den Maßnahmen kein Hinweis darauf, daß das 'Deny-all' Prinzip angewendet werden muss. Dieses läßt sich jedoch implizit aus der Anforderung ableiten, daß immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist (Maßnahme 2.8 IT-Grundschutz-Kataloge). Logischerweise läßt sich aus dieser Aussage schließen, das jemand keine Rechte bekommt, wenn er keine passenden Aufgaben hat. So wird eine Reinigungsfachkraft niemals eine Login für ein Computersystem bekommen, es sei denn, dieses würde explizit benötigt.

Der vollständige Baustein, wie auch die Gefährdungen findet sich in Anhang B.3.

6.3.3 Baustein bB 2

Nachdem bisher zwei relativ einfache Bausteine entwickelt worden sind, wird nun einen größerer Baustein betrachtet. Der Baustein "bB 2 - Verwenden Sie keine Standard-passwörter für Systeme oder sonstige Sicherheitseinstellungen" umfasst Regelungen, die sich mit der sicheren Konfiguration von IT-Systemen auseinandersetzt.

Die acht Maßnahmen des PCI DSS lauten wie folgt:

- 2.1 Always change the vendor-supplied defaults before you install a system on the network (e.g., passwords, SNMP community strings, elimination of unnecessary accounts, etc.).
- 2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, WEP keys, default SSID, passwords, and SNMP community strings, and disabling of SSID broadcasts. Enable Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.
- 2.2 Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices.
- 2.2.1 Implement only one primary function per server (e.g., web servers, database servers, and DNS should be implemented on separate servers).
- 2.2.2 Disable all unnecessary and insecure services and protocols (those services and protocols known to be insecure and/or not directly needed to perform the devices' specified function).
- 2.2.3 Configure system security parameters to prevent misuse.
- 2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (e.g. unnecessary, web servers).
- 2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Wie auch in den beiden Bausteinen zuvor, wird nun versucht, Parallelen in den Maßnahmen des IT-Grundschutzes zu finden. Von diesen gibt es viele, die den hier genannten Punkten angemessen sind. Diese gehe ich nun einzeln durch und erläutere meine Entscheidung von Fall zu Fall.

Die Maßnahme 2.1 des PCI DSS bezieht sich auf das Ändern standardmäßig gesetzter

Passwörter, Zugängen und weiteren Einstellungen. Der IT-Grundschutz bietet in diesem Falle einige Maßnahmen an, welche inhaltlich übereinstimmen. Zu diesen Maßnahmen gehören "M 4.7 Änderung voreingestellter Passwörter", "M 4.17 Sperren und Löschen nicht benötigter Accounts und Terminals" und "M 4.82 Sichere Konfiguration der aktiven Netzkomponenten". Dieser Fall ist wieder ein Beispiel für die "Abbildung durch mehrere Maßnahmen/Richtlinien" (siehe Kapitel 5.1). Drei Maßnahmen des IT-Grundschutz bilden eine Maßnahme des PCI DSS ab.

Die nächste zu besprechende Maßnahme bezieht sich auf sichere Einstellungen für Wireless LAN Umgebungen. Bei der Bearbeitung dieses Punktes fällt auf, daß der IT-Grundschutz kaum Bezug zur sicheren Nutzung dieser Umgebungen nimmt. Daher gibt es für die Maßnahme 2.1.1 kein passendes Gegenstück im IT-Grundschutz. Es muss hierfür eine neue Maßnahme geschrieben werden. Alle Anforderungen der Maßnahme des PCI DSS werden in Maßnahme "bM 5.1 Sichere Konfiguration von Wireless LAN" abgebildet. Die vollständige Maßnahmenbeschreibung findet sich unter Anhang C.5.

Die Maßnahme 2.2 muss näher betrachtet werden. Sie beschreibt die Einrichtung von Konfigurationsrichtlinien für alle standardmäßig genutzten Komponenten. Die Maßnahme ist organisatorischer Natur. Maßnahme 2.2.3 bezieht sich auch auf die sichere Konfiguration von IT-Systemen und ist daher technischer Natur. Der IT-Grundschutz bietet für beide Fälle eine Vielzahl von Maßnahmen an, welche sich jedoch nicht direkt auf eine der beiden Maßnahmen beziehen. Aus diesem Grund werden die Maßnahmen 2.2 und 2.2.3 zusammengefasst und die passenden Maßnahmen aus dem IT-Grundschutz herausgesucht. Hierdurch entsteht eine umfangreiche Maßnahmenliste, welche jedoch immer nur zu Teilen umgesetzt werden muss, da nicht immer alle hier genannten Komponenten zum Einsatz kommen. Folgende Maßnahmen wurden ausgewählt:

- M 2.87 - Installation und Konfiguration von Standardsoftware
- M 2.98 - Sichere Installation von Novell Netware Server

- M 2.99 - Sichere Einrichtung von Novell Netware Servern
- M 2.100 - Sicherer Betrieb von Novell Netware Servern
- M 2.125 - Installation und Konfiguration einer Datenbank
- M 2.148 - Sichere Einrichtung von Novell Netware 4.x Netzen
- M 2.149 - Sicherer Betrieb von Novell Netware 4.x Netzen
- M 2.174 - Sicherer Betrieb eines WWW-Servers
- M 2.223 - Sicherheitsvorgaben für die Nutzung von Standardsoftware
- M 2.273 - Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- M 2.316 - Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
- M 2.318 - Sichere Installation eines Servers
- M 3.11 - Schulung des Wartungs- und Administrationspersonals
- M 3.36 - Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
- M 3.37 - Schulung der Administratoren eines Apache-Webservers
- M 3.38 - Administratorenschulung für Router und Switches
- M 3.43 - Schulung der Administratoren des Sicherheitsgateways
- M 4.117 - Sichere Konfiguration eines Lotus Notes Servers
- M 4.126 - Sichere Konfiguration eines Lotus Notes Clients
- M 4.137 - Sichere Konfiguration von Windows 2000
- M 4.140 - Sichere Konfiguration wichtiger Windows 2000 Dienste
- M 4.141 - Sichere Konfiguration des DDNS unter Windows 2000

- M 4.142 - Sichere Konfiguration des WINS unter Windows 2000
- M 4.143 - Sichere Konfiguration des DHCP unter Windows 2000
- M 4.145 - Sichere Konfiguration von RRAS unter Windows 2000
- M 4.155 - Sichere Konfiguration von Novell eDirectory
- M 4.156 - Sichere Konfiguration der Novell eDirectory Clientsoftware
- M 4.162 - Sichere Konfiguration von Exchange 2000 Servern
- M 4.165 - Sichere Konfiguration von Outlook 2000
- M 4.175 - Sichere Konfiguration von Windows NT/2000 für den IIS
- M 4.194 - Sichere Grundkonfiguration eines Apache-Webservers
- M 4.209 - Sichere Grundkonfiguration von z/OS-Systemen
- M 4.237 - Sichere Grundkonfiguration eines IT-Systems
- M 4.252 - Sichere Konfiguration von Schulungsrechnern

Diese umfangreiche Liste wirkt auf den ersten Blick abschreckend. Wie jedoch zuvor erwähnt, müssen nicht alle Maßnahmen vollständig umgesetzt werden. In einem Unternehmen, welches nur Windows Server einsetzt, muß es zum Beispiel keine Richtlinie für Novell Netware Systeme geben. Es wird aber deutlich, daß der IT-Grundschutz sehr viel detailliertere Maßnahmen bereitstellt, als der in manchen Teilen allgemein gehaltene PCI DSS.

Maßnahme 2.2.1 läßt sich wiederum sehr einfach abbilden. Hierzu bietet der IT-Grundschutz das entsprechende Gegenstück durch die Maßnahme "M 4.97 Ein Dienst pro Server". Es handelt sich in diesem Fall um eine "beidseitige Übereinstimmung".

Als nächstes folgt die Maßnahme 2.2.2 des PCI DSS. Nach Durchsicht der Maßnahmen

des IT-Grundschutz stellt man fest, daß Maßnahme "M 4.95 Minimales Betriebssystem" die Anforderungen am besten abbildet. Es wird auch hier wieder deutlich, daß nicht alle Anforderungen abgebildet werden. So fehlen Maßnahmen, welche es verbieten, unsichere Protokolle zu verwenden. Der IT-Grundschutz gibt zwar den Hinweis, daß diese Protokolle nicht verwendet werden sollen, verbietet sie jedoch nicht völlig. Dieses Verbot ist aber zwingend für eine PCI DSS Zertifizierung erforderlich. Aus diesem Grund ist eine weitere neue Maßnahme "bM 5.2 Ersetzen unsicherer Protokolle" notwendig. Sie befasst sich mit den noch fehlenden Anforderungen bezüglich der Abschaltung unsicherer Protokolle bzw. dem zusätzlichen Schutz unsicher Protokolle durch sichere Protokolle, wie zum Beispiel durch ein VPN. Die vollständige Maßnahmenbeschreibung findet sich in Anhang C.6.

