h_da
Hochschule Darmstadt
SS 2009

Master-Seminar-Arbeit

IT-Grundschutz

Einsatz des BSI Maßnahmenkataloges

von
Marco Münch B.Sc.

bei
Prof. Dr. Peter Wollenweber

Abstract

In dieser Seminararbeit wurde der Grundlagenkatalog (Stand: Oktober 2008) vom Bundesamt für Sicherheit in der Informationstechnik bearbeitet. Im speziellen wurde im Maßnahmenkatalog der Unterpunkt *M 4 Hardware und Software* bearbeitet.

Die Aufstellung wurde dabei so überarbeitet, das sie einfacher Angewendet werden kann. Anschließend werden Möglichkeiten und Abläufe besprochen wie diese Maßnahmen an besten in einer Organisation einsetzen werden können. Darüber hinaus werden vorhandene Schwachstellen identifiziert und besprochen.

Auch wird erklärt, wie die Wirksamkeit und Effizienz der Maßnahmen durch eine Validierung überprüft werden kann.

Am Ende dieser Arbeit wird ein Fazit gezogen, ob der Grundlagenkatalog des Bundesamt für Sicherheit in der Informationstechnik wirklich einen guten IT-Grundschutz bietet.

Schlüsselwörter: IT-Grundschutz, BSI, Grundschutz-Katalog, Maßnahmenkatalog, M4, Validierung von Maßnahmen

Inhaltsverzeichnis

1 Warum IT-Grundschutz?

Materielle Güter sind relativ einfach zu schützen, bei immateriellen Gütern ist es schon komplizierter. Heutzutage wird fast alles in elektronischer Form abgespeichert: Kundendaten, Geschäftsberichte, Forschungsergebnisse, Mitarbeiter, diese Liste kann noch sehr lange fortgeführt werden. Diese ganzen Daten müssen irgendwie gesichert werden. Nachdem Konread Zuse 1941 dem ersten funktionsfähigen Digitalrechners Z3 gebaut hat, ging die Entwicklung dieser Rechner in einem atemberaubenden Tempo voran, ohne dass die Personen sich über die Sicherheit der Daten groß Gedanken gemacht hatten.

Erst als die Rechner dazu eingesetzt wurden wichtige Daten für Unternehmen zu speichern, wurde über das Thema Sicherheit dieser Daten nachgedacht. So war es noch in den 70er sehr einfach elektronische und rechnergestützte Anlagen mit simplen Tricks zu umgehen. 1971 hat der Amerikaner Abbie Hoffman in seinem Buch „Steal This Book“ [Hof71] erklärt wie mittels eines simplen Tones, der über das Telefon übertragen wird, kostenlos telefonieren werden konnte. Das haben natürlich viele Amerikaner nachgemacht und den Telefonfirmen viel Geld gekostet.

In Deutschland wurde 1981 der Chaos Computer Club [Cha09a] gegründet um unter anderem auf derartige Sicherheitsrisiken aufmerksam zu machen, die nicht sofort als solche erkennbar sind. So ist es sehr einfach möglich mit Kleber, einem Laserdrucker und einem Glas einen Fingerabdruck zu erstellen [Cha09b], der die gängigsten Biometrischen Fingerabdruckscanner überlisten kann.

Solche unbedachten Sicherheitsrisiken können einem Unternehmen extremen Schaden zufügen. So können Daten ohne Sicherung verloren gehen, durch Rechnerausfall können wichtige Daten nicht verarbeitet werden oder die Produktion muss stillstehen, durch ungesicherte Schnittstellen können Daten manipuliert werden oder vertrauliche Daten können nach aus gelangen.

Die Probleme hierbei liegen meist im gestiegenen Vernetzungsgrad, der immer breiter werdenden Anwendungsbereiche, der höheren Interaktivität der einzelnen Programme, der wichtigen Rolle der Nutzer und den Angriffen von Hackern. Dieses breite Spektrum ist unmöglich von den IT-Administratoren komplett zu Überblicken, so dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) [Bun09a] sehr viele Informationen zu diesem Thema gesammelt und im Internet veröffentlicht hat.

So werden im IT-Grundschutz-Katalog die einzelnen Bausteine erklärt, die mit den Bereich des IT-Grundschutzes verwoben sind, es werden bekannten Gefahren

vorgestellt und anschließend Maßnahmen dagegen besprochen.

Diese Arbeit befasst sich mit dem Maßnahmenkatalog; dem Bereich der Hardware und Software im Speziellen.

2 Die Maßnahmenkataloge

Die Maßnahmenkataloge enthalten eine umfangreiche Sammlung an Maßnahmen gegen verschiedene Gefahren. Welche Gefahren das sind, wie sie ausfindig gemacht werden können wird in der Seminararbeit „Gefährdungsermittlung mit dem IT-Grundschutz-Katalog“ von Martin Schultheiß erläutert [Sch09]. Insgesamt wurden vom BSI sechs Maßnahmenkataloge erstellt. Diese sind gegliedert in:

- M 1 Maßnahmenkatalog Infrastruktur
- M 2 Maßnahmenkatalog Organisation
- M 3 Maßnahmenkatalog Personal
- M 4 Maßnahmenkatalog Hardware und Software
- M 5 Maßnahmenkatalog Kommunikation
- M 6 Maßnahmenkatalog Notfallvorsorge

So enthält der Maßnahmenkatalog M 1 wichtige Hinweise wie die Infrastrukturen in einer Organisation aussehen sollten. In M 2 wird die Organisation der IT Abteilung und deren Umfeld besprochen und in M 3 wie mit dem Personal zu verfahren hat. Erst im vierten Maßnahmenkatalog wird Hardware- und Software-Maßnahmen besprochen. Der fünfte Maßnahmenkatalog beschäftigt sich mit den elektronischen Verbindungen zwischen Rechnern, aber auch den Kommunikationswegen wie Fax oder E-Mail Versand. Ein weiterer wichtiger Punkt, die Vorsorge für den Notfall, wird in M6 behandelt. Hierbei werden Notfallpläne erarbeitet oder Hinweise zur Datensicherung gegeben.

Die einzelnen Maßnahmenkataloge sind in viele Unterpunkte unterteilt und somit gibt es nur wenig Überblick. Insgesamt gibt es 1148 verschiedene Maßnahmen, die in einzelnen Punkte eingeteilt werden. In Abbildung 1 wird diese Einteilung in die einzelnen Kataloge deutlich gemacht.

Aus der Abbildung 1 wird ersichtlich das zwei Maßnahmenkataloge besonders viele Punkte aufweisen: M 2 Organisation mit 430 und M 4 Hardware und Software mit 324. Die anderen Kataloge haben deutlich weniger, was nicht heißen mag, dass diese nicht wichtig sind. Diese Kataloge sind als Gesamtpaket anzusehen.

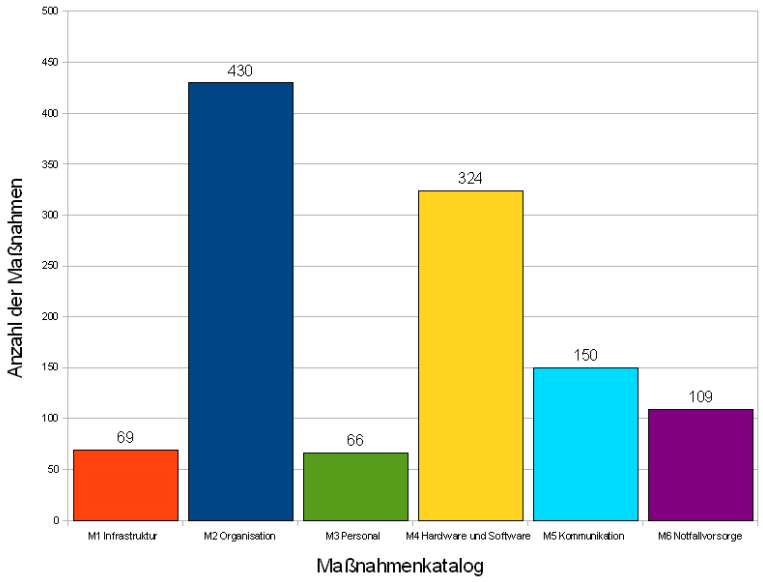

Abbildung 1: Anzahl der Maßnahmen

3 Der Maßnahmenkatalog M4

Der zweitgrößte Maßnahmenkatalog des BSI handelt über Hardware- und Software-Maßnahmen, der im weiteren Verlauf dieser Arbeit besprochen wird. Dieser Katalog enthält 324 verschiedene Maßnahmen (Stand: Oktober 2008). Dieser Katalog ist eine ungeordnete Liste an Maßnahmen.

