Bundesamt
für Sicherheit in der
Informationstechnik

Ein IT-Grundschutzprofil für eine kleine Institution

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Referat I.1.4 Systemsicherheit, Grundschutz
Postfach 200363
53133 Bonn
Tel:+49 (0) 1888-95820
E-Mail: gshb@bsi.bund.de
Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Hatten Sie schon einmal Probleme mit Computer-Viren?

Sind auf Ihren Rechnern vertrauliche oder personenbezogene Kunden-, Mandanten- oder Patientendaten gespeichert?

Sind Ihnen schon einmal Daten unwiederbringlich verloren gegangen? Haben Sie oder Ihre Mitarbeiter im Büro einen Internetzugang?

Sofern Sie eine der Fragen mit „Ja“ beantwortet haben, sollten Sie sich mit dem Thema Datensicherheit beschäftigen. In der heutigen Informationsgesellschaft unterstützen Computer nahezu alle Arbeitsbereiche. In den Büros von Handwerksbetrieben, Arztpraxen, Anwaltskanzleien oder Steuerberatern werden Computer und weitere Informationstechnologie (abgekürzt mit IT) eingesetzt. Hierbei werden oft sehr sensible Unternehmensdaten verarbeitet, die geschützt werden müssen.

Der Leitfaden IT-Sicherheit [LEITFADEN] vermittelt einen ersten Einstieg in die 50 wichtigsten Standard-Sicherheits-Maßnahmen. Eine Zusammenstellung von gesetzlichen Regelungen mit Bezug zur IT-Sicherheit, ein umfangreiches Glossar mit den wichtigsten Fachbegriffen sowie Darstellung von typischen Fehlern motivieren, das Thema IT-Sicherheit systematisch anzugehen.

In diesem Dokument wird Ihnen ein Beispiel gegeben, wie Sie in Ihrer Institution systematisch eine IT-Sicherheitskonzeption erstellen können. Sie werden mit konkreten Sicherheitsaspekten vertraut gemacht, die beim Einsatz von Informationstechnologie in einer kleinen Institution zu beachten sind. Ausgehend von einer beispielhaft dargestellten Institution mit wenigen Mitarbeitern wird gezeigt, wie Sie die jeweiligen Arbeitsschritte der IT-Grundschutz-Methodik angemessen anwenden können.

Typische kleine Institutionen sind z. B. Arztpraxen, Rechtsanwaltskanzleien, Steuerberater, kleinere Handwerksbetriebe, kleinere Behörden, Ämter, Reisebüros oder Hotels. In diesen Bereichen ist der Arbeitsbetrieb ohne Computer, Netzwerke und Internetzugang heutzutage kaum noch vorstellbar.

Das IT-Grundschutzhandbuch

Das IT-Grundschutzhandbuch (abgekürzt mit GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschreibt eine systematische Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten und enthält Standard-Sicherheitsmaßnahmen aus dem Bereich Organisation, Personal, Infrastruktur und Technik. Der vom GSHB verfolgte Best-Practice-Ansatz hat sich als Standardwerk zur IT-Sicherheit etabliert.

Zur Illustration verschiedener Risiken im Umgang mit IT und zur Beschreibung möglicher Gegenmaßnahmen wird uns im vorliegenden Dokument beispielhaft Herr Anders begleiten.

Die Beispiele werden im nachfolgenden Text optisch durch einen grauen Hintergrund und eine Umrandung hervorgehoben.

Herr Anders führt einen kleinen Familienbetrieb mit 3 Angestellten. Zu den Angestellten zählt Frau Bauer (eine Sekretariatskraft), die halbtags arbeitet und zwei Außendienstmitarbeiter, die den ganzen Tag vor Ort bei den Kunden des Familienbetriebs beschäftigt sind. Herr Anders selbst ist für die Akquisition der Kunden verantwortlich. Während der Ausführung der Arbeiten betreut er seine Kundschaft und kümmert sich um kleinere Details und kurzfristig von den Kunden geäußerte Sonderwünsche.

Die Kunden schätzen diesen Service und empfehlen den kleinen Betrieb gerne an Bekannte und Verwandte weiter. Ein guter Ruf ist für den Betrieb daher sehr wichtig und sichert langfristig die Kundschaft.

Herr Anders hat nach eigener Aussage keine Ahnung von Computern, obwohl er im Betrieb PCs und einen Laptop vielfältig einsetzt: das Führen der Kundenkartei, die Erstellung von Angeboten, das Schreiben der Rechnungen oder die elektronische Kontoführung über das Internet sind nur wenige Beispiele für den Einsatz von Computern in dem kleinen Betrieb.

Frau Anders hat sich in den Umgang mit PC und Netzwerk etwas eingearbeitet und hierfür einen Kurs in der Volkshochschule besucht. Sie hilft zeitweise im Betrieb aus und übernimmt insbesondere die Wartung und Pflege der PCs.

Im vorliegenden Dokument sind Merksätze und Handlungsanweisungen enthalten. Diese sind durch einen doppelt umrandeten Kasten gekennzeichnet.

Referenzen auf andere Dokumente werden mit einem Kürzel in eckigen Klammern (z. B. [ITGSHB]) angegeben. In Anhang B findet man mit dieser Bezeichnung dann den ausführlichen Literaturhinweis.

2 Rahmenbedingung des IT-Grundschutzprofils für einen kleinen IT-Verbund

2.1 Erläuterung zum Schutzbedarf

Wie wichtig sind Ihnen Ihre Kundendaten?

Wie lange können Sie problemlos arbeiten, wenn Ihr Computer ausfällt, die Festplatte nicht mehr lesbar oder Ihr Internetzugang/Telefonanschluss nicht nutzbar ist?

Wissen Sie, welche Daten innerhalb Ihrer Institution so bedeutend sind, dass ihr Verlust oder deren Offenbarung einen Verstoß gegen ein Gesetz, einen Vertrag oder eine Vorschrift bedeutet?

Wenn Sie sich mit IT-Grundschutz beschäftigen, müssen Sie diese wichtigen Fragen zunächst für sich beantworten.

Herr Anders hat in seiner Kundenkartei auf dem PC nicht nur alle Vorgänge von ausgeführten Aufträgen gespeichert, sondern auch vertrauliche Informationen, die ihm bei der Erstellung neuer Angebote nützlich sein können.