Eine neue Maßnahme ist für den nächsten Punkt nicht nötig. Maßnahme 2.2.4 des PCI DSS läßt sich durch fünf Maßnahmen des IT-Grundschutz abbilden:

- M 4.95 - Minimales Betriebssystem
- M 4.184 - Deaktivieren nicht benötigter Dienste beim IIS-Einsatz
- M 4.186 - Entfernen von Beispieldateien und Administrations-Scripts des IIS
- M 4.187 - Entfernen der FrontPage Server-Erweiterung des IIS
- M 5.72 - Deaktivieren nicht benötigter Netzdienste

Der letze Punkt , Maßnahme 2.3 des PCI DSS, bereitet wieder die Aufgabe, eine entsprechende Maßnahme im IT-Grundschutz zu finden. Es gibt zwar Hinweise für die Verschlüsselung von administrativen Zugängen, jedoch keine bindende Maßnahme, welche dies regelt. Aus diesem Grund muss eine neue Maßnahme "bM 4.1 Verschlüsselung aller administrativen Zugänge" erstellt werden. Diese regelt den Zugriff über eine Remote-Verbindung aus dem eigenen LAN. Remote-Verbindungen aus einem externen Netz erfordern wiederum stärkere Schutzmaßnahmen, die jedoch nicht Bestandteil dieses Bausteins sind. Die vollständige Maßnahmenbeschreibung findet sich unter Anhang C.4.

Der vollständige Text des neuen Bausteins findet sich unter Anhang B.1.

6.3.4 Baustein bB 11

Der letze im Rahmen dieser Diplomarbeit betrachtete Baustein bB 11 ist die Anforderung 11 des PCI DSS. Dieser Baustein beschreibt den fortlaufenden Prozess, in dem IT-Systeme und Prozesse regelmäßig getestet werden. Er bezieht sich zum einen auf Vulnerability Scans, Penetration Scans und den Einsatz von Intrusion Detection Systemen. Zum anderen erfolgt eine Prüfung aller Einstellungen des Netzwerkes, um Anomalien zu erkennen und zu unterbinden. Die Anforderung setzt sich aus den folgenden fünf Maßnahmen zusammen:

- 11.1 Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorised access attempts.
- 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). Note that external vulnerability scans must be performed by a scan vendor qualified by the payment card industry.
- 11.3 Perform penetration testing on network infrastructure and applications at least once a year, and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment).
- 11.4 Use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

- 11.5 Deploy file integrity monitoring to alert personnel to unauthorised modification of critical system or content files, and perform critical file comparisons at least daily (or more frequentlybe automated).

Maßnahme 11.1 des PCI DSS befasst sich mit der Sicherheit von Netzwerken, welche regelmäßig auf ihre Sicherheit überprüft werden sollen. Wie bereits bei anderen Maßnahmen werden passende Maßnahmen des IT-Grundschutzes gesucht. Diese werden ggf. ergänzt oder neue Maßnahmen erstellt. Nach diesem Schema lassen sich für Maßnahme 11.1 des PCI DSS folgende Maßnahmen des IT-Grundschutz festlegen:

- M 4.26 Regelmäßiger Sicherheitscheck des Unix-Systems
- M 4.69 Regelmäßiger Sicherheitscheck der Datenbank
- M 2.282 Regelmäßige Kontrolle von Routern und Switches
- M 2.330 Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung

Diese Maßnahmen decken schon einen großen Teil der Anforderungen ab, aber bleiben kleine Lücken, die eine Zertifizierung nach PCI DSS gefährden könnten. Daher wird eine neue Maßnahme "bM 5.3 Regelmäßiger Check der Sicherheitseinstellungen" (Anhang C.7) erstellt, welche die fehlenden kritischen Punkte abdeckt.

Die nächste Maßnahme ist ein Speziallfall. Maßnahme 11.2 des PCI DSS schreibt vor, daß das Netzwerk vierteljährlich gescannt werden muss. Solch ein Scan muss durch das eigene Personal intern und von zertifizierten Anbietern extern durchgeführt werden. Der IT-Grundschutz sieht hierfür nur interne Scans vor. Sie sollten aber im schlechtesten Fall wöchentlich durchgeführt werden. Dies wird durch die Maßnahme "M 5.8 Regelmäßiger Sicherheitscheck des Netzes" geregelt. Eine spezielle Maßnahme "bM 5.4 Regelmäßiger externer Vulnerability Scan" wird zur Regelung externer Scans erstellt (siehe Anhang C.8) erstellt.

Der Scan eines externen, zertifizierten Anbieters wird innerhalb von PCI DSS viermal pro Jahr durchgeführt und zeigt Schwachstellen an den "Internet-facing systems" auf, also jenen Systemen, die einem Angriff von aussen ausgesetzt sein könnten. Diese Scans laufen in der Regel vollautomatisch ab und beeinträchtigen die Erreichbarkeit des zu scannenden Systems nicht. Im Gegensatz zu dem in der nächsten Maßnahme beschriebenen Penetrationstest ist die Security- oder auch Vulnerability Scan genannte Überprüfung unkritisch, da keine Angriffe auf Systeme durchgeführt werden.

Maßnahme 11.3 des PCI DSS schreibt einen jährlichen Penetrations-Scan vor. Dieses Vorgehens ist zwar in einigen Nebensätzen der Maßnahmen des IT-Grundschutz genannt, jedoch nie genauer spezifiziert. An dieser Stelle sei ein kurzer Exkurs zur Erklärung eines Penetrationsscans angedacht.

Ein Penetrationsscan ist eine Überprüfung der IT-Landschaft aus der Sicht eines Hackers. Hierbei wird durch verschiedene Methoden und Programme ein Angriff auf ein System durchgeführt, welcher zum Ziel hat, in das System einzudringen. Hierzu wird in der Regel zuerst ein Black-Box-Test durchgeführt und mit diesen Ergebnissen ein White-Box Test angestoßen. Die Ergebnisse aus diesen Tests helfen einen Unternehmen, die eigenen Systeme sicherer zu machen. Weitere Informationen zum Thema Penetrationsscans finden Sie unter [PEN].

Um die Maßnahme 11.3 des PCI DSS umzusetzen, wird eine neue Maßnahme "bM 2.1 Durchführung eines Penetrationstests" erstellt, welche die speziellen Anforderungen von PCI DSS abbildet. Die vollständige Maßnahme finden Sie in Anhang C.1.

Zur vollständigen Abbildung des Bausteins müssen noch zwei Maßnahmen betrachtet werden. Maßnahme 11.4 des PCI DSS beschreibt die Anforderung, daß Intrusion Detection Systeme (IDS) eingesetzt werden müssen, um Angriffe auf den IT-Verbund frühzeitig zu erkennen und die entsprechenden Gegenmaßnahmen einleiten zu können. Der IT-

Grundschutz sieht für diesen Fall ebenfalls den Einsatz eines IDS vor, jedoch ist diese Maßnahme im Rahmen einer IT-Grundschutzzertifizierung nicht verbindlich umzusetzen.

Wie auch bei Virenscannern ist das regelmäßige Aktualisieren eines IDS sehr wichtig, da laufend neue Angriffsmuster entstehen. Diesen beiden Anforderungen wird durch die Maßnahmen "M 5.71 Intrusion Detection und Intrusion Response Systeme" und "M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates" Rechnung getragen.

Die letzte Maßnahme dieses Bausteins sieht vor, daß kritische Dateien durch einen Integritätsmonitor überwacht werden müssen. Diese Maßnahme läßt sich sehr einfach durch "M 4.93 Regelmäßige Integritätsprüfung" erfüllen, welche zudem noch konkrete Hinweise zur Umsetzung gibt.

Damit wäre auch der vierte exemplarisch betrachtete Baustein kombiniert. Der vollständige Baustein und die Gefährdungen, findet sich in Anhang B.4.

Die noch fehlenden acht Anforderungen des PCI DSS lassen sich über den hier beschriebenen Weg kombinieren. Eine derartige Lösung würde jedoch den Rahmen dieser Arbeit sprengen und wenig neue Erkenntnisse bringen. Daher wird an dieser Stelle darauf verzichtet.

Kapitel 7

Ausblick

In diesem Kapitel: Ausblick auf weitere Integrationsmöglichkeiten von ISMS.

7.1 Integration weiterer ISMS

Die zuvor genannte beispielhafte Kombination des PCI DSS mit Maßnahmen der IT-Grundschutz-Kataloge hat nur einen kleinen Teil der Möglichkeiten des Vorgehens gezeigt. Das Vorgehen ist bei den acht nicht betrachteten Anforderungen ähnlich. Man betrachtet eine Maßnahme eines ISMS und sucht die entsprechenden Maßnahmen des anderen ISMS. Hierbei ist das Vorgehensschema aus Kapitel 5.2 sehr sinnvoll.

Grundsätzlich lohnt es sich, die verschiedenen ISMS zu kombinieren und den Aufwand für die Pflege mehrer ISMS zu sparen. Eine solche Kosteneinsparung kann wiederum für die Umsetzung der Managementsysteme verwendet werden. Hier liegt das größte Problem der ISMS. Oft wird eine Umsetzung angefangen, jedoch nicht vollständig beendet. Meist wird das zur Verfügung gestellte Ressourcen in IT-Systeme investiert, welche die Sicherheit in einem Unternehmen garantieren sollen. In diesem Ansatz fehlt jedoch der organisatorische Gedanke, durch welchen ein umfassender Schutz erst möglich gemacht wird.

,

Über den vorgestellten Weg lassen sich auch andere ISMS Systeme wie ITIL (siehe auch [ITIL]) kombinieren. Die so entstehenden Synergieeffekte können zu einer kostengünstigen Kombination der verschiedenen ISMS genutzt werden.