Es werden sowohl Hardware wie Telekommunikations-Anlagen, Faxgeräte, Scanner, Drucker, Arbeitsplatz-PCs und Mainframes besprochen, als auch Softwareprodukte wie Novell eDirectory, IIS, Linux, viele Windows-Versionen und z/OS.Der Schwerpunkt liegt auf der Beschreibung von Software-Maßnahmen.

Einige Punkte, die im Maßnahmenkatalog angesprochen werden, sind allgemeingültig, wie z.b. der Einsatz von Virenscannern oder den Zugriffsschutz. Bei bestimmten Maßnahmen werden jedoch ganz bestimmte Maßnahmen für ganz bestimmte Produkte sehr ausführlich besprochen.

Damit im Maßnahmenkatalog nicht unnötig lange gesucht werden muss, wurden die Maßnahmen in Anhang A einmal nach den jeweilige Maßnahmen zusammengefasst. Zusätzlich wurden im Anhang B die Maßnahmen nach bestimmten Produkten geordnet.

3.1 Verantwortlich für die Umsetzung

Für die Gefahrenermittlung sind vier Personengruppen wichtig: Unternehmensführung, Interne Verantwortliche, Externer Berater und die Mitarbeiter [Sch09]. Unternehmensführung, Internere Verantwortliche und die Externer Berater stellen mögliche Maßnahmen zusammen und überprüfen sie Anhand einer Validierung (Siehe Kapitel 5).

Für die technische Umsetzung des Maßnahmenkataloges ist der Administrator verantwortlich. Und für die Einhaltung jeder einzelne Mitarbeiter.

Schon wenn ein einziger Mitarbeiter sich nicht an die Vorschriften hält, kann das komplette Sicherheitskonzept nicht mehr wirken. Darum benötigt die Firma auch einen IT-Schutzbeauftragten, der regelmäßig die Maßnahmen auf Nichteinhaltung hin überprüft. Bei Verstößen muss er tätig werden und den entsprechenden Mitarbeiter auf seinen Fehler hinweisen.

Ebenso müssen alle Mitarbeiter auf den neusten Stand gebracht werden, wenn neue Maßnahmen eingesetzt werden. Dies sollte nicht nur durch eine E-Mail oder einen Aushang passieren, sondern durch eine Gruppensitzung, damit sofort auftretende Fragen beantwortet werden können.

4 Anwendung des Maßnahmenkataloges M4

Der Umfang des Maßnahmenkataloges macht es schwierig, ohne langwierige Einarbeitungszeit, mit ihm zu arbeiten. Aus diesem Grund wurde, für diese Arbeit, der Maßnahmenkatalog M4 durchgearbeitet und aufbereitet. Dadurch ergibt sich folgender Ablauf, wie in Abbildung 2 zu sehen.

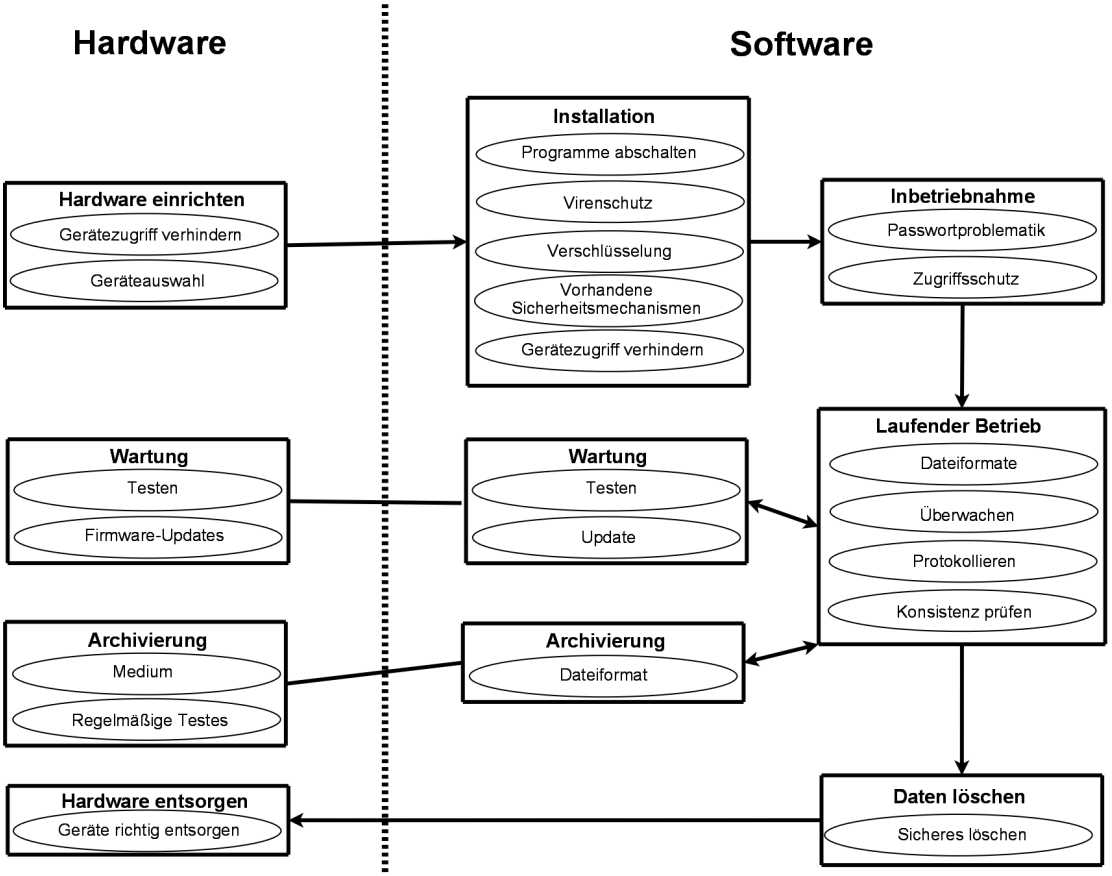

Abbildung 2: Möglichkeit einer Einteilung

Mit Hilfe dieses Schaubild und den folgenden Kapiteln soll es möglich sein, ohne umfassendes Studium des BSI Maßnahmenkataloges eine gewisse IT-Grundsicherung zu erreichen. Das Vorgehen kann in kleinen- und mittel-ständigen Unternehmen angewandt werden, bei größeren Unternehmen sollte zusätzlich einen IT-Sicherheitsexperten zu Rate ziehen, da hier die Gefahren komplizierter und verwobener sind.

Bei dieser Zusammenstellung gibt es unter anderem das Problem, das einige Punkte auch bei anderen Punkten mit aufgenommen werden könnte. So könnte der Punkt „Verschlüsselung“ nicht nur bei der „Installation“ stehen, sondern würde auch zum Punkt „laufenden Betrieb“ passen. In diesem Fall wird der Punkt zum frühst möglichen Zeitpunkt erwähnt.