Herr Campe, ein nicht ganz so erfolgreicher Konkurrent von Herrn Anders, möchte zu gern hinter dessen Geheimnisse kommen. Zu diesem Zweck lässt er von einem befreundeten Informatik-Studenten ein Schadensprogramm erstellen, welches er an ein harmloses kleines Computerspiel anhängt. Dieses so modifizierte Computerspiel spielt er Frau Bauer zu. Das Schadensprogramm nutzt Schwächen des Betriebssystems von PCs aus, um Zugriffe auf deren Festplatten über das Internet zu ermöglichen.

Nachdem Frau Bauer das Spiel aufgerufen hat, setzt es das Schadensprogramm frei. Dieses öffnet eine Hintertür in den Computern und ermöglicht es Herrn Campe, über das Internet auf die Computer von Herrn Anders zuzugreifen.

Da Frau Anders die Betriebssysteme und die vorhandenen Schutzprogramme der Computer (Virenscanner, Firewall, etc.) längere Zeit nicht aktualisiert hat, kann sich das Schadensprogramm ausbreiten. Herrn Campe wird es hierdurch ermöglicht, auf die Festplatten und somit auf die Daten von Herrn Anders zuzugreifen.

Unter den Daten findet Herr Campe auch die Vorbereitungsunterlagen für eine Ausschreibung, an der er sich ebenfalls beteiligen will. Herr Campe kann anhand der Daten die Kalkulation von Herrn Anders nachvollziehen. So ist er in der Lage, ein vergleichbares Angebot zu einem geringeren Preis anzubieten.

In diesem Beispiel wurde der Grundwert der „Vertraulichkeit“ verletzt.

Vertraulichkeit besagt, dass Daten nur von berechtigten Personen **gelesen** werden dürfen. Herr Campe konnte auf interne Informationen von Herrn Anders zugreifen, somit ist die Vertraulichkeit verletzt worden.

Zusätzlich zur Vertraulichkeit sind auch die Grundwerte „Integrität“ und „Verfügbarkeit“ von Bedeutung.

Unter **Integrität** von Daten versteht man die Tatsache, dass Daten nur von Befugten in beabsichtigter Weise verändert und z. B. von Unbefugten nicht modifiziert werden können. **Verfügbarkeit** bedeutet, dass Daten und Systeme zur Verfügung stehen, wenn Sie benötigt werden.

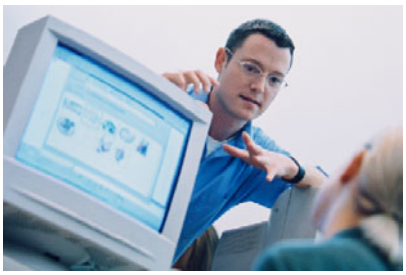
Bedenken Sie die Folgen, die es haben kann, wenn Unberechtigte Zugriff auf Ihre Daten erhalten, wenn Ihnen Systeme, die Sie im Tagesverlauf nutzen, nicht zur Verfügung stehen oder Daten, die Sie bearbeiten müssen, verändert oder gelöscht wurden.

Jeder Geschäftsführer sollte wissen, dass es für seine Institution schwerwiegende Konsequenzen haben kann, wenn unberechtigte Personen Zugang zu vertraulichen Informationen erlangen können. Mit der Methodik des GSHB werden Sie in die Lage versetzt, Maßnahmen auszuwählen, die die IT-Sicherheit in Ihrer Institution verbessern.

2.2 Verantwortlichkeit

Wissen Sie, wer die Verantwortung bei Sicherheitsvorfällen trägt?

Welche Aufgaben muss der Chef einer kleinen Institution selbst erledigen, bzw. in welche erforderlichen Tätigkeiten ist er intensiv eingebunden, um seine Institution abzusichern?



Der Chef muss

- eine Sicherheits-Leitlinie erstellen (vgl. hierzu Kapitel 4.1 und das Beispiel für eine Sicherheits-Leitlinie in Abschnitt 11.1),
- eine Risikobewertung mittels der Schutzbedarfsfeststellung durchführen (siehe Kapitel 6 und Abschnitt 11.4),
- für jedes System einen PC-Pass (siehe Abschnitt 11.2) ausfüllen (lassen); lässt er ihn durch einen Mitarbeiter ausfüllen, so muss er ihn danach inhaltlich und auf Vollständigkeit prüfen,
- relevante Sicherheitsmaßnahmen in seiner Institution umsetzen (hierzu geben wir in Kapitel 8 Beispiele, die für einen kleinen IT-Verbund relevant sind) und
- alle Vorgänge und Maßnahmen dokumentieren (vgl. auch die Checklisten aus Abschnitt 11.6).

In kleinen Institutionen ist der Chef (Geschäftsführer oder Institutionsleiter) für alle wichtigen Punkte selbst verantwortlich. Insbesondere beim Thema IT-Sicherheit hat der Chef einer kleinen Institution wenig Möglichkeiten, Verantwortung an seine Mitarbeiter zu delegieren.

3 Definition und Abgrenzung des IT-Verbundes

Wie sehen Sie als Geschäftsführer Ihren IT-Verbund?

Welche IT-Systeme gibt es in Ihrer Institution?

Am Wochenende hat Herr Anders Zeit, sich zu entspannen. Dann fallen ihm oft Verbesserungen für sein Unternehmen ein, die er dann schnell umsetzen möchte. Er ist immer noch enttäuscht über den Ausgang der Ausschreibung, bei der Herr Campe zu einem günstigeren Preis als er anbieten konnte. Um in Zukunft besser geschützt zu sein, hat er seine Frau gebeten, die Betriebssysteme der Firmenrechner zu prüfen und auf den neuesten Stand zu bringen. Leider ist Frau Anders in der vergangenen Woche erkrankt und konnte deshalb nicht die geplanten Updates an den Betriebssystemen der PCs vornehmen. Da nur Frau Anders genau weiß, welche Systeme überhaupt vorhanden sind, wo diese stehen und wie sie konfiguriert und miteinander vernetzt sind, kann niemand die geplanten Änderungen vertretungsweise vornehmen.