7.1.1 Ansätze für die Integration des ISO 27001

Einen interessanten Ansatz zur Kombination zeigt das BSI. Der IT-Grundschutz wurde grundlegend überarbeitet und bietet nun, in der Version von 2005, eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz an. Das nähere Vorgehen sowie Ziele und Zertifizierungsschemas findet sich unter [27001-GS].

"Die ursprüngliche Zertifizierung nach IT-Grundschutz wird nach einer Übergangszeit durch eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz vollständig abgelöst. Die Integration von ISO 27001, die aus der BS 7799-2 hervorgegangen ist, macht diese ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz besonders für eine international tätige Institution interessant."[1]

7.1.2 Ansätze für die Integration anderer Sicherheitsmanagementsysteme

Auf Basis der in dieser Diplomarbeit genannten Vorgehensweisen ist eine Kombination verschiedener ISMS möglich. Daraus erwächst der Vorteil, daß nur ein System gepflegt werden muss und man trotzdem alle wichtigen Zertifizierungen durchführen lassen kann.

7.2 Schlussfolgerung

Die beiden kombinierten ISMS bieten ein gutes und zukunftssicheres System, welches den aktuellen Stand in der IT-Sicherheit wiederspiegelt. Einzig das fest durch PCI DSS

[1] BSI: http://www.bsi.bund.de/gshb/zert/ISO27001/ISO27001.htm

vorgegebene Risiko-Manangement stört diesen guten Eindruck. Dennoch wird die Kombination der Systeme für viele Unternehmen ein Anreiz sein, eine Zertifizierung anzustreben und somit einen besseren Stand im Umfeld der Mitbewerber zu haben.

Regierungsstellen verlangen zunehmend bei ihren Ausschreibungen eine Zertifizierung nach IT-Grundschutz oder auch ISO27001. Auch die steigende Abhängigkeit von IT-Systemen verstärkt innerhalb der Unternehmung den Druck zur Umsetzung eines ISMS, um Risiken besser abschätzen zu können und sich besser auf Probleme vorbereiten zu können.

Gerade für kreditkartendatenverarbeitende Unternehmen ist der Ansatz zur Kombination verschiedener ISMS der richtige Weg, um Kosten zu sparen und ein vollständiges IT-Sicherheitsmanagement zu haben. PCI DSS beschreibt hier nur einem kleinen Teil des Sicherheitsmanagements. Eine solche Vorgehensweise erhöht die Akzeptanz innerhalb des Unternehmens, da ein schlüssiges Gesamtkonzept vorhanden ist.

Kapitel 8

Fazit

In diesem Kapitel: Mein persönliches Fazit aus der Diplomarbeit.

Ich habe durch diese Arbeit tiefe Einblicke in viele IMSM gewonnen und kenne nun die Stärken und Schwächen dieser Systeme. Speziell mit dem PCI DSS und IT-Grundschutz habe ich mich im Rahmen dieser Arbeit sehr detailliert beschäftigt.

Das Thema an sich wird meines Erachtens in Zukunft weitere Betrachtung finden und in dieser Hinsicht bin ich für meine berufliche Zukunft sehr gut aufgestellt. Mein erworbenes Wissen bringe ich schon jetzt in ein Unternehmen ein und nutze das dort vorhandene Wissen, um auch in andere Bereiche des IT-Sicherheitsmanagements vorzudringen.

Anhang A

Detailierte Änderungen am mittleren Profil

Anwendung: ARB, ANW Arbeitzzeitauswertung (allgemeine Anwendung)			
Vertraulichkeit:	hoch	Begründung:	Personenbezogene Daten!
Integrität:	normal	Begründung:	Veränderungen von Daten können schnell erkennt und behoben werden.
Verfügbarkeit:	normal	Begründung:	Nichtverfügbarkeit für mehr als 24 Stunden ist unkritisch.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PC201		

Anwendung: DB, ANW Datenbank (Datenbank)

Vertraulichkeit:	hoch	Begründung:	Kreditkartendaten sind höchst vertraulich und dürfen nicht in die Hände dritter gelangen.
Integrität:	hoch	Begründung:	Die Daten müssen einer erhöhten Intigritätsprüfung unterliegen.
Verfügbarkeit:	hoch	Begründung:	Ein Ausfall der Anwendung von bis zu 24 Stunden ist nicht tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :	SRV DB , SRV ENT		

Anwendung: ENT, ANW Entwicklungsumgebung ([allgemeine Anwendung])			
Vertraulichkeit:	normal	Begründung:	Informationen aus der Anwendung genießen hinsichtlich der Vertraulichkeit maximal einen mittleren Schutzbedarf, da ein Verlust der Vertraulichkeit maximal mittelschwere Auswirkungen auf die Institution hat.

Integrität:	normal	Begründung:	Da durch Verletzungen der Integrität nur die Ordnungsmäßigkeit der internen Abläfe gefährdet ist, wird der Schutzbedarf mit mittel eingeschätzt.
Verfügbarkeit:	normal	Begründung:	Auf die Anwendung kann für mehr als 24 Stunden verzichtet werden.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PCENT		

Anwendung: LOG, ANW Logging ([allgemeine Anwendung])			
Vertraulichkeit:	hoch	Begründung:	Die Logfiles beinhalten teils personenbezogene Daten.
Integrität:	hoch	Begru?ndung:	Die Logfiles dürfen nicht mehr Veränderbar abgespeichert werden.
Verfügbarkeit:	normal	Begründung:	Ein Ausfall der Anwendung von bis zu 24 Stunden ist tolerabel. Logfiles werden nach dem Ausfall gesammelt übertragen.

gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :	SRG LOG		

Anwendung: MAIL, ANW Mailserver und Groupware (E-Mail)			
Vertraulichkeit:	normal	Begründung:	Per Mail werden keine als vertraulich eingestuften Informationen versandt. Ebenso werden in der Groupware-Software keine vertraulichen Daten abgelegt.
Integrität:	normal	Begründung:	Veränderungen an Mails und in der Groupwarelösung abgelegter Daten können schnell erkannt und kompensiert werden.
Verfügbarkeit:	normal	Begründung:	Ein Ausfall der Mail-/Groupwarelösung für mehr als 3 Stunden kann toleriert werden, daher wird der Schutzbedarf als mittel eingestuft.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
IT-Systeme :	SRV MAIL		

Anwendung: OFF, ANW Office Lösung ([allgemeine Anwendung])			
Vertraulichkeit:	normal	Begründung:	Informationen aus der Anwendung genießen hinsichtlich der Vertraulichkeit maximal einen mittleren Schutzbedarf, da ein Verlust der Vertraulichkeit maximal mittelschwere Auswirkungen auf die Institution hat.
Integrität:	normal	Begründung:	Da durch Verletzungen der Integrität nur die Ordnungsmäßigkeit der internen Abläfe gefährdet ist, wird der Schutzbedarf mit mittel eingeschätzt.
Verfügbarkeit:	normal	Begründung:	Auf Informationen aus der Anwendung kann für mehr als 24 Stunden verzichtet werden, daher wird der Schutzbedarf als niedrig eingestuft.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PCENT , PC999 , PC , PC201		

Anwendung: RECH, ANW Rechnungswesen ([allgemeine Anwendung])			
Vertraulichkeit:	hoch	Begründung:	Informationen aus der Anwendung genießen hinsichtlich der Vertraulichkeit maximal einen mittleren Schutzbedarf, da ein Verlust der Vertraulichkeit maximal schwere Auswirkungen auf die Institution hat.
Integrität:	normal	Begründung:	Verletzungen der Integrität werden durch interne Kontrollmaßnahmen (z.B. interne Qualitätssicherung) erkannt und beseitigt werden.
Verfügbarkeit:	normal	Begründung:	Auf Informationen aus der Anwendung kann für mehr als 24 Stunden verzichtet werden, daher wird der Schutzbedarf als niedrig eingestuft.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PC201		

Anwendung: ANWSPEZ, ANW Spezialanwendung ([allgemeine Anwendung])			
Vertraulichkeit:	normal	Begründung:	Informationen aus der Anwendung genießen hinsichtlich der Vertraulichkeit maximal einen mittleren Schutzbedarf, da ein Verlust der Vertraulichkeit maximal mittelschwere Auswirkungen auf die Institution hat.
Integrität:	normal	Begründung:	Verletzungen der Integrität werden durch interne Kontrollmaßnahmen (z.B. Qualitätssicherung) erkannt und beseitigt werden.
Verfügbarkeit:	normal	Begründung:	Auf Informationen aus der Anwendung kann für mehr als 24 Stunden verzichtet werden, daher wird der Schutzbedarf als niedrig eingestuft.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PCENT , PC		

Anwendung: WEB, ANW Webserver (Apache Webserver)			
Vertraulichkeit:	hoch	Begründung:	Kreditkartendaten sind höchst vertraulich und dürfen nicht in die Hände dritter gelangen.
Integrität:	hoch	Begründung:	Die Daten müssen einer erhöhten Intigritätsprüfung unterliegen.
Verfügbarkeit:	hoch	Begründung:	Ein Ausfall der Anwendung von bis zu 24 Stunden ist nicht tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :	SRV ENT , SRV WEB		

Anwendung: ZEIT, ANW Zeiterfassung (Datenbank)			
Vertraulichkeit:	normal	Begründung:	Informationen aus der Anwendung genießen hinsichtlich der Vertraulichkeit maximal einen mittleren Schutzbedarf, da ein Verlust der Vertraulichkeit maximal mittelschwere Auswirkungen auf die Institution hat.