Welche Maßnahmen ergriffen werden sollen, müssen erst Vorüberlegungen zeigen. Eine Möglichkeit hierfür ist die Anwendung der Gefährdungsformel $G_E = p_E * s_E$, wobei für G_E = Gefährdung, p_E = Wahrscheinlichkeit, dass ein Ereignis eintritt und s_E = Der durch das Ereignis verursachte Schaden steht. Je höher der Schaden aus dieser Formel ist, desto eher sollten Maßnahmen dagegen ergreifen werden. Wie Gefahren erkannt werden können und diese Formel anwendet wird, kann aus der Seminararbeit „Gefährdungsermittlung mit dem IT-Grundschutz-Katalog“ [Sch09] entnommen werden.

Die folgenden Punkte erhalten viele praktischen und anwendbaren Beispiele.

4.1 Hardware einrichten

Der erste wichtige Punkt, um seine Daten zu schützen, ist die Wahl der richtigen Hardware und der richtigen Konfiguration. Diese beiden Punkte werden in den folgenden zwei Unterkapitel besprochen.

4.1.1 Geräteauswahl

Anfang dieses Jahres wurde von Saarbrückener Wissenschaftler bewiesen, dass Nadeldrucker, mit etwas technischen Aufwand, abgehört werden können [Net09] [Win09b]. Gerade in Banken oder Arztpraxen stehen heutzutage noch sehr viele Nadeldrucker und gerade dort muss der Datenschutz besonders gewahrt bleiben.

Daher sollte vor dem Kauf von Hardware über mögliche Gefahren geschaut werden.

Geräte, die kabellos kommunizieren, sind besonders vor Abhören zu schützen oder möglichst komplett auf sie zu verzichten. Kabellose Funk-Mäuse und -Tastaturen übertragen ihre Eingaben unverschlüsselt und sind leicht abzuhören. Damit können Passwörter ausgespäht werden. Andere Kabellose Übertragungstechniken, wie WLAN, können verschlüsselt werden und sollten es auch. Trotz der Verschlüsselung sind WLANs ein attraktives Ziel für potenzielle Angreifer, da das WLAN über eine große Reichweite verfügt und es viele Angriffspunkte gibt. Daher muss bei der Auswahl von WLAN-Geräten neben guten Verschlüsselungstechniken (aktuell gilt WPA2 als sicher) auch auf hohe Sicherheitseinstellungen wie MAC-Filter achtet werden.

Ebenso sollte die Hardware über entsprechende Zugriffsschutzfunktionen verfügen, die, entsprechend der Aufgabe des Gerätes, sehr streng ausfallen kann. Ein Laptop

eines Handelsvertreters mit Kundendaten sollte sehr guten Zugriffsschutz bieten. Denkbar hierfür wäre die Anmeldung mit einer Chipkarte oder einen Fingerabdruckscanner.Das BSI empfehlt auch auf Zugriffsschutzfunktionen von Drucker, Kopierer und Multifunktionsgeräte zu achten und anzuwenden.

Viele Geräte bieten einen Passwortschutz, der auf jeden Fall benutzt werden sollte. Wie das Passwort zu wählen ist, wird in Kapitel 4.3.1 besprochen. Hierfür sollte das Standarddpasswort sofort geändert werden.

4.1.2 Gerätezugriff verhindern

Nachdem die entsprechende Hardware ausgewählt wurde, müssen die entsprechenden Sicherheitsvorkehrungen, welche die Hardware selbst bietet, konfiguriert werden. Das dies nicht immer ausreicht konnte 2001 eine österreichische Telefongesellschaft feststellen, als Hacker ein nicht ausreichendes gesichertes Gateway angegriffen und einen Schaden von 66 Millionen Dollar verursachten [Cha01]. Es sind nicht nur eingebaute Sicherheitsvorkehrungen zu empfehlen, sondern auch durch zusätzliche Vorkehrungen.

So schlägt das BSI vor auf jeden Fall nicht benötigte Hardware und Hardwarebausteine, nach Möglichkeit, komplett auszuschalten oder zu entfernen. Anrufbeantworter sind beispielsweise nur an zuschalten, wenn keine Person in der Nähe ist, um die Zeit des Missbrauchs möglichst gering zu halten. Nicht benötigte Schnittstellen an Telekommunikationsanlagen sind, wenn sie benötigt werden, verschraubt und verplombt zu werden um einen unbefugten Zugriff durch abzuschrecken und, wenn er trotzdem stattfinden sollte, sofort zu bemerken.

Selbst für Faxgeräte gibt es Möglichkeiten den Zugriff auf ankommende Nachrichten zu erschweren. Dazu wird vor dem Fax ein Zusatzgerät montiert, welches die ankommenden Nachrichten faltet und einschweißt. Wenn jemand diese Nachrichten lesen möchte, so muss er erst die Versiegelung brechen und das fällt auf.

Der Hardwarezugriff sollte generell auf das Nötigste beschränkt werden, damit nur geringe Angriffsfläche zu bieten.

4.2 Software-Installation

Nachdem die Hardware soweit gesichert wurde, erfolgt die Installation und Konfiguration der Software durch den Administrator. Die beinhaltet sowohl die Installation von Arbeitsplatz-Rechnern, Mainframes und sonstigen Geräten. Die wich-

tigsten Punkte werden in den folgenden Kapitel erläutert.

4.2.1 Programme abschalten

Es sollten unnötige Programme abgeschaltet oder erst gar nicht installiert werden. Damit soll der Nutzer gar nicht in die Gelegenheit kommen über Programme, bewusst oder unbewusst, Schaden zu verursachen.

Es sollte generell das Prinzip des minimalsten Betriebssystems verfolgt werden, das heißt, das nur die Programme zu installieren sind, die auch wirklich benötigt werden. Nach der Installation eines Betriebssystems sollen, nach BSI, alle nicht benötigten Dienste abgeschaltet und nicht benötigte Programme deinstalliert werden.

Gerade Windows Betriebssysteme sind sehr anfällig gegenüber Manipulation durch Programme. Einige von Mircosoft beworbenen Programmen sollten durch andere alternative Programme ersetzt werden, da viele Attacken durch Viren, Trojanern oder Hackern auf Schwachstellen von den Microsoft-Produkten abzielen, weil sie eine große Verbreitung haben (Siehe Abbildung 3 und 4).

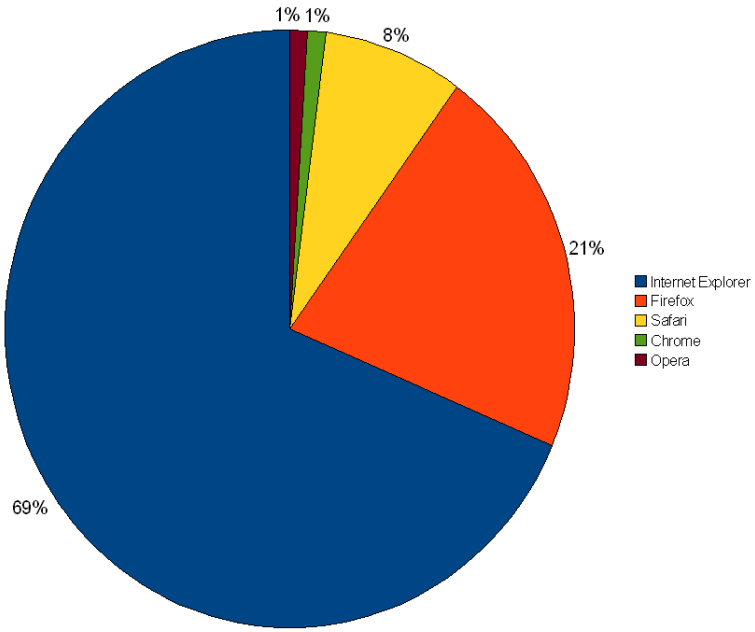

Abbildung 3: Browser Verteilung 2008 [hei09a]

So sollte der Internet Explorer durch Mozilla Firefox oder Opera ersetzt werden und der E-Mail-Client Outlook durch Mozilla Thunderbird oder Lotus Notes. Hierbei ist auch anzumerken, das manche dieser Produkte nicht über den gleichen Funktionsumfang wie das Originalprodukt verfügt.