Nachdem es Frau Anders wieder besser geht, bittet Herr Anders sie, eine Übersicht über alle relevanten Systeme und die Vernetzung anzufertigen. Falls Frau Anders nun einmal verhindert ist, kann er auf diese Aufstellung zurückgreifen und die Änderungen ggfs. von einem Dienstleister durchführen lassen.

In diesem Abschnitt wird der IT-Verbund der Institution aus Sicht des Geschäftsführers beschrieben. Der IT-Verbund aus Sicht des GSHB befindet sich in Abschnitt 5 (Strukturanalyse).

Als IT-Verbund wird gemäß GSHB die Gesamtheit der infrastrukturellen, organisatorischen, personellen und technischen Komponenten verstanden, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

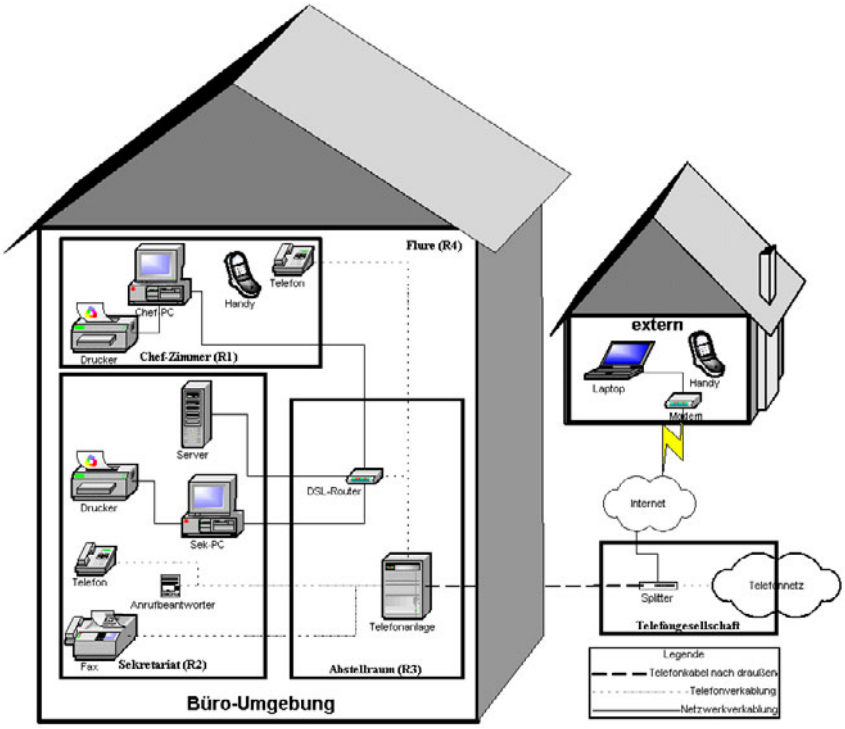


Abbildung 1: kleiner IT-Verbund

Abbildung 1 zeigt Ihnen den IT-Verbund, der diesem Dokument zugrunde liegt. Die Büro-Umgebung der dargestellten Institution besteht aus verschiedenen Räumlichkeiten (R1-R4). Befindet sich der Laptop in der Büro-Umgebung, so steht er im Chef-Zimmer (R1).

In welchen Räumen sind die Geräte aufgestellt?

- **Chef-Zimmer (R1):** Chef-PC, Drucker, Telefon, Laptop, Handy.
- **Sekretariat (R2):** Sekretariats-PC, Drucker, Telefon, Faxgerät, Anrufbeantworter, Server.
- **Abstellraum (R3):** Telefonanlage, DSL-Router mit Firewall.

- **Verbindungsräume (R4, z. B. Flure):** Teile der Verkabelung

  Diese Räume sind nicht öffentlich und nur durch die Eingangstür der Institution erreichbar.

Welche IT-Systeme sind installiert?

Der Arbeitsplatzrechner des Geschäftführers (**Chef-PC**) läuft unter Windows XP und der **Sekretariats-PC** unter Windows 2000 mit ähnlicher Konfiguration und gleichen Anwendungen. Der **Server** läuft unter Windows 2000 und dient zur zentralen Datenspeicherung verschiedener Anwendungen. An der **Telefonanlage** (TK-Anlage) sind alle **Telefone**, das **Faxgerät**, der **Anrufbeantworter** sowie der DSL-Router angeschlossen. Der **Laptop** läuft unter Windows 2000 und besitzt ein eingebautes Modem. Die Firewall des **DSL-Router**s besitzt ein spezielles Betriebsystem des Herstellers. Das **Handy** ist ein mobiles IT-System, welches der Geschäftsführer bei sich trägt.

Welche Computerprogramme werden verwendet?

Neben einer Spezialsoftware, die den Geschäftsprozess der Institution unterstützt, wird Microsoft Office 2000 eingesetzt.

Von jedem PC aus kann man auf alle Festplatten zugreifen und auf jedem Drucker ausdrucken.

Über welche (Kommunikations-)Leitungen werden Daten übertragen?

Die Kommunikationsleitungen (IT-Verbindungen) bestehen aus der internen Verkabelung und der Außenanbindung ins Internet und Telefonnetz.

Anwendung des IT-Grundschutz-Profils

Welche Parallelen zu Ihrem eigenen Büro finden Sie?

Wie können Sie die im vorliegenden Dokument beschriebenen IT-Grundschutz-Maßnahmen (siehe Kapitel 8) für Ihre individuelle Umgebung nutzen?

Frau Anders hat nach ihrer Genesung die gewünschte Übersicht über die Systeme erstellt und vergleicht die Aufstellung mit dem beispielhaften IT-Verbund des BSI in diesem Dokument. Sie stellt fest, dass in ihrem Betrieb noch ein alter PC mit Windows 95, dafür aber kein PC mit Windows XP eingesetzt wird.

Am Beispiel der in diesem Dokument beschriebene Institution wird ein vollständiges IT-Sicherheitskonzeption erstellt. Das Beispiel muss nicht notwendigerweise in allen Punkten mit den Gegebenheiten Ihrer Institution übereinstimmen. Vielmehr soll sie Ihnen als Vorlage dienen, an der Sie ohne allzu großen Aufwand kleinere Änderungen vornehmen können.