Integrität:	normal	Begründung:	Verletzungen der Integrität werden durch interne Kontrollmaßnahmen (z.B. monatlich zu unterschreibender Arbeitszeitbogen) erkannt und beseitigt werden.
Verfügbarkeit:	normal	Begründung:	Auf Informationen aus der Anwendung kann für mehr als 24 Stunden verzichtet werden, daher wird der Schutzbedarf als niedrig eingestuft.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
IT-Systeme :	SRV-ZEIT		

IT-System: PCENT, PC Entwickler (Client/PC unter Windows 2000)			
Standort:	R-ENT, Büro Entwickler		
Vertraulichkeit:	normal	Begründung:	Es werden nur Daten verarbeitet/gespeichert, die innerhalb der Institution öffentlich sind.

Integrität:	normal	Begründung:	Veränderungen können durch die Mitarbeiter schnell erkannt und rückgängig gemacht werden.
Verfügbarkeit:	normal	Begründung:	Ausfall für mehr als einen Arbeitstag ist tolerabel. Es kann an einem Ersatzrechner weitergearbeitet werden.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
Netze :	LAN		
Anwendungen :	ENT , OFF , ANWSPEZ		

IT-System: PC999, PC Gast (Client/PC unter Windows 2000)			
Standort:	R205, Raum Kopierrer		
Vertraulichkeit:	normal	Begründung:	Speichern/Verarbeiten vertraulicher Daten ist untersagt.
Integrität:	normal	Begründung:	Speichern/Verarbeiten von Daten mit bedarf an Integrität ist untersagt.
Verfügbarkeit:	normal	Begründung:	Verfügbarkeit des Systems wird nicht gefordert.
gesamt:	normal		

benutzerdefiniert:		Begründung:	
Netze :	NETGAST		
Anwendungen :	OFF		

IT-System: PC, PC MA (Client/PC unter Windows 2000)			
Standort:	R-MA, Büro Mitarbeiter		
Vertraulichkeit:	normal	Begründung:	Es werden nur Daten verarbeitet/gespeichert, die innerhalb der Institution öffentlich sind.
Integrität:	normal	Begründung:	Veränderungen können durch die Mitarbeiter schnell erkannt und rückgängig gemacht werden.
Verfügbarkeit:	normal	Begründung:	Ausfall für mehr als einen Arbeitstag ist tolerabel. Es kann an einem Ersatzrechner weitergearbeitet werden.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
Netze :	LAN		
Anwendungen :	OFF , ANWSPEZ		

IT-System: PC201, PC Organisation/Finanzen (Client/PC unter Windows 2000)	
Standort:	R-ORG/FIN, Büro Organisation/Finanzen

Vertraulichkeit:	hoch	Begründung:	Da personenbezogene Daten verarbeitet werden, wird hohe Vertraulichkeit benötigt. Zusätzlich verabreiten diese Systeme senible Kreditkartendaten.
Integrität:	normal	Begründung:	Veränderungen an Daten können schnell erkannt und behoben werden.
Verfügbarkeit:	normal	Begründung:	Ausfall für mehr als einen Arbeitstag ist tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	NETORG		
Anwendungen :	ARB , OFF , RECH		

IT-System: SRV DB, Server DB (Server unter Unix/Linux)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	hoch	Begründung:	Kreditkartendaten sind höchst vertraulich und dürfen nicht in die Hände Dritter gelangen

Integrität:	hoch	Begründung:	Kreditkartendaten müssen einer erhöhten Integritätsprüfung unterliegen.
Verfügbarkeit:	hoch	Begründung:	Ein Ausfall des Systems von mehr als 24 Stunden ist nicht tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	DMZ DB		
Anwendungen :	DB		

IT-System: SRV ENT, Server Entwicklung (Server unter Unix/Linux)			
Standort:	R-ENT, Büro Entwickler		
Vertraulichkeit:	normal	Begründung:	Auf dem Server gespeicherte Informationen genießen hinsichtlich der Vertraulichkeit maximal einen mittleren Schutzbedarf, da ein Verlust der Vertraulichkeit maximal mittelschwere Auswirkungen auf die Institution hat.

Integrität:	normal	Begründung:	Verletzungen der Integrität der auf dem System gespeicherten Daten werden durch interne Kontrollmaßnahmen (z.B. Qualitätssicherung) erkannt und beseitigt werden.
Verfügbarkeit:	hoch	Begründung:	Ein Ausfall des Systems von mehr als 24 Stunden ist nicht tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	LAN		
Anwendungen :	DB , WEB		

IT-System: SRV-FILE01, Server File/Print (Server unter Windows 2000)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	hoch	Begründung:	Durch den Backup von Kreditkartendaten und personenbeogenen Daten, hat dieses System einen hohen Schutzbedarf.

Integrität:	hoch	Begründung:	Durch die Verarbeitung von Kreditkartendaten muss eine erhöhten Integritätsprüfung durchgeführt werden.
Verfügbarkeit:	normal	Begründung:	Das System ist redundant ausgelegt (Verteilungseffekt)
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	LAN		
Anwendungen :			

IT-System: FIREWALL01, Server Firewall (Client/PC unter Unix/Linux)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	normal	Begründung:	Filterlisten verden nicht als besonders schützenswert angesehen.
Integrität:	hoch	Begründung:	Integrität der gespeicherten Regeln muss sichergestellt sein.
Verfügbarkeit:	hoch	Begründung:	Ein Ausfall des Systems von mehr als 24 Stunden ist nicht tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	DMZ DB , DMZ WEB , NETGAST , LAN , INET		

Anwendungen :	

IT-System: SRG LOG, Server Logging (Server unter Unix/Linux)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	hoch	Begründung:	Da personenbezogene Daten verarbeitet werden, wird hohe Vertraulichkeit benötigt.
Integrität:	hoch	Begründung:	Die Integrität der Logfiles muss sichergestellt sein.
Verfügbarkeit:	hoch	Begründung:	Ein Ausfall des Systems von mehr als 24 Stunden ist nicht tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	LAN		
Anwendungen :	LOG		

IT-System: SRV MAIL, Server Mail (Server unter Unix/Linux)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	normal	Begründung:	Es werden keine personenbezogenen Daten gespeichert, da private Mails nicht erlaubt sind.

Integrität:	normal	Begründung:	Verletzungen der Integrität der auf dem System gespeicherten Daten werden durch interne Kontrollmaßnahmen (z.B. Qualitätssicherung) erkannt und beseitigt werden.
Verfügbarkeit:	normal	Begründung:	Ausfall für mehr als einen Arbeitstag ist tolerabel.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
Netze :	LAN		
Anwendungen :	MAIL		

IT-System: SRV WEB, Server Web(Server unter Unix/Linux)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	hoch	Begründung:	Kreditkartendaten sind höchst vertraulich und dürfen nicht in die Hände Dritter gelangen
Integrität:	hoch	Begründung:	Kreditkartendaten müssen einer erhöhten Intigritätsprüfung unterliegen.

Verfügbarkeit:	hoch	Begründung:	Ein Ausfall des Systems von mehr als 24 Stunden ist nicht tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	DMZ WEB		
Anwendungen :	WEB		

IT-System: SRV-ZEIT, Server Zeiterfassung (Server unter Unix/Linux)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	hoch	Begründung:	Es werden personenbesogene Daten gespeichert.
Integrität:	normal	Begründung:	Verletzungen der Integrität der auf dem System gespeicherten Daten werden durch interne Kontrollmaßnahmen (z.B. Qualitätssicherung) erkannt und beseitigt werden.
Verfügbarkeit:	normal	Begründung:	Ausfall für mehr als einen Arbeitstag ist tolerabel.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
Netze :	LAN		

Anwendungen :	ZEIT

IT-System: TKA, TK Anlage (TK-Anlage)			
Standort:	R210, Raum Server/IT/TK		
Vertraulichkeit:	normal	Begründung:	Die in der TK-Anlage gespeicherten Daten werden als nicht besonders Schützenswert angesehen.
Integrität:	normal	Begründung:	Die in der TK-Anlage gespeicherten Daten werden als nicht besonders Schützenswert angesehen.
Verfügbarkeit:	normal	Begründung:	Einen Ausfall von bis zu 24h kann toleriert werden, da Mobiltelefone als Ausweichmöglichkeit existieren.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
Netze :	ISDN		
Anwendungen :			

IT-System: AB, TK Anrufbeantworter (Anrufbeantworter)	
Standort:	R-MA, Büro Mitarbeiter

Vertraulichkeit:	normal	Begründung:	Auf dem Anrufbeantworter werden keine vertraulichen Informationen gespeichert.
Integrität:	normal	Begründung:	Die Integrität der gespeicherten Daten kann einfach überprüft und wiederhergestellt werden.
Verfügbarkeit:	normal	Begründung:	Ein Ausfall des Anrufbeantworters hat keine negativen Folgen.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
Netze :	ISDN		
Anwendungen :			

IT-System: Fax, TK Fax (Faxgerät)			
Standort:	R-MA, Büro Mitarbeiter		
Vertraulichkeit:	normal	Begründung:	Auf dem FAX werden keine vertraulichen Informationen gespeichert.
Integrität:	normal	Begründung:	Die Integrität der gespeicherten Daten kann einfach überprüft und wiederhergestellt werden.