Top 10 email clients used by business recipients

Email client	Market share
Outlook	36%
Outlook 2003 and earlier	29%
Outlook 2007	7%
Hotmail	33%
Yahoo! Mail	14%
Gmail	6%
Apple Mail	4%
Windows Live Mail (Desktop)	3%
Thunderbird	2.4%
iPhone	1.3%
Lotus Notes	0.2%
AOL Mail	0.1%

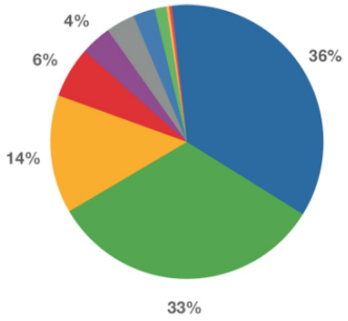

Abbildung 4: E-Mail Client-Verbreitung Sep.2008 [lit09]

4.2.2 Virenschutz

Viren sind kleine Computerprogramme, die erheblichen Schaden verursachen können. Der BSI schätzt den Schaden, der allein in der Bundesrepublik Deutschland durch Viren entstehen, auf eine dreistellige Millionensumme [Bun09b]. Die Schäden können recht unterschiedlich sein, wie die folgenden Auflistung des BSI zeigt:

- Beabsichtigte, programmierte zerstörerische Schadensfunktionen
- Unbeabsichtigte Seiteneffekte bei angeblich harmlosen „Scherz-Viren“
- Inanspruchnahme von Speicherplatz im Hauptspeicher und auf Datenträgern
- Materieller und personeller Aufwand beim Suchen und Entfernen
- Zusätzlich zu ergreifende organisatorische Abwehr-Maßnahmen
- Panik-Reaktionen von Anwendern
- Verunsicherung der Anwender

Windows Betriebssysteme sind auf den meisten Arbeitsplatz-Rechner zu finden, des wegen sind auch die meisten Viren für Windows programmiert. Als Schutz ist daher ein Virenscanner unerlässlich, der permanent im Hintergrund nach Viren scannt. Ein gutes Anti-Viren-Programm sollte nicht nur möglichst viele Viren erkennen sondern auch die Art des Virus, damit der Administrator das Schadenspotenzial abschätzen kann und ihn richtig entfernen kann. Das Anti-Viren-Programm sollte immer auf den aktuellsten Stand sein, das heißt es sollte automatisch Updates mit neuen Viren-Signaturen herunterladen können, um diese zu erkennen.

Dadurch soll verhindert werden, dass der Virus Schaden verursachen kann und er sich nicht im Netzwerk verteilt.

Das reicht nicht aus um das Betriebssystem einigermaßen sicher zu bekommen. Weitere Schritte dafür wären:

- Nutzer darf keine Administrator Rechte verfügen
- bestimmte Dateiformate sollten mit sicheren Programmen geöffnet werden (Siehe Kapitel 4.4.1)
- Regelmäßige Updates von Programmen und Betriebssystem (Siehe Kapitel 4.5.2)
- Überprüfen von neuen Speichergeräten auf Viren
- Überprüfen von neuer Software auf Viren
- Protokollieren und Überwachen von Änderungen von Systemdateien (Siehe Kapitel 4.4.2 und **??**)
- Regelmäßige Integritätsprüfung

Wenn diese Punkte eingehalten werden, dürften die meisten Viren keine Chance haben.

4.2.3 Verschlüsselung

Sensible Daten sollten möglichst verschlüsselt werden. Diese können in einer Datenbank oder einem Arbeitsplatz-Rechner liegen. Besonders bei transportablen Speichergeräten wie Laptops, USB-Platten und andere Speicergeräte, die in diese Kategorie hineinfallen, ist das Risiko diese Daten zu verlieren besonders groß. Wenn dies geschehen sollte, sind die verschlüsselten Daten vor unbefugten Zugriff sicher.

Ein besonders heikler Punkt ist die Kommunikation über das Internet per E-Mail. Viele Firmen wickeln oft wichtige und vertrauenswürdige Details über E-Mail ab, den viele wissen nicht, dass diese Nachrichten im Standard-E-Mail-Format als Klartext übertragen wird. Diese Daten werden über viele Netzwerkknoten verschickt, die alle potenziell Gefährlich sind und diese Nachrichten abfangen können. Hier rät das BSI den Einsatz von Verschlüsselungssoftware wenn

wichtige Daten über das Internet verschickt werden. Hier wird zwischen der bedarfsabhängigen Verschlüsselung auf dem Endgerät und einer automatischen Verschlüsselung durch das Sicherheitsgateway unterschieden. Beide Verfahren haben sowohl Vor- als auch Nachteile, wie aus der Tabelle 5 zu entnehmen ist.

Auf dem Sicherheitsgateway:	Auf den Endgeräten:
• Zentrale Datenprüfung	• Ende-zu-Ende Sicherheit
• Zentrale Schlüsselverteilung	• Keine Protokollprobleme
• Detailliertes Accounting	• benutzerabhängig
• Zugriff vom Sicherheitsgateway auf internes Netz	• Keine Kontrollmöglichkeiten auf dem Sicherheitsgateway
• Keine Ende-zu-Ende-Sicherheit	• Oft werden Public-Key-Infrastrukturen benötigt

Abbildung 5: Vor- und Nachteile der Verschlüsselung über ein Sicherheitsgateway und auf den Endgerät [Bun09a]

Einen ähnlichen Punkt ist die Frage ob eine Online- oder Offline-Verschlüsselung durch den Nutzer erwünscht ist. Bei einer Online Verschlüsselung wird die komplette Festplatte mit dem Betriebssystem verschlüsselt, so dass der Nutzer nur einmal beim Start ein Kennwort eingeben muss. Bei der Offline-Verschlüsselung erfolgt das Verschlüsseln durch den Nutzer selbst, wobei hier nur einzelne Teile verschlüsselt werden. Beim letzten genannten Verfahren besteht die Gefahr, dass das Verschlüsseln sensibler Daten vergessen wird.

4.2.4 Vorhandene Sicherheitsmechanismen anschalten

Viele Betriebssysteme und Programme verfügen über verschiedene Sicherheitsmechanismen, die erst eingeschaltet werden müssen. Dies können Firewalls, Virenscanner (Siehe Kapitel 4.2.2) und automatische Updates (Siehe Kapitel 4.5.2) sein, die vom Betriebssystem zur Verfügung gestellt werden.

Des Weiteren gibt es zahlreiche Mechanismen die zuerst nicht als Sicherheitsmechanismus verstanden werden. Ein Beispiel hierfür ist der Bildschirmschoner des Betriebssystems. Hier empfiehlt das BSI den Bildschirmschoner mit Passworteingabe zu versehen. Dadurch soll unbefugter Zugriff während der Abwesenheit verhindert werden.

4.2.5 Geräte abschalten

Während der Installation sollten nicht benötigte Hardwarebauteile deaktiviert werden, wenn diese nicht ausgebaut werden können. Denn jeder Zugang durch Hardwarekomponenten kann dazu benutzt werdenDaten zu entwenden oder Schadprogramme durch verseuchte Datenträger einzuschleusen.