Prüfen Sie, inwieweit der beschriebene IT-Verbund mit den Gegebenheiten in Ihrer Institution übereinstimmt. Sollte sich Ihre IT-Struktur wesentlich von der hier beschriebenen unterscheiden, so sind andere Profile zu empfehlen (vgl. z. B. [GSHBPROF1] und [GSHBPROF2]).

4 Sicherheits-Leitlinie und Sicherheitskonzeption

Wissen Sie, was eine Sicherheits-Leitlinie ist und was zu einer Sicherheitskonzeption gehört? Wofür benötigen Sie die Sicherheits-Leitlinie und das Sicherheitskonzept?

Eine Sicherheits-Leitlinie definiert die zu erreichenden und gewünschten Sicherheitsziele für die Institution. Das Sicherheitskonzept beschreibt, wie diese Ziele erreicht werden sollen.

Zwei wesentliche Aspekte bei der Umsetzung des GSHB sind die Erstellung einer Sicherheits-Leitlinie und einer Sicherheitskonzeption. Dokumentieren Sie die in den nachfolgenden Kapiteln erläuterten Schritte und Sie haben diese Ziele erreicht!

4.1 Sicherheits-Leitlinie

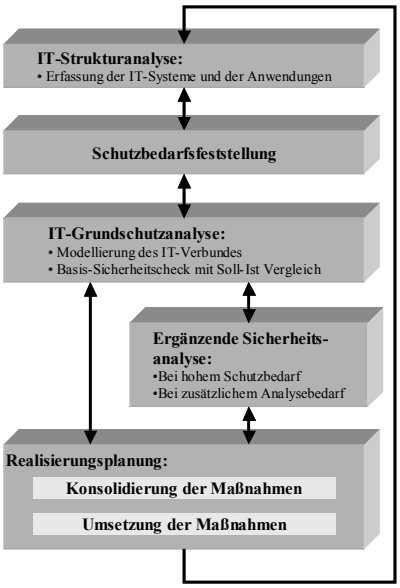
Die Sicherheits-Leitlinie definiert das angestrebte Sicherheitsniveau. Sie enthält die angestrebten Sicherheitsziele sowie die verfolgte Sicherheitsstrategie und ist daher Anspruch und Aussage zugleich. Hiermit wird das angestrebte „Ziel“ (= Sicherheitsniveau) der Institution festgelegt.

Wie Sie eine Sicherheits-Leitlinie erstellen können, ist im Dokument [BSISIPOL] beschrieben. Eine aus dieser Vorlage abgeleitete und auf eine kleine Institution angepasste Sicherheits-Leitlinie finden Sie in Abschnitt 11.1.

Bestimmen und dokumentieren Sie Ihre Sicherheits-Leitlinie auf Basis des Beispiels in Abschnitt 11.1 ggfs. unter Berücksichtigung der besonderen Anforderungen ihrer Institution.

4.2 Sicherheitskonzeption

Was genau muss ich schützen? Wogegen muss ich es schützen? Wie kann ich einen wirksamen Schutz erreichen?



Wenn Sie die Sicherheit Ihrer IT verbessern wollen, werden Sie sich schnell mit diesen Fragen konfrontiert sehen. Eine IT-Sicherheitskonzeption gibt Antwort auf die oben gestellten Fragen und gliedert sich in mehrere Teilaufgaben.

Nachdem sie die Sicherheitsziele in der Sicherheitsleitlinie festgelegt haben, ist im Rahmen der Sicherheitskonzeption der Schutzbedarf der IT-Anwendungen und IT-Systeme festzustellen und es sind dafür angemessene Sicherheitsmaßnahmen umzusetzen.

In den nächsten Kapiteln sehen Sie, wie Sie sich mit einfachen Hilfsmitteln eine IT-Sicherheitskonzeption erstellen können. Beispiele und Checklisten helfen Ihnen, die Vorgänge in Ihrer Institution zu dokumentieren und geeignete Sicherheitsmaßnahmen auszuwählen.

Legen Sie einen Ordner für die Sicherheitskonzeption an. Füllen Sie die Checkliste aus und heften Sie diese in dem Ordner ab, d.h. dokumentieren Sie, dass die Sicherheitsmaßnahmen umgesetzt sind. Ist der Ordner vollständig, haben Sie eine IT-Sicherheitskonzeption erstellt!

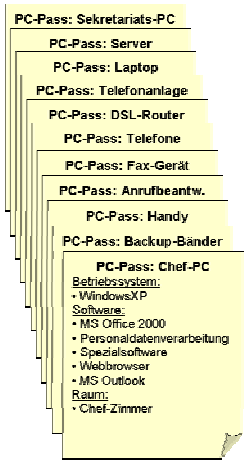
Nachdem Frau Anders die Übersicht über die IT-Systeme erstellt und die Betriebssysteme auf den neuesten Stand gebracht hat, passt sie die beispielhafte Sicherheits-Leitlinie auf die Gegebenheiten ihres Unternehmens an. Sie bespricht die Leitlinie nochmals mit ihrem Mann. Herr Anders unterzeichnet sie und gibt sie allen Mitarbeitern zur Kenntnis und erläutert

ihnen die Hintergründe. Herr Anders möchte, dass allen Mitarbeitern bewusst wird, dass die IT-Systeme einen kritischen Erfolgsfaktor für das Unternehmen darstellen. Er bittet seine Frau eine IT Sicherheitskonzeption zu erstellen.

5 Strukturanalyse

Welche Systeme und Daten gibt es in meiner Institution?

Der erste Schritt bei der Erstellung der Sicherheitskonzeption ist die Durchführung der Strukturanalyse, mit der genau diese Frage beantwortet wird. Hierzu müssen Sie zunächst für jedes IT-System folgende Informationen erfassen, um schnell alle relevanten Daten und Informationen vorliegen zu haben (z. B. im Schadensfall).



- *Bezeichnung des IT-Systems*
- *Betriebssystem des IT-Systems*
- *Anwendungen/Programme auf dem IT-System*
- *Werden mit den Anwendungen personenbezogene Daten verarbeitet?*
- *In welchem Raum steht das System?*

Zur Dokumentation der Informationen hat sich das Erstellen eines PC-Passes als nützlich erwiesen. Im PC-Pass werden alle wichtigen Daten eines IT-Systems festgehalten.