Verfügbarkeit:	normal	Begründung:	Ein Ausfall des Faxgeräts hat keine negativen Folgen.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
Netze :	ISDN		
Anwendungen :			

IT-System: MOB01-MOBxx, TK Mobiltelefon (Mobiltelefon)			
Vertraulichkeit:	normal	Begründung:	Auf den Mobiltelefonen werden keine vertraulichen Informationen gespeichert.
Integrität:	normal	Begründung:	Die Integrität der gespeicherten Daten kann einfach überprüft und wiederhergestellt werden.
Verfügbarkeit:	normal	Begründung:	Ein Ausfall Mobiltelefons hat keine negativen Folgen.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
Netze :			
Anwendungen :			

Netz: DMZ DB, NET DMZ DB (heterogenes Netz)			
Vertraulichkeit:		Begründung:	

Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			
benutzerdefiniert:		Begründung:	
IT-Systeme :	SRV DB , FIREWALL01		

Netz: DMZ WEB, NET DMZ WEB (heterogenes Netz)			
Vertraulichkeit:		Begründung:	
Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			
benutzerdefiniert:		Begründung:	
IT-Systeme :	FIREWALL01 , SRV WEB		

Netz: NETGAST, NET Gast (heterogenes Netz)			
Vertraulichkeit:		Begründung:	
Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			
benutzerdefiniert:		Begründung:	
IT-Systeme :	PC999 , FIREWALL01		

Netz: LAN, NET Instituts-LAN (heterogenes Netz)			
Vertraulichkeit:		Begründung:	
Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			

benutzerdefiniert:		Begründung:	
IT-Systeme :	PCENT , PC , SRV ENT , SRV-FILE01 , FIREWALL01 SRG LOG , SRV MAIL , SRV-ZEIT		

Netz: INET, NET Internet (ISDN-Anbindung)			
Vertraulichkeit:		Begründung:	
Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			
benutzerdefiniert:		Begründung:	
IT-Systeme :	FIREWALL01		

Netz: ISDN, NET ISDN (Kommunikationsverbindung)			
Vertraulichkeit:		Begründung:	
Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			
benutzerdefiniert:		Begründung:	
IT-Systeme :	TKA , AB , Fax		

Netz: NETORG, NET ORG/FIN (heterogenes Netz)			
Vertraulichkeit:		Begründung:	
Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			
benutzerdefiniert:		Begründung:	
IT-Systeme :	PC201		

Gebäude: GEB, Bürogebäude der Institution ([allgemeines Gebäude])			
Vertraulichkeit:		Begründung:	
Integrität:		Begründung:	
Verfügbarkeit:		Begründung:	
gesamt:			
benutzerdefiniert:		Begründung:	
Räume :	AR , R-ENT , R-MA , R-ORG/FIN , R205 , R210 , SAFE		

Raum: AR, Archiv (Datenträgerarchiv)			
Gebäude :	GEB		
Vertraulichkeit:	hoch	Begründung:	Der im Archiv untergerachte Safe hate eine hohen Schutzbedarf. Somit erbt das Archiv den hohen Schutzbedarf.
Integrität:	normal	Begründung:	Die Intigrität des Archivraumes wird als normales Schutzbedarf angesehen.

Verfügbarkeit:	normal	Begründung:	Der Archivraum kann ohne Probleme bis zu 24 Stunden nicht verfügbar sein. Die Backupbänder im Safe können auch bis zu 24 Stunden nicht verfügbar sein, da ein Backup der letzten zwei Tage auch auf dem File-server liegt.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :			

Raum: R-ENT, Büro Entwickler (Büroraum)			
Gebäude :	GEB		
Vertraulichkeit:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Integrität:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Verfügbarkeit:	hoch	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	

IT-Systeme :	PCENT , SRV ENT		

Raum: R-MA, Büro Mitarbeiter (Büroraum)			
Gebäude :	GEB		
Vertraulichkeit:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Integrität:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Verfügbarkeit:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PC , AB , Fax		

Raum: R-ORG/FIN, Büro Organisation/Finanzen (Büroraum)			
Gebäude :	GEB		
Vertraulichkeit:	hoch	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Integrität:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.

Verfügbarkeit:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PC201		

Raum: R205, Raum Kopierrer ([allgemeiner Raum])			
Gebäude :	GEB		
Vertraulichkeit:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Integrität:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Verfügbarkeit:	normal	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
gesamt:	normal		
benutzerdefiniert:		Begründung:	
IT-Systeme :	PC999		

Raum: R210, Raum Server/IT/TK (Serverraum)			
Gebäude :	GEB		
Vertraulichkeit:	hoch	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.

Integrität:	hoch	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
Verfügbarkeit:	hoch	Begründung:	Leitet sich direkt aus dem Schutzbedarf der IT-Systeme ab.
gesamt:	hoch		
benutzerdefiniert:	Begründung:		
IT-Systeme :	SRV DB , SRV-FILE01 , FIRE-WALL01 , SRG LOG , SRV MAIL , SRV WEB , SRV-ZEIT , TKA		

Raum: SAFE, Safe (Schutzschrank)			
Gebäude :	GEB		
Vertraulichkeit:	hoch	Begründung:	Die auf den Backupbändern gespeicherten Daten haben einen hohen Wert für das Unternehmen.
Integrität:	hoch	Begründung:	Die Intigrität des Safe ist wichtig für das Unternehmen

Verfügbarkeit:	normal	Begründung:	Die Backupbänder im Safe können auch bis zu 24 Stunden nicht verfügbar sein, da ein Backup der letzten zwei Tage auch auf dem Fileserver liegt.
gesamt:	hoch		
benutzerdefiniert:		Begründung:	
IT-Systeme :			

Anhang B

Beschreibung neuer Bausteine im Rahmen der Beispielumsetzung

B.1 Baustein bB 2

Verwenden Sie keine Standardpasswörter für Systeme oder sonstige Sicherheitseinstellungen

Orginal: Do not use vendor-supplied defaults for system passwords and other security parameters

Beschreibung:

Ziel dieses Bausteins ist die sichere Inbetriebnahme von IT-Systemen. Hierzu werden verschiedene Maßnahmen definiert, welche zum Schutz vor fehlerhaften Konfigurationen dienen. Dies umfasst zum Beispiel das Ändern von Standardpasswörtern, Erstellung einer Konfigurationsrichtlinie und die Minimierung von Netzwerkdiensten.

Gefährdungslage:

Für den IT-Grundschutz werden bezüglich der sicheren Inbetriebnahme die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel:s

- G 2.5 Fehlende oder unzureichende Wartung
- G 2.23 Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz
- G 2.31 Unzureichender Schutz des Windows NT Systems
- G 2.34 Fehlende oder unzureichende Aktivierung von Novell Netware Sicherheitsmechanismen
- G 2.38 Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen

Menschliche Fehlhandlungen:

- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.18 Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
- G 3.20 Ungewollte Freigabe des Leserechtes bei Schedule+
- G 3.23 Fehlerhafte Administration eines DBMS
- G 3.26 Ungewollte Freigabe des Dateisystems
- G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.46 Fehlkonfiguration eines Lotus Notes Servers
- G 3.47 Fehlkonfiguration des Browser-Zugriffs auf Lotus Notes
- G 3.48 Fehlkonfiguration von Windows 2000/XP Rechnern

- G 3.49 Fehlkonfiguration des Active Directory
- G 3.50 Fehlkonfiguration von Novell eDirectory
- G 3.52 Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory
- G 3.53 Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory
- G 3.56 Fehlerhafte Einbindung des IIS in die Systemumgebung
- G 3.57 Fehlerhafte Konfiguration des Betriebssystems für den IIS
- G 3.58 Fehlkonfiguration eines IIS
- G 3.60 Fehlkonfiguration von Exchange 2000 Servern
- G 3.61 Fehlerhafte Konfiguration von Outlook 2000 Clients
- G 3.62 Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
- G 3.63 Fehlerhafte Konfiguration eines Apache-Webservers
- G 3.64 Fehlerhafte Konfiguration von Routern und Switches
- G 3.65 Fehlerhafte Administration von Routern und Switches
- G 3.67 Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems
- G 3.68 Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers
- G 3.72 Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF

Technisches Versagen:

- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.22 Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:

- G 5.10 Missbrauch von Fernwartungszugängen

- G 5.7 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.104 Ausspähen von Informationen

Maßnahmenempfehlungen:

Umd den genannten Bedrohungen zu begegnen empfielt es sich, eine sichere Konfiguration der IT-Landschaft sicherzustellen. Hierzu helfen Konfigurationsrichtlinien sowie allgemeine Regeln zur Abschicherung der IT-Landschaft. Folgende Maßnahmen sind hierfür umzusetzen.