Am Arbeitsplatz-Rechner wird dringend empfohlen CD- und DVD-Laufwerke abzuschalten, ebenso Speicherkartenleser und USB Ports, wenn sie nicht zur Arbeit benötigt werden. Die beiden zuletzt genannten Anschlüsse gelten als besonders problematisch, da der Benutzer einfach Speichermedien anschließen und damit entweder Daten entwenden oder schädliche Programme einspeisen kann.

Auch sind fest installierte Mikrofone und Webcams zu deaktivieren, da hier die Möglichkeit besteht, dass sie angezapft und somit Gespräche abgehört oder Bilder ab gefilmt werden können. Das dies Möglich ist, wurde mit der Entwicklung des Bundestrojaners bestätigt [Win07].

4.3 Inbetriebnahme

Nachdem die notwendigen Vorkehrungen an der Hardware vorgenommen wurden, kann sie vom endgültigen Nutzer in betrieb genommen werden. Dabei sind einige Punkte zu beachten, die in den folgenden Punkten besprochen werden.

4.3.1 Passwortproblematik

Ein besonders heikler Punkt ist die Wahl eines guten Passwortes. Leider zeigen Studien und Umfragen immer wieder, dass viele Personen zu einfache Passwörter verwenden [net05]. Selbst wichtige Personen wie Barack Obama verwenden schwache Passwörter, die einfach zu raten sind. Er benutzte den Twitter-Microblog-Dienst um über seinen Wahlkampf zu berichten, dessen Passwort dann von Unbekannten erraten wurde. [hei09b]. Passwörter sollten nach folgenden Vorgaben erstellt werden

- keine Wörter, Namen, etc.
- mindestens 8 Zeichen
- gute Mischung aus Groß- und Klein-Buchstaben, Zahlen und Sonderzeichen

Diese Passwörter gelten als sicher. Das beste Passwort ist wirkungslos, wenn es nicht sicher bewahrt wird.Hierbei sollte das Passwort in einem Umschlag versiegelt und dann versteckt werden, besser ist es jedoch, wenn es nirgends Notiert wird. Niemals sollte das Passwort elektronisch abgespeichert werden.

Darüber hinaus sollten die Passwörter spätestens alle 90 Tage geändert werden. Um es durchzusetzen kann die Dauer eines Passwortes auf 90 Tage begrenzt werden. Dadurch muss der Nutzer ein neues Passwörter eingeben.

Generell ist hierbei die Frage aufzuwerfen in wie weit die Passwortproblematik in den Griff zu bekommen ist. Überall muss ein Nutzer sich Passwörter merken, so dass schnell der Überblick verloren geht. Die Firma könnte ihre Mitarbeiter entlasten, indem Biometrische Zugangskontrollen oder ein Zugriff über Chipkarten realisiert werden.

4.3.2 Zugriffsschutz

Die Software sollte immer über einen guten Schutz gegen unerlaubte Zugriffe bieten, das heißt dass niemand ohne die erforderliche Berechtigung zugang zu diesem System erhält. Der Zugang zu den entsprechenden Systemen ist entweder durch sytemeigene Methoden oder durch fremde Software-Lösungen zu gewährleisten.

Ein Punkt, der immer wieder problematisch ist, ist der Zugriff auf das WLAN. So sind etwa 30% aller WLANs in Deutschland ungesichert, da kein ausreichender Zugriffsschutz bestrieben wird [CM09].

4.4 Laufender Betrieb

Nachdem die vorbereitenden Maßnahmen getroffen wurden erfolgen Maßnahmen, die während des Laufenden Betriebes beachtet werden sollten.

4.4.1 Dateiformate

Die Nutzer der Arbeitsplatz-Rechner sollten darauf aufmerksam gemacht werden, das viele Viren und sonstige unerwünschte Schädlinge über bestimmte Dateiformate auf die Rechner kommen. Sie nutzen dazu Schwachstellen von den jeweiligen Programm, mit dem diese Datei geöffnet wird. Im Jahre 2008 wurden etwa 35% aller Angriffe über Dateiformate von Microsoft Office [**?**] getätigt, während im ersten Halbjahr 2009 mit knapp 50% die Hauptangriffsquelle der Adobe Reader

war [Win09a].
Als nahezu ungefährlich gelten nach BSI folgende Dateien:

- Textdateien (.TXT)
- JPEG-Bilddateien (.JPG, .JPEG)
- GIF-Bilddateien (.GIF)

Besonders sollte der Nutzer auf folgende Dateiformate sensibilisiert werden, da sie sehr häufig Überträger von schädlichen Programmcode sind:

- HTML (.HTML) auch in E-Mail
- MS Office (.DOC, .XLS, .PPT, .SDW, .SXW usw.)
- ausführbaren Programme (wie .COM, .EXE, .PIF)
- Skript-Sprachen (.VBS, .JS, .BAT, Perl- oder Shellskripte)
- Registrierungsdateien (.REG)
- Bildschirmschoner (.SCR)
- Portable Document Format (.PDF)

Dateien mit diesen Endungen sollten niemals geöffnet werden wenn sie von unbekannter Quelle stammen. Auch wenn diese Dateien von bekannten Quellen stammt besteht immer ein Restrisiko und sollte nur mit Vorsicht geöffnet werden. Dieses Risiko kann minimiert werden, indem diese Dateien mit Programmen geöffnet werden, die nicht über die bekannten Schwachstellen verfügen. So wären MS-Office Dateien mit einem alternativen Office Programm wie Open Office zu öffnen. Skript-Sprachen oder Registrierungsdateien mit einem normalen Texteditor und PDF-Dateien mit einem anderen pdf-Reader wie Foxit Reader. Vorsicht ist auch bei gepackten Dateien (.ZIP, .RAR, .7ZIP) geboten, denn sie können auch diese gefährlichen Dateien enthalten.

4.4.2 Protokollierung und Überwachen

Um mögliche Fremdeinwirkung auf den Rechner oder sonstiger Hardware zu bemerken, sollen, nach Möglichkeit, Hard- und Software eigene Protokollierungmethoden angeschaltet werden. Diese Protokolle sollen dem Administrator ermöglichen

schädliche Modifikationen an Systemdateien zu erkennen, diese rückgängig zu machen und vielleicht den Urheber ausfindig zu machen. Falls es keine systemeigenen Protokolle zur Verfügung stehen, sollte diese nachträglich über Fremdsoftware nachgerüstet werden.

Bei all diesen Möglichkeiten ist sicher zu stellen, das diese Protokollierung und Überwachung nicht gegen die aktuellen Datenschutzbestimmungen verstößt.

4.4.3 Konsistenz prüfen

Um einen reibungslosen Arbeitsablauf zu gewährleisten sollen gelegentlich alle Daten in der Systemverwaltung und der Firmendatenbank auf Konsistenz geprüft werden. Dies kann automatisch durch Tools, aber auch manuell durch den Administrator geschehen. Bei dieser Vorgehensweise sind alle Daten auf Widerspruchsfreiheit zu überprüfen.

4.5 Wartung

Alle Hard- und Software sind durch regelmäßige Tests zu überprüfen und durch Updates auf den neusten Stand zu halten.

4.5.1 Testen

Hard- und Software sind sowohl vor dem eigentlichen Gebrauch als auch während des Betriebes auf funktionstüchtigkeit zu überprüfen. Als besonders anfällig erweisen sich Speichermedien aller Art. Viele Totalausfälle machen sich oft schon durch kleine Fehler im voraus bemerkbar, die durch den Nutzer oft nicht bemerkbar sind. Sie kann erst durch Spezialsoftware des Administrators entdeckt werden. Um einen Totalverlust vorzubeugen sind regelmäßige Sicherungen unerlässlich (Siehe Kapitel 4.6). Ebenso kann es passieren, das durch Hard- oder Softwarefehler der Nutzer Rechte bekommt, die er nicht besitzen dürfte. Auch dies ist durch regelmäßige Tests zu überprüfen.