Kopieren Sie einfach den PC-Pass aus Abschnitt 11.2 und füllen Sie einen PC-Pass für jedes Ihrer IT-Systeme aus. Die vorgesehenen Einträge zum Schutzbedarf müssen Sie im Moment noch nicht ausfüllen. Lassen Sie diese noch frei.

Sich einen Überblick über die eigenen Systeme, Anwendungen und Daten zu verschaffen, ist ein wesentlicher Schritt bei der Erstellung der Sicherheitskonzeption. Diesen Schritt haben Sie erledigt, wenn Sie den PC-Pass für alle Geräte in Ihrer Institution ausgefüllt haben.

Hinweis: Die direkt an die PCs angeschlossenen Drucker werden nicht als eigenständige Komponenten, sondern als Teil des jeweiligen PCs erfasst. In den PC-Pässen sind sie unter Peripherie in Punkt Hardware aufgeführt.

Hinweis: Eine Telefonanlage, ein Handy oder ein Anrufbeantworter sind zwar keine PCs, dennoch sollten Sie einen „PC-Pass“ für diese Geräte ausfüllen. Nicht zutreffende Felder im Formular des PC-Passes (z. B. Betriebssystem des Faxgerätes) lassen Sie einfach frei. Einen exemplarisch vollständig ausgefüllten PC-Pass für den Chef-PC aus dem Beispiel finden Sie in Abschnitt 11.3.

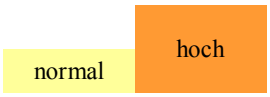
Frau Anders füllt die PC-Pässe für alle Systeme aus und heftet sie in einen separaten Ordner. Da sie sich erst vor kurzem einen Überblick über die Systeme verschafft und bei einigen Rechnern Updates des Betriebssystems und neue Anwendersoftware installiert hat, war diese Aufgabe schnell erledigt.

6 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung gibt Antworten auf Fragen nach zu schützenden Informationen und danach, wo sich diese befinden und verarbeitet werden. In der Schutzbedarfsfeststellung wird somit versucht, die folgenden Fragen zu beantworten:

Was ist zu schützen? Auf welchen Systemen werden sensible Daten verarbeitet?

Die Schutzbedarfsfeststellung dokumentiert nachvollziehbar das Sicherheitsverständnis Ihrer Institution.



Ziel der Schutzbedarfsfeststellung ist es, für jede erfasste IT-Anwendung einschließlich ihrer Daten zu entscheiden, welcher Schaden entstehen kann, wenn die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit verletzt werden. Da eine Einschätzung des möglichen Schadens meist nicht exakt quantifizierbar ist, sollten Sie zwei Kategorien definieren, die einen „normalen“ oder einen „hohen“ Schutzbedarf unterscheiden.

Die Auswahl der Maßnahmen des GSHBs und für welche Komponenten zusätzliche Maßnahmen notwendig sind, werden dadurch erleichtert. Bei einem „normalem“ Schutzbedarf sind die Standard-Sicherheitsmaßnahmen im GSHB ausreichend und angemessen. Für Komponenten mit „hohem“ Schutzbedarf kann es erforderlich sein, zusätzliche Maßnahmen zu ergreifen.

Herr Anders wird von einem potenziellen Kunden aufgefordert, schnell ein aus seiner Sicht umfangreiches Angebot abzugeben. Herr Anders hat dazu ein ausführliches Gespräch mit dem Kunden geführt und dabei mit seinem Laptop die wichtigsten Punkte notiert. Herr Anders ist sehr daran interessiert ein Angebot abzugeben, da der Umfang der durchzuführenden Arbeiten etwa 25.000 Euro betragen wird. Für das Angebot und die auszuführenden Arbeiten hat er schon während des Kundengesprächs eine Idee entwickelt, die auf einer vor einigen Jahren von seiner Firma durchgeführ-

ten Dienstleistung beruht. Auf dieser Grundlage sollte es ihm über das Wochenende möglich sein, ein fundiertes, aussagekräftiges und attraktives

Angebot zu unterbreiten. Es ist ihm sehr wichtig, diesen größeren Auftrag zu erhalten.

Als Herr Anders am Abend im Büro sitzt, muss er feststellen, dass die Unterlagen aus den früheren Jahren nicht auf dem Server abgelegt sind. Es fällt ihm ein, dass die Festplatte vor einiger Zeit getauscht wurde. Er ruft seine Frau und sagt ihr, dass er jetzt sehr schnell diese Unterlagen benötigt, da ihm sonst ein größerer Auftrag verloren geht.

Die Schutzbedarfskategorien werden anhand von Schadenszenarien, die individuell auf die Anforderungen Ihrer Institution abgestimmt sind, festgelegt. Mögliche Schäden sind dabei nicht nur finanzieller Art, betrachtet werden müssen beispielsweise auch Imageschäden sowie Verstoß gegen Gesetze, Vorschriften und Verträge.

In allen Szenarien müssen Sie entscheiden, wie wichtig Ihnen Ihre Daten sind, und darüber hinaus die individuellen Gegebenheiten Ihrer Institution berücksichtigen. Z. B. ist ein Schaden von 200.000 Euro gemessen am Umsatz für eine Bank eher gering, würde aber für einen Reisebüro zum Konkurs führen. Das GSHB liefert weitere Beispiele und Fragen um die Schutzbedarfskategorien zu definieren.

Für Herrn Anders ist ein Auftrag, der für sein Unternehmen zu etwa 25.000 Euro Umsatz führt, sehr wichtig. Von daher stuft er die Verfügbarkeit seiner Daten, die er zur schnellen Erstellung des Angebots benötigt, als 'hoch' ein.

Um die Schutzbedarfskategorien für Ihre Institution zu definieren, passen Sie einfach die Vorgaben der Tabellen aus Abschnitt 11.4 auf Ihre Institution an. Sind für Sie zusätzliche Schadensszenarien relevant, ergänzen Sie diese bitte.

6.1 IT-Anwendungen

Sie müssen für jede IT-Anwendung einschließlich ihrer Daten entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzt.

Im PC-Pass erfassen Sie für jede auf dem IT-System installierte Anwendung, ob dort personenbezogene Daten verarbeitet werden, und bestimmen – unterschieden nach den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit – den Schutzbedarf in den Kategorien normal und hoch.