- bM 4.1 Verschlüsselung aller administrativen Zugänge
- bM 5.1 Sichere Konfiguraion von Wireless LAN
- bM 5.2 Ersetzen unsicherer Protokolle
- M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems
- M 2.78 Sicherer Betrieb eines Sicherheitsgateways
- M 2.87 Installation und Konfiguration von Standardsoftware
- M 2.98 Sichere Installation von Novell Netware Servern
- M 2.99 Sichere Einrichtung von Novell Netware Servern
- M 2.100 Sicherer Betrieb von Novell Netware Servern
- M 2.125 Installation und Konfiguration einer Datenbank
- M 2.148 Sichere Einrichtung von Novell Netware 4.x Netzen
- M 2.149 Sicherer Betrieb von Novell Netware 4.x Netzen
- M 2.174 Sicherer Betrieb eines WWW-Servers
- M 2.223 Sicherheitsvorgaben für die Nutzung von Standardsoftware

- M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- M 2.316 Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
- M 2.318 Sichere Installation eines Servers
- M 3.11 Schulung des Wartungs- und Administrationspersonals
- M 3.36 Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
- M 3.37 Schulung der Administratoren eines Apache-Webservers
- M 3.38 Administratorenschulung für Router und Switches
- M 3.43 Schulung der Administratoren des Sicherheitsgateways
- M 4.7 Änderung voreingestellter Passwörter
- M 4.17 Sperren und Löschen nicht benötigter Accounts und Terminals
- M 4.82 Sichere Konfiguration der aktiven Netzkomponenten
- M 4.95 Minimales Betriebssystem
- M 4.97 Ein Dienst pro Server
- M 4.117 Sichere Konfiguration eines Lotus Notes Servers
- M 4.126 Sichere Konfiguration eines Lotus Notes Clients
- M 4.137 Sichere Konfiguration von Windows 2000
- M 4.140 Sichere Konfiguration wichtiger Windows 2000 Dienste
- M 4.141 Sichere Konfiguration des DDNS unter Windows 2000
- M 4.142 Sichere Konfiguration des WINS unter Windows 2000
- M 4.143 Sichere Konfiguration des DHCP unter Windows 2000

- M 4.145 Sichere Konfiguration von RRAS unter Windows 2000
- M 4.155 Sichere Konfiguration von Novell eDirectory
- M 4.156 Sichere Konfiguration der Novell eDirectory Clientsoftware
- M 4.162 Sichere Konfiguration von Exchange 2000 Servern
- M 4.165 Sichere Konfiguration von Outlook 2000
- M 4.175 Sichere Konfiguration von Windows NT/2000 für den IIS
- M 4.184 Deaktivieren nicht benötigter Dienste beim IIS-Einsatz
- M 4.186 Entfernen von Beispieldateien und Administrations-Scripts des IIS
- M 4.187 Entfernen der FrontPage Server-Erweiterung des IIS
- M 4.194 Sichere Grundkonfiguration eines Apache-Webservers
- M 4.209 Sichere Grundkonfiguration von z/OS-Systemen
- M 4.237 Sichere Grundkonfiguration eines IT-Systems
- M 4.252 Sichere Konfiguration von Schulungsrechnern
- M 5.72 Deaktivieren nicht benötigter Netzdienste

B.2 Baustein bB 5

bB 5 Verwenden Sie eine Anti-Virus Software und aktualisieren Sie diese regelmäßig

Originaltext: Use and regularly update anti-virus software

Beschreibung:

Ziel eines Computer-Viren-Schutzkonzeptes ist es, geeignete Maßnahmen zum Schutz vor

Schadprogrammen zusammenzustellen. Es soll gewährleistet sein, daß das Auftreten von Computer-Viren verhindert oder so früh wie möglich erkannt wird. Zusätzlich sind Maßnahmen zu benennen, die Schäden minimieren helfen, wenn ein Schadprogramm nicht rechtzeitig entdeckt werden konnte. Wesentlich ist die konsequente Anwendung der Maßnahmen und die ständige Aktualisierung der eingesetzten technischen Methoden. Diese Forderung begründet sich durch die täglich neu auftretenden Computer-Viren bzw. der Variation schon bekannter Computer-Viren. Durch die Weiterentwicklung von Betriebssystemen, Programmiersprachen und Anwendungssoftware entstehen weitere mögliche Angriffspotentiale für Computer-Viren, so daß rechtzeitig geeignete Gegenmaßnahmen eingeleitet werden müssen.

Wenn Behörden oder Unternehmen an öffentliche Kommunikationsnetze angeschlossen sind, ist die Gefahr durch Computer-Viren besonders groß. Die eingesetzten Rechner mu?ssen daher permanent auf Computer-Viren kontrolliert werden.

Gefährdungslage:

Für den IT-Grundschutz werden bezüglich Computer-Viren die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.8 Unkontrollierter Einsatz von Betriebsmitteln

- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren

Menschliche Fehlhandlungen:

- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.44 Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:

- G 4.22 Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.80 Hoax

Maßnahmenempfehlungen:

Bei der Erstellung eines Computer-Viren-Schutzkonzepts (siehe M 2.154 Erstellung eines Computer-Virenschutzkonzept,) muss zunächst ermittelt werden, welche der vorhandenen oder geplanten IT-Systeme in das Computer-Viren-Schutzkonzept einzubeziehen sind (siehe M 2.155 Identifikation potentiell von Computer-Viren betroffener IT-Systeme). Für diese IT-Systeme müssen die für die Umsetzung von Sicherheitsmaßnahmen relevanten

Einflussfaktoren betrachtet werden. Darauf aufbauend können dann die technischen und organisatorischen Maßnahmen ausgewählt werden. Hierzu ist insbesondere die Auswahl geeigneter technischer Gegenmaßnahmen wie Computer-Viren-Suchprogramme zu beachten (siehe M 2.156 Auswahl einer geeigneten Computer-Virenschutz-Strategie und M 2.157 Auswahl eines geeigneten Computer-Viren-Suchprogramms). Neben der Koordinierung der Aktualisierung eingesetzter Schutzprodukte (siehe M 2.159 Aktualisierung der eingesetzten Computer-Viren-Suchprogramme) ist für die Umsetzung auch das Speichern aller Vorfälle von Nöten (siehe bM 2.158).

Planung und Konzeption

- M 2.154 (A) Erstellung eines Computer-Virenschutzkonzepts
- M 2.155 (A) Identifikation potentiell von Computer-Viren betroffener IT-Systeme
- bM 2.156 Auswahl einer geeigneten Computer-Virenschutz-Strategie

Beschaffung

- M 2.157 (A) Auswahl eines geeigneten Computer-Viren-Suchprogramms

Betrieb

- bM 2.158 Logging von Computer-Virusinfektionen
- M 2.159 (A) Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
- M 4.3 (A) Regelmäßiger Einsatz eines Anti-Viren-Programms
- M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung

B.3 Baustein bB 7

Beschränken Sie den Zugriff auf Daten nach dem 'need-to-know' Prinzip

Orginaltext Restrict access to data by business need-to-know

Beschreibung

In diesem Baustein wird das Vorgehen für eine sichere Rechteverwaltung nach dem 'Need-to-know' Prinzip, sowie der 'Deny-All' Regel des Requirements 7 der PCI DSS dargestellt.

Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.9 Unberechtigte IT-Nutzung
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten

- G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/-2000/XP Systemen

Maßnahmenempfehlungen

Ein Mindestschutzniveau kann nur erreicht werden, wenn übergreifende Regelungen zur IT-Sicherheit verbindlich festgelegt werden. Hierzu sind eine Reihe von Maßnahmen umzusetzen, beginnend mit Festlegung und Zuweisung von verantwortlichen Personen für einzelne IT-Objekte (z. B. Anwendungen, IT-Komponenten) über entsprechende organisatorische Handlungsanweisungen bis hin zur ehandlung von schützenswerten Betriebsmitteln. Die Schritte, die dabei im Sinne eines kontinuierlichen IT-Sicherheitsprozesses durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Für die Initiierung und die Umsetzung der sich aus den Sicherheitszielen und Sicherheitsrichtlinien ergebenden Prozesse sind organisatorische und personelle Festlegungen zu treffen. Hierbei sind gegebenenfalls die Mitbestimmungsrechte des Personal- bzw. Betriebsrates zu wahren (siehe M 2.40 Rechtzeitige Beteiligung des Personal-/Betriebsrates). Die verschiedenen Organisationsebenen und die hier tätigen Personen benötigen konkrete Handlungsanweisungen und Verantwortlichkeiten zur Abwicklung der sie betreffenden Prozesse (siehe M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten).

Die strategischen Überlegungen sind in einem Betriebskonzept bezüglich ihrer Umsetzung im Unternehmen bzw. in der Behörde zu detaillieren.

Der Einsatz der erforderlichen Betriebsmittel ist auf die Aufgabenerfüllung und die Sicherheitsanforderungen abzustimmen und über eine Betriebsmittelverwaltung (siehe M 2.2 Betriebsmittelverwaltung) zu dokumentieren. Diese muss vollständig sein und durch

entsprechende Prozesse auch jederzeit aktuell gehalten werden.

Voraussetzung für eine funktionierende IT-Infrastruktur, die auch auf Störungen adäquat reagieren kann, sind Regelungen für Ersatzteilbeschaffung, Reparaturen und Wartungsarbeiten (siehe M 2.4 Regelungen für Wartungs- und Reparaturarbeiten). In Wartungsverträgen ist die terminliche und inhaltliche Wartung einzelner IT-Systeme (oder Gruppen) verbindlich zu regeln, ebenso wie die erforderlichen Zugänge (Remote, vor Ort) und die an die Sicherheitsanforderungen angepassten Reaktionszeiten des mit der Wartung beauftragten Personals.

Die Aufgabenverteilung und die hierfür erforderlichen Funktionen (siehe M 2.5 Aufgabenverteilung und Funktionstrennung) sind so zu strukturieren, daß operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu minimieren oder ganz auszuschalten.