4.5.2 Updates

Jede Sicherheitslücke in Hard- und Software sollte möglichst schnell geschlossen werden. Dies geschieht über Updates, die der Hersteller zur Verfügung stellt. Oh-

ne diese Updates bleiben Lücken, die von Angreifern benutzt werden können. Die Software verfügt meist über ein automatisches Update-Programm, das aktiviert werden sollte. Hierbei kann es vorkommen, dass das Programm eine Administrator-Freigabe benötigt, darauf sollte der Administrator achten.

Der Administrator sollte gelegentlich nach Firmware-Updates schauen, da es Viren geben kann, die die Hardware befallen und schädigen können [boo06]. Bei Hardware gibt es leider keine automatisierten Updates, so muss jeder Aktualisierung von Administrator vorgenommen werden.

4.6 Archivierung

Es sollten regelmäßige Datensicherungen vorgenommen werden und an einem anderen Ort archiviert werden. Denn falls der schlimmste Fall eintreten sollte und die originalen Daten vernichtet werden, so können sie bei Ordnungsgemäßer Archivierung wiederhergestellt werden.

Es reicht nicht aus, alles zu archivieren, wenn nicht einige Punkte beachtet werden. So wurden früher in der DDR sehr viele Daten gespeichert, die heute nicht mehr bearbeitet werden können. Das Problem hierbei liegt bei inkompatiblen Datenträgern zu heutigen Technik und nicht genormte Dateiformate [Obe08].

4.6.1 Dateiformat

Damit archivierte Daten möglichst lange gelesen und verarbeitet werden können, sollte auf Standardisierte Dateiformate gesetzten werden. Um Texte und Dokumente richtig zu speichern, soll fast ausschließlich auf auf ASCII-Formate wie SGML und XML gesetzt werden. Nur wenn auch das Layout mit gespeichert werden soll, so empfiehlt das BSI die Speicherung im PDF-Format.

Falls Bilder unterschiedlicher Art archiviert werden soll, so soll auch hier auf Standardformate wie JPEG, GIFF oder TIFF verwendet werden.

Audio- und Videodateien sollen als MPEG, ITU H.261 oder ITU H.263 gespeichert werden.

4.6.2 Medien

Ebenso wichtig wie das Dateiformat ist die Wahl des richtigen Speichermediums. Diese können je nach Verwendung des Archives unterschiedliche ausfallen. So sind

Fragen wie der Umfang der Archivierung (1 Gigabyte oder 10 Terrabyte), der Zugriff auf die Archivierungsdaten (Einzelzugriff oder Komplettsicherung), wie lange Archiviert werden soll (1 Woche oder 10 Jahre) und ob die Daten nicht überschrieben werden dürfen (revisionssicher).

Bei allen Medien ist zu beachten, das sie alle anfällig gegen physikalischen Beschädigungen wie Feuer, Wasser oder Sabotage sind. Insgesamt gibt es drei wichtige Techniken um Daten zu speichern.

Digitale magnetische Systeme :

Bei Digitalen magnetischen Systemen wird durch lokale Veränderung des Magnetfeldes auf dem Speichermedium der Speichereffekt erzielt. Die Speichermedium dafür Disketten, Festplatten und Magnetbänder. Laut BSI sind diese Medien für kurz- bis mittelfristige Speicherdauer geeignet. Die Daten darauf sind allerdings nicht vor Veränderungen geschützt, also nicht revisionssicher.

Besonders anfällig sind diese Speichermedien gegen Magnetfelder (Siehe Kapitel 4.8).

Digitale optische Systeme :

Bei diesem Speichermedium wird der Speichereffekt durch eine oberflächliche Veränderung der Struktur erzielt. Mit einem Laser können diese Veränderungen (Pits) gelesen werden. Hierunter fallen CDs, CD-Rohlinge, DVDs, DVD+R, DVD-R oder DVD-RW. Auch hier sind die Daten nur kurz- bis mittelfristig gesichert. Einige dieser Medien können revisionssicher gespeichert werden (CD-Rohling, DVD+R, DVD-R), andere allerdings nicht (CD-RW, DVD-RW, DVD-RAM).

Anfällig sind die Medien durch Kratzer auf der optischen Datenfläche (Siehe Kapitel 4.8).

Magneto-Optische Systeme :

Magneto-Optische Systeme sind ein Medium, die durch Veränderung des lokalen Magnetfeldes die Daten schreibt, aber durch eine Optik die Daten ließt. Die Datenträger besitzen zwei Schichten: die erste ist die magnetische Schicht und die zweite eine optische Schicht. Bei Schreiben wird das Magnetfeld der ersten Schicht so verändert, dass ein Laserstrahl sie durchdringen kann. An Stellen, an denen das nicht geschehen ist, wir der Laser nicht reflektiert. Dadurch können ebenfalls Daten gespeichert werden.

Die Lebensdauer dieser Medien wird mit bis zu 30 Jahren angegeben und manche Medien sind auch revisionssicher, aber leider hat der letzte große Hersteller Fujitsu den Verkauf von MO-Laufwerken schon 2007 eingestellt [Wik09], so dass dieses Medium, trotz seiner guten Archivierungseigenschaften, nicht weiter zu empfehlen ist.

4.6.3 Regelmäßige Tests

Speichermedien können kaputt gehen oder durch physikalische Gesetze ihre Speichereigenschaften verlieren. Daher ist es unerlässlich sie regelmäßig auf ihre Funktionalität zu überprüfen. Das BSI empfiehlt die Medien jedes Jahr mindestens einmal auf Datenverlust oder beginnende Defekte zu überprüfen, damit möglichst viele Daten von diesem Medium gerettet werden können.

4.7 Daten löschen

Wie Stichproben immer wieder zeigen, werden Speichermedien nach Gebrauch nur unzureichend gelöscht. Gerade in Firmen oder Behörden, in denen eigentlich besonderer Datenschutz gewährleistet sein müsste, werden Speichermedien verkauft, ohne das diese richtig gelöscht werden [hei08].

Die Speichermedien werden gelöscht, indem auf den Speicherplatz zufällige Werte geschrieben werden. Dieser Vorgang sollte mindestens zwei Mal wiederholt werden, damit eventuelle Datenstücke auch wirklich gelöscht werden. Dieses „Sichere Löschen“ kann nur mit Fremdprogrammen erreicht werden, selbst durch Formatieren werden nur die Verweise auf die Speicherorte von der Festplatte gelöscht, aber nicht die Daten selbst. Sie können mit speziellen Programmen wiederhergestellt werden.

4.8 Hardware entsorgen

Der letzte Punkt ist das Entsorgen nicht mehr benötigter Hardware. Vor allem Speichermedien sollten sorgfältig entsorgt werden, da darauf wichtige Daten sein können.

Hierbei sind zum einen die Digitalen magnetische Systeme (Siehe Kapitel 4.6.2) zu nennen. Falls der Datenträger noch funktioniert, kann er mit „Sicheren Löschen“ (Siehe Kapitel 4.7) unleserlich gemacht werden. Ist kein Zugriff auf den Daten-

träger mehr möglich, kann nur noch ein starkes Magnetfeld diese Daten löschen. Das ist nötig, da spezialisierte Firmen den Datenträger öffnen können, und diese Daten auslesen können.

Bei Digitale optische Systeme ist der Fall leichter, da hier nur der Datenträger in kleine Teile zerbrochen werden muss. Um sich vor Verletzungen zu schützen, ist ein moderner Aktenvernichter mit eingebauter CD-Schredder-Einheit zu empfehlen.