Für den Chef-PC aus unserem exemplarischen IT-Verbund würde der Eintrag im PC-Pass wie folgt aussehen:

PC-Pass: Chef-PC

Anwendungen/Programme/Daten	Hotline	Personenbez Daten	Schutzbedarf: Verfügbarkeit	Schutzbedarf: Vertraulichkeit	Schutzbedarf: Integrität
MS-Office		Π	☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
Spezialsoftware		Π	☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch

Abbildung 2: Exemplarische Schutzbedarfsfeststellung am Beispiel des Chef-PCs

Die Information über den Schutzbedarf der einzelnen IT-Anwendungen gibt Ihnen einen Überblick, wie wichtig die einzelnen IT-Anwendungen für Ihre Institution sind und in welchem Maße sie von der Sicherheit der einzelnen Anwendungen abhängig sind.

Frau Anders führt die Schutzbedarfsfeststellung für die im Familienbetrieb genutzten IT-Anwendungen durch. Dabei fällt ihr auf, dass die vollständige Kundendatei mit allen Einträgen nur auf dem Laptop ihres Mannes gespeichert sind. Sie erinnert sich daran, dass sie diese Vorgehensweise mit ihrem Mann abgesprochen hat, damit aus Sicherheitsgründen kein Unbefugter Einblick in die Daten nehmen kann. Insbesondere wegen der Einträge der speziellen Sonderwünsche seiner Kunden, auf die er flexibel und

schnell reagiert. Herrn Anders ist diese Datei sehr wichtig. Herr Anders lässt seinen Laptop daher nie unbeaufsichtigt.

Frau Anders nimmt eine Bewertung des Schutzbedarfs für die Kundendatei vor. Der Ausfall der Kundendatei über einen begrenzten Zeitraum beeinflusst den Geschäftsbetrieb sehr, daher entscheidet sie sich zu einer „normalen“ Einstufung. Die Vertraulichkeit stuft sie mit „normal“ ein, da die Informationen in der Kundendatei Rückschlüsse und Einblicke in das Geschäftsmodell erlauben und der Konkurrenz z. B. die Möglichkeit bieten würde, einem Kunden ein günstigeres Angebot zu unterbreiten. Der Verlust der Vertraulichkeit stellt jedoch keine existenziell bedrohliche Gefahr dar. Da Fehler in der Kundendatei rasch erkannt und die Daten nachträglich korrigiert werden können, stuft Sie den Schutzbedarf für die Integrität mit „normal“ ein.

Bewerten Sie - wie Frau Anders im Beispiel - den Schutzbedarf für alle Anwendungen auf den IT-Systemen in Ihrer Institution und tragen Sie die Ergebnisse in den jeweiligen PC-Pass ein.

6.2 IT-Systeme

IT-Systeme werden eingesetzt, um Anwendungen zu unterstützen. Daher wird der Schutzbedarf der IT-Systeme von den Anwendungen bestimmt, die auf ihnen laufen. Unter einem IT-System werden nicht nur PCs und Laptops, sondern auch Kopierer, Faxgeräte oder Telefone verstanden.

Damit Sie den Schutzbedarf eines IT-Systems bestimmen können, müssen Sie zunächst alle IT-Anwendungen betrachten, die auf diesem System laufen. Eine Übersicht über die relevanten IT-Anwendungen und deren Schutzbedarf finden Sie in den ausgefüllten PC-Pässen. Der Schutzbedarf der IT-Anwendungen "vererbt" sich auf die IT-Systeme.

Zur Ermittlung des Schutzbedarfs des IT-Systems müssen Sie die möglichen Schäden der relevanten IT-Anwendungen in ihrer Gesamtheit betrachten. Im Wesentlichen bestimmt der Schaden mit den schwerwiegends-

ten Auswirkungen den Schutzbedarf eines IT-Systems (Maximum-Prinzip).

Der Eintrag in den PC-Pass für den Chef-PC des kleinen IT-Verbundes gemäß Kapitel 3 lautet daher wie folgt:

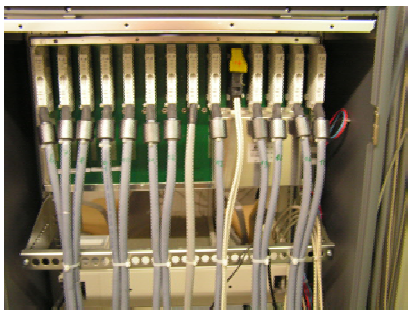
PC-Pass: Chef-PC

Anwendungen/Programme/Daten	Hotline	Personenbez Daten	Schutzbedarf: Verfügbarkeit	Schutzbedarf: Vertraulichkeit	Schutzbedarf: Integrität
MS-Office		Π	☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
Spezialsoftware		Π	☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
Abgeleiteter Schutzbedarf des Systems			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch

Abbildung 3: Bestimmung des Schutzbedarfs des IT-Systems am Beispiel des Chef-PCs

Vervollständigen Sie nun den PC-Pass für jedes IT-System Ihrer Institution, indem Sie den Schutzbedarf der Anwendungen auf das IT-System "vererben".

6.3 Kommunikationsverbindungen



Welche schutzbedürftigen Kommunikationsverbindungen gibt es in der Institution?

Kommunikationsverbindungen sind hinsichtlich der Schutzbedarfsfeststellung ein nicht zu unterschätzender Teil des IT-Verbundes. Kommunikationsverbindungen spielen für den Geschäftsbetrieb eine wichtige Rolle, wenn z. B. sensible Daten übertragen werden. Das GSHB betrachtet nur kritische Kommunikationsverbindungen,

- die Außenverbindungen darstellen, d. h. die in oder über unkontrollierte Bereiche führen (z. B. ins Internet oder über öffentliches Gelände),
- über die Informationen übertragen werden, an die ein hoher Anspruch an Vertraulichkeit, Integrität oder Verfügbarkeit erhoben wird, oder
- über die Informationen mit sehr hohem Schutzbedarf nicht übertragen werden dürfen.

Im IT-Verbund aus Kapitel 3 zählt die Internetanbindung zu den kritischen Kommunikationsverbindungen, da sie in einen unkontrollierten Bereich führt. Im Beispiel aus Kapitel 2.1 haben wir gesehen, wie durch das Schadensprogramm Informationen an einen Unbefugten übertragen wurden.