Betrieb
Die festgelegten Konzeptionen werden in konkrete Handlungsanweisungen gefasst und für den Betrieb verbindlich verabschiedet. Mitarbeiterbezogene Regelungen müssen hierbei die komplette Laufbahn eines Mitarbeiters im Unternehmen vom Eintritt bis zum Austritt betrachten. Durch Anwendung des Need-to-Know-Prinzips und des Vier-Augen-Prinzips ist sicher zu stellen, das Berechtigungen auf den verschiedenen Ebenen (z. B. Zutritt zu Räumen, Zugang zu IT-Systemen) zielgerichtet vergeben werden und auch praktikabel sind (siehe M 2.6 Vergabe von Zutrittsberechtigungen und M 2.7 Vergabe von Zugangsberechtigungen).

Diese Berechtigungen sind zu dokumentieren und durch verschiedene Methoden zu unterstützen, wie z. B. kontrollierte und nachweisbare Ausgabe von Schlüsseln nur an Berechtigte (siehe M 2.14 Schlüsselverwaltung), Authentisierung von Zugriffen, Zutrittskontrollsysteme für speziell gesicherte Bereiche und Kontrolle der Aktionen Betriebsfremder

(siehe M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen). Die Zuordnung von Personen oder Personengruppen zu Rollen erleichtert die Verwaltung von Berechtigungen (siehe M 2.8 Vergabe von Zugriffsrechten). Werden Regelungen bewusst oder unbewusst verletzt, so müssen die hieraus ableitbaren Informations- und Eskalationsprozesse den Mitarbeitern bekannt sein, so daß eine zielgerichtete Reaktion auf die Verletzung erfolgen kann (siehe M 2.39 Reaktion auf Verletzungen der Sicherheitspolitik).

Nachfolgend wird das Maßnahmenbündel für den Bereich Baustein bB 7 vorgestellt:

Betrieb

- M 2.7 (A) Vergabe von Zugangsberechtigungen
- M 2.8 (A) Vergabe von Zugriffsrechten
- M 2.220 (A) Richtlinien für die Zugriffs- bzw. Zugangskontrolle

B.4 Baustein bB 11

Testen Sie regelmäßig die Sicherheitssysteme und Prozesse.

Orginal: Regularly test security systems and processes.

Beschreibung

Ziel dieses Bausteins ist die Überwachung und Überprüfung von Sicherheitsparametern des Netzwerkes. Hierzu kann man sich Vulnerability Scans, Penetration-Scans und Intrusion Detection Systemen behelfen. Diese bieten einen guten Grundschutz des Netzwerkes und der angeschlossenen IT-Systeme.

Gefährdungslage.

Für den IT-Grundschutz werden bezüglich der sicheren Inbetriebnahme die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel:

- G 2.4 - Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.7 - Unerlaubte Ausübung von Rechten
- G 2.37 - Unkontrollierter Aufbau von Kommunikationsverbindungen

Menschliche Fehlhandlungen

- G 2.37 - Unkontrollierter Aufbau von Kommunikationsverbindungen
- G 3.38 - Konfigurations- und Bedienungsfehler
- G 3.46 - Fehlkonfiguration eines Lotus Notes Servers
- G 3.47 - Fehlkonfiguration des Browser-Zugriffs auf Lotus Notes
  itemG 3.48 - Fehlkonfiguration von Windows 2000/XP Rechnern
- G 3.49 - Fehlkonfiguration des Active Directory
- G 3.50 - Fehlkonfiguration von Novell eDirectory
- G 3.61 - Fehlerhafte Konfiguration von Outlook 2000 Clients
- G 3.62 - Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
- G 3.63 - Fehlerhafte Konfiguration eines Apache-Webservers
- G 3.64 - Fehlerhafte Konfiguration von Routern und Switches
- G 3.65 - Fehlerhafte Administration von Routern und Switches

Technisches Versagen:

- G 4.22 Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:

- G 5.2 - Manipulation an Daten oder Software
- G 5.18 - Systematisches Ausprobieren von Passwörtern
- G 5.28 - Verhinderung von Diensten
- G 5.39 - Eindringen in Rechnersysteme über Kommunikationskarten
- G 5.48 - IP-Spoofing
- G 5.49 - Missbrauch des Source-Routing
- G 5.50 - Missbrauch des ICMP-Protokolls
- G 5.51 - Missbrauch der Routing-Protokolle
- G 5.55 - Login Bypass
- G 5.57 - Netzanalyse-Tools
- G 5.58 - "Hacking Novell Netware"
- G 5.108 - Ausnutzen von systemspezifischen Schwachstellen des IIS
- G 5.109 - Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver

Maßnahmenempfehlungen

Umd den genannten Bedrohungen zu begegnen empfielt es sich, eine sichere Konfiguration der IT-Landschaft sicherzustellen. Hierzu behilft man sich in der Regel durch Sicherheitsscans und Penetrationsscans sowie Integritätspüfenden Systemen

- bM 2.1 Durchführung eines Penetrationstests
- bM 5.3 Regelmäßiger Check des Sicherheitseinstelungen
- bM 5.4 Regelmäßiger externer Vulnerability Scan

- M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- M 2.282 Regelmäßige Kontrolle von Routern und Switches
- M 2.330 Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung
- M 4.26 Regelmäßiger Sicherheitscheck des Unix-Systems
- M 4.69 Regelmäßiger Sicherheitscheck der Datenbank
- M 4.93 Regelmäßige Integritätsprüfung
- M 5.8 Regelmäßiger Sicherheitscheck des Netzes
- M 5.71 Intrusion Detection und Intrusion Response Systeme

Anhang C

Beschreibung neuer Maßnahmen im Rahmen der Beispielumsetzung

C.1 Maßnahme bM 2.1

Durchführung eines Penetrationstests

Führen Sie mindestens einmal pro Jahr einen Penetrationstest auf das Netzwerk und Anwendungen durch. Dieser Test muss auch Durchgeführt werden, wenn signifikanten Änderungen an den Systemen vorgenommen worden sind.

C.2 Maßnahme bM 2.156

Auswahl einer geeigneten Computer-Virenschutz-Strategie

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Für die Umsetzung eines Computer-Virenschutzes sind personelle und finanzielle Ressourcen erforderlich, die in einem angemessenen Verhältnis zu dem tatsächlichen Bedrohungspotential stehen müssen. Für die Gesamtheit der identifizierten potentiell durch Computer-Viren bedrohten IT-Systeme sind folgende Einflussfaktoren zu erheben:

- Wie häufig findet über die vorhandenen Schnittstellen ein Datentransfer statt, der zu einer Infektion bzw. Verbreitung von Computer-Viren führen kann?
- Mit welchen Folgen ist bei einer tatsächlichen Infektion zu rechnen, wenn keine Schutzmaßnahmen ergriffen werden?
- Wie zuverlässig werden von den IT-Benutzern IT-Sicherheitsmaßnahmen durchgeführt, die periodisch zu veranlassen sind?
- Wieviel Zeitaufwand kann den IT-Benutzern für Computer-Viren-Schutzmaßnahmen zugemutet werden?

Bei Kenntnis der daraus und aus Fachveröffentlichungen ableitbaren Häufigkeit von Computer-Viren-Infektionen und der daraus entstehenden möglichen Folgeschäden ist unter Einbeziehung des Managements zu entscheiden, welche finanziellen Ressourcen für notwendige Maßnahmen zur Verfügung gestellt werden müssen und welche personellen Ressourcen bereitgestellt werden. In Kenntnis der finanziellen und personellen Ressourcen, die für den Computer-Virenschutz zur Verfügung stehen, und der identifizierten potentiell bedrohten IT-Systeme können Strategien ausgewählt werden, wie ein geeigneter Schutz erreicht werden kann.

Folgende Strategie ist für PCI DSS vorgeschrieben:

Computer-Viren-Suchprogramme auf allen Servern und Endgeräten. Diese Kombination obiger Strategien bietet den maximalen Schutz, da Computer-Viren sofort beim Auftreten erkannt werden und nicht über Server weiterverteilt werden. Darüber hinaus können

Computer-Viren-Suchprogramme verschiedener Hersteller eingesetzt werden, um so die Erkennungsrate für Computer-Viren zu erhöhen. Vorteile:

- Ein geeignetes, aktuelles und residentes Computer-Viren-Suchprogramm gewährleistet einen maximalen Schutz bei gleichzeitig minimalen Aufwand für den IT-Benutzer.
- Computer-Viren werden nicht über Server weiterverteilt.

Nachteile:

- Anschaffungskosten sowie Administrationsaufwand für jeden Server und jedes Endgerät. Unabhängig davon, welche Strategie für den Computer-Virenschutz gewählt wird, verbleibt immer das Restrisiko, daß Computer-Viren-Suchprogramme nur diejenigen Computer-Viren erkennen, die zum Entwicklungszeitpunkt des Programms bekannt waren. Das heißt, daß neue Viren ggf. nicht erkannt werden und Schäden anrichten können.

Die Wahl der richtigen und unter Kostengesichtspunkten angemessenen Strategie ist von der jeweiligen IT-Landschaft abhängig. Da jedoch beim Kauf von Mehrfach-Lizenzen der gängigen, geeigneten Computer-Viren-Suchprogramme sich meist die Kosten pro Lizenz stark reduzieren, empfiehlt es sich, über eine Komplettausstattung aller Server und Endgeräte nachzudenken.