Magneto-Optische Speichermedien können auf mehrere Arten gelöscht werden. Entweder durch „Sicheren Löschen“, wenn es sich um eine wieder beschreibbares Medium handelt. Ansonsten kann ein starkes Magnetfeld oder die Zerstörung der optische Oberfläche durch den Aktenvernichter die Daten restlos vernichten.

Eine Sonderstellung sind die modernen Flash-Speicher-Karten wie SD-Karten oder Solid State Drive. Hierbei werden die Daten nicht mehr auf Scheiben gespeichert, sondern in Mikrochips, die selbst nach dem Ausschalten die Daten behalten. Hier sollte versucht werden den Speicher mit „Sicheren Löschen“ zu überschreiben. Wenn die Medien kaputt sind, so kann höchstens Feuer oder eine Mikrowelle, den kleinen Mikrochip mit den Daten zerstören.

5 Validierung

Um die Wirksamkeit und die Effizienz der Maßnahmen zu überprüfen, ist es ratsam diese in der Praxis durch Simulationen oder Praxistests zu validieren. Darüber hinaus soll durch die Validierung weitere Faktoren überprüft werden [Ker08]:

- Kosten der Maßnahme (externe und interne Kosten)
- Akzeptanz der Maßnahme bei den Nutzern
- Praktikabilität
- Angemessenheit im Vergleich zu den Geschäftsrisiken, die sie mindern soll

Vor dem Beginn der Validierung sollten folgende Punkte feststehen:

- Auswahl der Maßnahmen
- Art der Validierung (Simulation oder Test)
- Kennzahlen festlegen
- Rahmen (Szenario, Beteiligte, Zeitdauer)
- Verantwortlicher für die Durchführung festlegen
- Verantwortlicher für die Auswertung bestimmen

Wenn über die gewünschte Maßnahme noch keinerlei Erfahrungen existieren, so kann sie durch Praxistests erhalten. Zur Unterstützung der Auswertung ist es hilfreich sich Kennzahlen zu überlegen die Aussagen über das Ziel liefern können. Diese Kennzahlen sollten aussagekräftig und eindeutig sein. Für die anschließende Beobachtung in der Testphase sollten die vorher festgelegten Kennzahlen gemessen werden, damit später die Wirksamkeit überprüft werden kann. Der Beobachtungszeitraum sollte nur in absoluten Ausnahmefällen sechs Monate dauern. Im Normalfall ist eine deutlich kürzere Beobachtungsphasen erstrebenswert. Abhängig von der Validierung kann eine Maßnahme eingeführt, überarbeitet oder abgelehnt werden.

5.1 Beispiel

Um den Ablauf einer Validierung zu verdeutlichen, wird es an einem Beispiel gezeigt:

Durch Anmietung von Büroräumen zu denen auch weitere Mieter Zugang haben; kommt es zu einem Diebstahl eines Servers. Die Daten auf dem Server sind durch sichere Algorithmen verschlüsselt, externe Backups der Daten sind vorhanden. Um einen weiteren Diebstahl zu verhindern sollen geeignete Maßnahmen ergriffen werden, damit das nicht mehr geschehen kann.

1. Auswahl der Maßnahmen Als Maßnahme sollen die Server durch einen abschließbaren, im Boden verankerten Käfig gesichert werden. Als Schloss soll ein Biometrisches Zugangssystem dienen.

2. Art der Validierung Simulation

3. Kennzahlen festlegen Kosten $<$ 100.000 Euro, Zustimmung des Vermieters, Sicherheit = 24 Stunden

4. Rahmen (Szenario, Beteiligte, Zeitdauer) Preiskalkulation, Anfrage

Der Käfig sorgt dafür, das der Server nicht mehr gestohlen werden kann, wenn die Tür verschlossen bleibt oder sie nicht aufgebrochen wird. Durch den Käfig ist auch ein 24-Stunden-Schutz gewährleistet. Wenn der Vermieter zustimmt, dass die Firma den Käfig um den Server bauen darf, und die Kosten unter 100.000 Euro liegen, so wäre die Maßnahme anzuwenden, wenn es keine bessere Maßnahme zutrifft.

6 Fazit

Der gesamte IT-Grundschutz-Katalog des BSI bietet eine sehr gute Hilfestellung dabei das Unternehmen sicherer zu machen und dadurch nicht nur sich, sondern auch Andere zu schützen. Dabei hilft das BSI zum einen durch die Onlinekataloge, aber auch durch zahlreiche Dokumente, wie Checklisten, um Gefahren zu erfassen, an die ansonsten nicht gedacht worden wäre. Ebenso bietet das BSI Kurse an, um Personen für Gefahren zu sensibilisieren, oder Programme wie GTools um eine rechnergestützte Umsetzung des BSI IT-Grundschutz-Kataloges zu ermöglichen.

Dies ist aber leider etwas zu relativieren, weil vor allem die Katalog an manchen Stellen nicht mehr aktuell sind, so wird Windows Vista wird nicht besprochen, obwohl es seit 2007 auf dem Markt ist, oder Magneto-Optische Speichermedien werden besprochen, die Produktion ist seit 2007 eingestellt worden. Ebenso bieten manche Hinweise zu wenig Informationen, so soll eine WLAN-Verbindung verschlüsselt werden, aber es gibt keinerlei Hinweise mit welchen Algorithmus dies geschehen sollte Hier sind weitere Recherchen außerhalb des IT-Grundschutz-Kataloges des BSI notwendig.

Die Umsetzung des Kataloges nützt nicht nur dem eigenen Unternehmen, sondern auch seinen Kunden und Lieferanten, da mögliche Gefahren schon möglichst früh vermieden werden. Das kann auch durch einen Auditor vom BSI testiert werden, wenn mehr als 55% der Maßnahmen umgesetzt worden sind. Dadurch erhält das Unternehmen ein Zertifikat für zwei Jahre.

Es sollte versucht werden möglichst viele Maßnahmen umzusetzen. Viele vom BSI vorgestellten Maßnahmen sind kostenlos, da sie durch Organisation, durch das Personal und durch eingebaute Maßnahmen in der Hard- und Software, einfach realisiert werden können. Der einzigste Kostenfaktor der anfällt ist die Arbeitszeit des

Besonders wichtig ist es, dass das Personal über die Gefahren aufgeklärt wird und die Maßnahmen einhält. Regelmäßige Kontrollen, das dies geschieht, sind daher unumgänglich.

Anhang

A Nach Maßnahmen geordnet

Auf den folgenden Seiten werden die Maßnahmen nach der entsprechenden Problematik geordnet wiedergegeben. Hierbei wurde keine Unterscheidung getroffen ob es sich dabei um Hardware oder um Software handelt, diese Einteilung wird in Anhang B vorgenommen.