6.4 Räume

In dem vorliegenden kleinen und übersichtlichen IT-Verbund kann konkrete Vererbung des Schutzbedarf von den Systemen auf die Räume vernachlässigt werden. Da viele kleine Institutionen Publikumsverkehr haben, ist pauschal von ein höheren

Schutzbedarf der Räume auszugehen.

6.5 Interpretation der Ergebnisse

Die vorangegangenen Abschnitte haben Ihnen gezeigt, dass alle Aspekte gleichermaßen berücksichtigt werden müssen.

Die Beispiele aus den Abschnitten haben verdeutlicht, dass Sie alle Grundwerte (Vertraulichkeit, Verfügbarkeit und Integrität) bei der Erstellung eines Sicherheitskonzepts berücksichtigen müssen. Bereits ein vernachlässigter Grundwert kann erhebliche Auswirkungen auf die Sicherheit Ihrer Institution haben.

Mit Abschluss der Schutzbedarfsfeststellung haben Sie folgendes erreicht:

- Sie haben eine aktuelle Übersicht über die eigene IT und ein gutes Verständnis der Bedeutung Ihrer IT zur Erledigung Ihrer Aufgaben.
- Zusätzlich haben Sie bereits ein Gefühl für mögliche Gefahren und deren Auswirkungen im Zusammenhang mit der IT in Ihrer Institution entwickelt.

In den nachfolgenden Kapitel werden auf Grundlage der nun vorliegenden Schutzbedarfsfeststellung konkrete Maßnahmen für den IT-Verbund Ihrer Institution abgeleitet, die den Gefährdungen begegnen und damit zu einer Minimierung der Schadensauswirkungen führen.

7 Modellierung

Das GSHB umfasst derzeit (Stand: Oktober 2003) 58 Bausteine, 331 Gefährdungen und 722 Maßnahmen.

Aber keine Angst, Sie müssen nicht alle Gefährdungen und Maßnahmen einzeln durchgehen und für Ihre Institution bewerten.

Jeder Baustein des GSHBs behandelt ein bestimmtes Themengebiet und verweist jeweils auf die dafür relevanten Gefährdungen und Standard-Sicherheitsmaßnahmen. Zur Gliederung gehört jeder Baustein - je nach Themengebiet - zu einer der folgenden Schichten:

1. Übergreifende Aspekte: Konzepte und Regelungen, die für die gesamte Institution gelten, z. B. Datensicherungskonzept, Notfallvorsorgekonzept, Outsourcing
2. Infrastruktur: baulich-physische Sicherheitsmaßnahmen, z. B. Schutz vor Feuer, Einbruch, Stromversorgung im Gebäude, Verkabelung usw.
3. IT-Systeme: Sicherheitsaspekte von IT-Systemen, z. B. Server, Clients, TK-Anlagen
4. Netze: Vernetzung von IT-Systemen, z. B. Modem
5. Anwendungen: Sicherheit von typischen IT-Anwendungen, z. B. E-Mail, Datenbanken, Apache Webserver

Das GSHB gibt Ihnen in Kapitel 2.3.1 Bausteine zur Hand, mit denen Sie Ihre IT-Umgebung nachbilden (modellieren) können. Insbesondere wird beschrieben, wann die einzelnen Bausteine sinnvollerweise eingesetzt werden sollten und auf was sie anzuwenden sind. (Modellierungshinweise)

Stellen Sie eine Verknüpfung zwischen den Bausteinen des GSHB und Ihrer realen Informationstechnik her, in dem Sie die Bausteine mit den Modellierungshinweisen systematisch abarbeiten. Legen Sie sich dazu eine

Tabelle an, in der Sie die Bausteinzuordnung zum Anwendungsbereich notieren. (für das betrachtete Beispiel ist dies in Anhang 11.5 vollständig ausgeführt)

Nr.	Baustein	anzuwenden auf
Übergeordnete Komponenten		
B 3.0	IT-Sicherheitsmanagement	gesamten IT-Verbund
B 3.1	Organisation	gesamten IT-Verbund
B 3.2	Personal	gesamten IT-Verbund
B 3.4	Datensicherungskonzept	gesamten IT-Verbund
B 3.6	Computer-Virenschutzkonzept	gesamten IT-Verbund
B 3.9	Hard- und Software-Management	gesamten IT-Verbund
B 9.1	Standardsoftware	gesamten IT-Verbund

Abbildung 4: Auszug aus der Modellierung nach GSHB mit den in jedem Fall anzuwendenden Bausteinen

Als Herr Anders vor einiger Zeit für die schnelle Erstellung eines Angebots die Daten einer ausgetauschten Festplatte benötigte, konnte ihm seine Frau schnell weiterhelfen. Sie hatte vor dem Wechsel der Festplatte alle Daten auf einem Band gesichert und konnte die gewünschten Dateien innerhalb einer Viertelstunde zurückspielen. Ihr Mann hatte damit alles zur Verfügung, was er zur Erstellung des Angebots für den neuen Kunden brauchte. Dies war möglich, weil Frau Anders die Hinweise des Bausteins B 3.4 des GSHB beachtet hatte, die u.a. eine regelmäßige Datensicherung vorsehen.

Das Ergebnis der Modellierung ist ein Teil der IT-Sicherheitskonzeption, da jeder Baustein des GSHB auf die jeweils dafür umzusetzenden Sicherheitsmaßnahmen verweist.

8 Selbstüberprüfung

Wir kommen nun zum letzten Schritt bei der Erstellung einer IT-Sicherheitskonzeption, der zur Beantwortung der folgenden Frage führt:

Welche Standard-Sicherheitsmaßnahmen sind bereits umgesetzt und wo ist noch Handlungsbedarf?

Dieses Kapitel wird Ihnen dabei helfen, Defizite innerhalb Ihrer Institution zu erkennen, die zu einem Risiko für Ihre IT-Systeme und Daten führen können und konkrete Gegenmaßnahmen festzulegen. Hierzu werden die für den IT-Verbund identifizierten Bausteine des GSHB herangezogen. Die Maßnahmen und Gefährdungen der einzelnen Bausteine sind im GSHB unter der entsprechenden Bausteinnummer beschrieben. Anhand von konkreten Beispielen einzelner Bausteine erfahren Sie, wie Sie das GSHB anwenden können und wie die Anforderungen sinnvoll auf Ihren IT-Verbund angewendet werden können.