Ergänzende Kontrollfragen:
Sind in der Vergangenheit Computer-Viren aufgetreten? Welche Schäden wurden verursacht (finanzielle Einbußen, Arbeitsausfall, ...)?
Wird die Entscheidung über den Ressourceneinsatz für den Computer-Virenschutz vom Management getragen?
Ist sichergestellt, daß bei Änderungen der IT-Landschaft über eine Anpassung der Computer-Virenschutz-Straegie nachgedacht wird?
Wurden die mit der gewählten Strategie verbundenen Nachteile dem IT-Sicherheitsmana-

gement verdeutlicht?
Werden die entstehenden Restrisiken getragen?

C.3 Maßnahme bM 2.158

Logging von Computer-Virusinfektionen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement
Verantwortlich für Umsetzung: Leiter IT

Nach PCI DSS ist es vorgeschrieben, Meldungen der Anti-Viren-Software zuprotokolieren. Das Protokoll muss nach den unternehmensinternen Aufbewahungs-Policien gespeichert werden.

Ergänzende Kontrollfragen:

Werden alle Meldungen der Anti-Viren-Software protokolliert?
Werden die Log-Files gemäßt der Aufbewahrungspolicy gespeichert?

C.4 Maßnahme bM 4.1

Verschlüsselung aller administrativen Zugäng

Alle nicht lokalen administrativen Aktivitäten müssen über verschlüsselte Verbindungen erfolgen. Dies kann über SSH, VPN, SSL/TLS für Web-basierte Systeme oder ein anderes abgescihertes System.

C.5 Maßnahme bM 5.1

Sichere Konfiguraion von Wireless LAN

Ändern Sie in die Standard Einstellungen in Wireless Umgebungen. Folgende Maßnahmen müssen durchgeführt werden:

- Der Standard WEP Schlüssel wurde nach der Installation geändert.
- Der WEP Schlüssel muss nach dem Verlassen eines Mitarbeiters geändert werden.
- Die Standard SSID muss geändert werden.
- SSID-Broadcast muss abgeschaltet sein
- Standard SNMP Community Strings der Access Points müssen geändert werden
- Die Standard Passwörter müssen geändert werden
- WPA muss aktiviert werden, falls das Wireless System dies unterstützt.
- Verwendung von herstellerspezifischen Sicherheitsmaßnahmen

C.6 Maßnahme bM 5.2

Ersetzen unsicherer Protokolle

Unsichere Protokolle wie TELNET, FTP, etc. müssen durch sichere Protokolle wie SSH oder andere Veschlüsselungstechnologien ersetzt/gesichert werden.

C.7 Maßnahme bM 5.3

Regelmäßiger Check der Sicherheitseinstellungen

Prüfen Sie regelmäßig

- Sicherheitskontrollen
- Limitationen
- Netzwerkverbindungen
- Restriktionen

des Netzwerkes, um unauthorisierten Zugriff zu unterbinden.

C.8 Maßnahme bM 5.4

Regelmäßiger externer Vulnerability Scan

Führen sie vierteljährliche Security Scans der Systeme durch. Diese müssen intern, durch eigenes Personal, wie auch extern durch einen qualifizierten PCI DSS Scan Anbieter.

Anhang D

Literaturverzeichnis

In diesem Kapitel: Literaturverzeichnis mit ISBN-Nummer bzw. Internetadresse.

Literaturverzeichnis

[GSHB]

Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz-Kataloge 2005*, 2005

`BSI, Bonn; http://www.bsi.de/gshb/deutsch/download/itgshb_2005.pdf`

[BSI-100-1]

Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*, 2005

`BSI, Bonn; http://www.bsi.bund.de/literat/bsi_standard/standard_1001.pdf`

[BSI-100-2]

Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise*, 2005

`BSI, Bonn; http://www.bsi.bund.de/literat/bsi_standard/standard_1002.pdf`

[BSI-100-3]

Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz*, 2005

`BSI, Bonn; http://www.bsi.bund.de/literat/bsi_standard/standard_1003.pdf`

[LEITFADEN]

Bundesamt für Sicherheit in der Informationstechnik: *Leitfaden IT-Sicherheit*, 2005
`BSI, Bonn; http://www.bsi.bund.de/gshb/Leitfaden/GS-Leitfaden.pdf`

[KLEINES]

Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutzprofil für eine kleine Institution*, 2005
`BSI, Bonn; http://www.bsi.bund.de/gshb/deutsch/hilfmi/profil_kl_institution.pdf`

[MITTLERES]

Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz für den Mittelstand*, 2005
`BSI, Bonn; http://www.bsi.bund.de/gshb/deutsch/hilfmi/profil_mittl_IT_Verbund.pdf`

[GROSSES]

Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz für eine große Institution*, 2005
`BSI, Bonn; http://www.bsi.bund.de/gshb/deutsch/hilfmi/profil_grosser_IT_Verbund.pdf`

[27001-GS]

Bundesamt für Sicherheit in der Informationstechnik: *ISO 27001-Grundschutz –Zertifizierungsschema*, 2005
`BSI, Bonn; http://www.bsi.bund.de/gshb/zert/ISO27001/schema.htm`

[ITIL]

Bundesamt für Sicherheit in der Informationstechnik: *ITIL und Informationssicher-*

heit, 2005

BSI, Bonn; http://www.bsi.de/literat/studien/ITinf/itil.pdf

[PEN]

Bundesamt für Sicherheit in der Informationstechnik: *BSI-Studie "Durchführungskonzept für Penetrationstests"*, 2005

BSI, Bonn; http://www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf

ISO

[27001]

British Standards Institute: *ISO/IEC 27001:2005*, 2005

BSI, UK; http://17799.standardsdirect.org

[17799]

British Standards Institute: *ISO/IEC 17799:2005*, 2005

BSI, UK; http://17799.standardsdirect.org

[13335]

International Standards Organisation: *ISO/IEC 13335:2005*, 2004

International Standards Organisation; http://www.iso.org

PCI

[PCIDSS]

Visa: *PCI Data Security Standard*, 2006

VISA, Europe; http://www.visaeurope.com/documents/ais/appendix_a.pdf

[PCIQUEST]

Visa: *PCI Self Assessment Questionnaire*, 2006

VISA, Europe; http://www.visaeurope.com/documents/ais/appendix_d.pdf

[PCIAUDIT]

Visa: *PCI Security Audit Procedures*, 2006

VISA, Europe; http://www.visaeurope.com/documents/ais/appendix_b.pdf

[PCISCAN]

Visa: *PCI Security Scanning Procedures*, 2006

VISA, Europe; http://www.visaeurope.com/documents/ais/appendix_c.pdf

[AIS]

Visa: *Account Information Security*, 2006

VISA, Europe; http://www.visaeurope.com/aboutvisa/
security/ais/main.jsp

[SDP]

MasterCard: *Site Data Protection*, 2006

MasterCard, International; https://sdp.mastercardintl.com/

Gesetze

[BDSG]

Bundesministerium der Justiz: *Bundesdatenschutzgesetz*, 1990

JURIS; http://www.gesetze-im-internet.de/bundesrecht/
bdsg_1990/gesamt.pdf

Sonstiges

[DEMING]

Deming W.E.: *Out of the Crisis*, 1986

MIT Press, Cambrigde MA; ISBN: 0262541157

[BB-IKT]

Globis GmbH *Bedeutung und Nutzung von Informations-, Kommunikationstechno-*

logien und E-Government-Lösungen in Brandenburger Unternehmen, 2005
Land Brandenburg; http://www.brandenburg.de/cms/media.php/1312/IuK_Studie_2005.pdf

[RISK-MITTEL]
Werner Gleißner, Herbert Lienhard, Dirk H. Stroeder: *Risikomanagement im Mittelstand*, 2004
RKW Verlag, Eschborn; ISBN: 3-89644-224-4

[SZENARIO-RISK]
Volker Bieta, Johannes Kirchhoff, Hellmuth Milde, Wilfried Siebe: *Szenarienplanung im Risikomanagement*, 2004
WILEY-VCH Verlag, Weinheim; ISBN: 3-89644-224-4

[SICHERHEITSMAN]
Maximilian Edelbacher, Paul Reither, Werner Preining: *Sicherheitsmanagement*, 1999
Linde Verlag, Wien; ISBN: 3-85122-955-X

[NACH-MS]
Jürgen Löbel, Heinz-Albert Schröder, Heiko Closhen: *Nachhaltige Managementsysteme*, 2005
Erich Schmidt Verlag, Berlin; ISBN: 3-503-08381-2

[COBIT]
Frederick Gallegos, Sandra Senft, Daniel P. Manson, Carol Gonzales: *Information Technology Control and Audit*, 2004
Auerbach Publications, New York; ISBN: 0-8493-2032-1

[ITIL-SF]
Peter T. Köhler: *ITIL. Das IT-Servicemanagement Framework*, 2005
Springer, Berlin; ISBN: 3540228934

[13335-TR]

Serdar Ayalp: *IT-Sicherheitsbewertung und ISO/IEC TR 13335*, 2006

Universität Koblenz, Koblenz; http://www.uni-koblenz.de/

s̃erdarayalp/ausarbeitung/tr.pdf

Erklärung:

Ich versichere, die von mir vorgelegte Arbeit selbständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Weilerswist, den

Daniel Jedecke