Problemtaik	Maßnahme im Maßnahmenkatalog
Absichern gegen Abhören	39, 40, 89, 254
Administration	80, 204, 230, 236, 287, 288
Archivierung	168, 169, 170, 171, 172. 173
Dateiformate	199
Daten löschen	17, 28, 32, 56, 64, 234
Datenkonsistenz	68, 235
Filtern von Inhalten	62, 98, 238
Gerätenutzung einschränken	52, 57, 59, 60
Installation (dieser Teil ist sehr Produkt spezifisch) (mehr dazu in Anhang B)	55, 78, 82, 83, 91, 105, 109, 116, 126 127, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 161, 162, 153, 164, 165, 166, 167, 174, 175, 201, 202, 203, 204, 207, 208, 209, 210, 211, 212, 223, 224, 225, 229, 230, 231, 248, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 277, 278, 279, 280, 281, 282, 283, 284, 307, 308, 309, 310, 311
Passwortproblematik	1, 10, 14, 27, 46, 306
nicht benötigte Programme abschalten	12, 38, 95, 96, 184, 186, 187, 190, 285, 322
Protokollierung	5, 25, 47, 54, 81, 106, 172, 205, 270, 292
nutzen fremder Rechner	251

Problemtaik	Maßnahme im Maßnahmenkatalog
vorhandene Sicherheitsmechanismen nutzen	61, 84, 102, 107, 114, 117, 130, 206, 244, 246, 247
Speichersysteme	232, 274
Testen	65, 69, 173, 240
Überwachen von Programmen	70, 132, 148, 160, 182, 312, 316
Updates	83, 249, 324, 323
Verschlüsselung	29, 34, 72, 85, 86, 87, 88, 90, 101, 131
Virenschutz	3, 33, 44, 226, 253, 271
Zugriffsschutz	58, 67, 75, 77, 79, 80, 94, 98, 99, 100, 113, 120, 121, 124, 125, 133, 135, 149, 185, 188, 189, 190, 200, 213, 216, 219, 232, 242, 286, 299, 303, 319, 320, 321

B Massnahmen Nach Produkt geordnet

In diesem Teil des Anhangs werden die Maßnahmen nach der angesprochenen Hardware und Software geordnet.

Hardware	Maßnahme im Maßnahmenkatalog
Drucker	299, 300, 301, 302, 303, 304
Domänen-Controller	138, 313, 314
Fax	36, 37, 43
Handy	114, 115
Laptop	27, 28, 29, 235, 236
PC	151, 152,
PDA	228, 229, 230, 231
Router/Switches	60, 201, 202, 203, 204, 205
Scanner	303
Server	39, 103, 113, 239, 240
Tastatur	254
USB-Geräte	200
WLAN	295, 296, 297, 298
Zusatzspeicher	200, 232

Software	Maßnahme im Maßnahmenkatalog
Apache	191, 192, 193, 194, 195, 196, 197, 198
Exchange/Outlook 2000	161, 162, 163, 164, 165, 166, 167
Linux für zSeries	212
Lotus Notes	116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132
Novell 4.11	102
Novell eDirectory	153, 154, 155, 156, 157, 158, 159, 160
Outlook 2000	siehe Exchange
SAP	256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273
UNIX	
VoIP-Programme	287, 288, 289, 290, 291, 292
Virenschutzprogramme	3, 33, 226, 271
Windows 95	46, 58, 74,
Windows NT	48, 49, 50, 51, 52, 53, 54, 55, 75, 76, 77, 174, 175, 283
Windows 2000	136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 174, 175, 283
Windows XP	49, 52, 75, 146, 147, 148, 149, 243, 244, 245, 244, 245, 246, 247, 248, 249
Windows Vista	-
Web (IIS)	174, 175, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 282,
Z/OS	207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221

Abbildungsverzeichnis

Literatur

[boo06] BOOTSEKTORBLOG.DE: *Erster Hardware-Virus entdeckt*. Website, 2006. Online verfügbar unter `http://www.bootsektorblog.de/2006/02/erster_hardware.html`; besucht am 27. Juni 2009.

[Bun09a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Bundesamt für Sicherheit in der Informationstechnik*. Website, 2009. Online verfügbar unter `http://www.bsi.de/`; besucht am 12. Mai 2009.

[Bun09b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Computer-Viren Definition und Wirkungsweise*. Website, 2009. Online verfügbar unter `http://www.bsi.bund.de/literat/faltbl/F19Kurzviren.htm`; besucht am 20. Juni 2009.

[Cha01] CHANNELPARTNER: *Millionenschaden durch Telefon-Hack*. Website, 2001. Online verfügbar unter `http://www.channelpartner.de/news/218216/index.html`; besucht am 18. Juni 2009.

[Cha09a] CHAOS COMPUTER CLUB E.V.: *Chaos Computer Club*. Website, 2009. Online verfügbar unter `http://www.ccc.de/`; besucht am 12. Mai 2009.

[Cha09b] CHAOS COMPUTER CLUB E.V.: *Chaos Computer Club*. Website, 2009. Online verfügbar unter `http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml`; besucht am 12. Mai 2009.

[CM09] CALL-MAGAZIN: *BSI bezeichnet Lage der IT-Sicherheit als "katastrophal"*. Website, 2009. Online verfügbar unter `http://www.call-magazin.de/internetzugang-isdn-modem/internet-nachrichten/bsi-bezeichnet-lage-der-it-sicherheit-als-katastrophal_25370.html`; besucht am 17. Juni 2009.

[hei08] HEISE: *Erneut Festplatte mit Daten britischer Bürger verkauft*. Website, 2008. Online verfügbar unter `http://www.heise.de/newsticker/Erneut-Festplatte-mit-Daten-britischer-Buerger-verkauft--/meldung/115021`; besucht am 17. Juni 2009.

[hei09a] HEISE: *Firefox auf dem Vormarsch*. Website, 2009. Online verfügbar unter `http://www.heise.de/open/Firefox-auf-dem-Vormarsch--/news/meldung/121652`; besucht am 20. Juni 2009.

[hei09b] HEISE: *Lehren aus dem Twitter-Hack*. Website, 2009. Online verfügbar unter http://www.heise.de/security/Lehren-aus-dem-Twitter-Hack--/news/meldung/121286; besucht am 17. Juni 2009.

[Hof71] HOFFMAN, ABBIE: *Steal This Book*. Penguin Classics, 1971. ISBN 978-0143105336.

[Ker08] KERSTEN, HEINRICH; REUTER, JÜRGEN; SCHRÖDER, KLAUS-WERNER: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*. Vieweg+Teubner, 2008. ISBN 978-3834801784.

[lit09] LITMUSAPP: *Email client market share*. Report, 2009. Online verfügbar unter http://litmusapp.com/email-client-stats/email-stats-report.pdf; besucht am 20. Juni 2009.

[net05] NETZEITUNG: *Viele Menschen wählen zu einfache Passwörter*. Website, 2005. Online verfügbar unter http://www.netzeitung.de/internet/349393.html; besucht am 17. Juni 2009.

[Net09] NETZWELT: *Datenschutz: Nadeldrucker können abgehört werden*. Website, 2009. Online verfügbar unter http://www.netzwelt.de/news/79984-datenschutz-nadeldrucker-abgehoert.html; besucht am 20. Juni 2009.

[Obe08] OBERHACK, SILVIA: *Die Stasi hatte nicht nur Papier!* Text, 2008. Online verfügbar unter http://www.bstu.bund.de/cln_012/nn_1028968/DE/Archiv/Aktuelles/texte/08-10-20__unesco__tag__ipn__pdf,templateId=raw,property=publicationFile.pdf/08-10-20_unesco_tag_ipn_pdf.pdf; besucht am 17. Juni 2009.

[Sch09] SCHULTHEISS, MARTIN: *Gefährdungsermittlung mit dem IT-Grundschutz-Katalog*. Seminararbeit, 2009.

[Wik09] WIKIPEDIA.DE: *Magneto Optical Disk*. Website, 2009. Online verfügbar unter http://de.wikipedia.org/wiki/Magneto_Optical_Disk#Verbreitung; besucht am 28. Juni 2009.

[Win07] WINFUTURE.DE: *IT-Branche spricht sich gegen Bundestrojaner aus*. Website, 2007. Online verfügbar unter http://winfuture.de/news,30711.html; besucht am 27. Juni 2009.

[Win09a] WINFUTURE: *F-Secure rät Anwendern vom Adobe Reader ab.* Website, 2009. Online verfügbar unter `http://winfuture.de/news,46666.html`; besucht am 17. Juni 2009.

[Win09b] WINFUTURE: *Sicherheitsrisiko: Nadeldrucker in Praxen & Banken.* Website, 2009. Online verfügbar unter `http://winfuture.de/news,47467.html`; besucht am 20. Juni 2009.