8.1 Umsetzungsbeispiele

Die nachfolgenden Abschnitte befassen sich beispielhaft mit einigen Bausteinen des GSHB. Am Textrand finden Sie Hinweise auf die detailliert im GSHB beschriebenen Maßnahmen (gekennzeichnet durch Mx.y, wobei x und y auf die entsprechenden Nummern im GSHB verweisen) und auf die in den Checklisten formulierten Fragen (gekennzeichnet durch Fn, wobei n die fortlaufende Nummer der Frage in Abschnitt 11.6 bezeichnet). Um mehr über die einzelnen Maßnahmen zu lesen, schlagen Sie das GSHB unter den entsprechenden Maßnahmennummern auf.

8.2 Baustein B 3.4 Datensicherungskonzept

F11 F12 F18

Computersysteme und Datenspeicher (z. B. Festplatte) können ausfallen und hierdurch gravierende Schäden verursachen, da gespeicherte Daten ggf. die Grundlage der Arbeitsprozesse sind. Daher müssen Sie gewährleisten, dass die Schäden aufgrund eines Ausfalls von Datenspeichern minimiert sind.

An folgende Punkte müssen Sie denken:

M 6.24
M 6.32
M 6.36
M 6.37
M 2.41
M 2.137

- Schaffen Sie ein Speichermedium an, mit dem Sie regelmäßig (mindestens wöchentlich, besser täglich) Ihre Daten sichern können (z. B. Bandlaufwerk). Achten Sie dabei auf eine ausreichende Speicherkapazität und beschriften Sie die Datenträger eindeutig.

  Sinnvoll ist hier eine automatisierte Durchführung der Datensicherung, bei der nur einmal wöchentlich das Medium gewechselt werden muss. (Benennen Sie einen Verantwortlichen)

  Erstellen Sie eine PC-Notfalldiskette für jedes IT-System.

  Hinweis: Lagern Sie die Backup-Datenträger (z. B. CD-R, Bänder) außerhalb ihrer Büroumgebung (z. B. im Bankschließfach).

M 6.41

- Prüfen Sie regelmäßig, ob Sie die Daten auf den Backupmedien (z. B. CD-R) lesen und nutzen können.

Die Nützlichkeit der von Frau Anders vorgenommenen Datensicherung einer getauschten Festplatte wurde bereits illustriert. Darüber hinaus macht Frau Anders einmal in der Woche, in der Regel am Samstagnachmittag, von allen PCs ein Backup auf ein Sicherungsband. Sie benutzt in zyklischem Wechsel hierfür insgesamt drei Bänder. Diese bewahrt sie in einem Stahlschrank im Keller des Privathauses auf. Jeden Monat macht sie zusätzlich eine Sicherung, die sie in den Tresor der örtlichen Bank bringt. Selbstverständlich hat sie auch Notfalldisketten für alle PCs erstellt.

8.3 Baustein B 7.4 E-Mail

F10 F32
F33 F34

Mit E-Mails (Electronic Mail) können beliebige elektronische Daten über das Internet von einem Computer zu einem anderen gesendet werden. Bei der Nutzung von E-Mails müssen Sie insbesondere auf die Virenproblematik achten und Dateianhänge eingehender E-Mails sensibel handhaben. Weiterhin ist wichtig, dass Sie festlegen, welche Informationen nicht per E-Mail versendet werden dürfen.

Wertvolle zusätzliche Informationen zum Thema E-Mail finden Sie auch auf den Seiten [WWW1] und [WWW2] im Internet.

Denken Sie an folgende Punkte:

M 2.118 M 2.119 M 2.121 - Beim Einsatz von E-Mails sollten gewisse Regeln gelten. Weisen Sie Ihre Mitarbeiter an, E-Mails regelmäßig zu löschen. Teilen Sie ihnen mit, wann E-Mails verschlüsselt werden müssen.

M 5.53 M 5.54 M 5.55 - Dateianhänge an E-Mails können schadhafte Funktionen beinhalten und ebenso wie Werbe E-Mails (Spam) zu Beeinträchtigungen führen. Weisen Sie Ihre Mitarbeiter an, sorgsam mit E-Mails umzugehen und verdächtige Anhänge (Attachments) und unerwartet erhaltene E-Mails nicht zu öffnen, da diese häufig Viren enthalten. Setzen Sie sich ggf. mit den Absendern der E-Mails telefonisch in Verbindung.

M 2.118 - Teilen Sie Ihren Mitarbeitern mit, welche Informationen nicht oder nur verschlüsselt per E-Mail versandt werden dürfen. Kunden- oder Patientendaten sind ein Beispiel für Informationen, die nicht unverschlüsselt per E-Mail versandt werden sollten.

M 5.108 M 5.88 - Setzen Sie ein Produkt zur Verschlüsselung von E-Mails ein, wenn Sie per E-Mail sensible Daten mit einem Geschäftspartner austauschen.

  Ein kostenloses Verschlüsselungsprodukt sind z. B. die Windows Privacy Tools ([WINPT]). Windows Privacy Tools ist eine Sammlung mehrsprachiger Programme für einfache Verschlüsselung und digitale Signierung von Daten.

  Eine Übersicht über Verschlüsselungsprodukte finden Sie unter [CRYPT].

M 2.274 - Bedenken Sie in Ihrer Vertretungsregelung, dass E-Mails von Mitarbeitern, die im Urlaub oder erkrankt sind, beantwortet werden.

Auf allen Rechnern in den Büroräumen und auf dem Laptop hat Frau Anders Virenscanner installiert. Mit der wöchentlichen Datensicherung aktualisiert sie auch diese Programme. Wenn Sie Hinweise über neue gefährliche Viren, etwa aus den Nachrichten, erhält, aktualisiert sie die Virenscanner, sobald es ihr möglich ist und wartet nicht bis zum Wochenende.

Manche Kunden Ihres Mannes bevorzugen den Austausch von Informationen bis hin zur Angebotsabgabe per E-Mail. Für diese Fälle hat Frau An-

ders ein leicht zu bedienendes Verschlüsselungstool auf den Firmenrechnern installiert, was auch den Kunden zur Verfügung gestellt wird. Somit ist ein vertraulicher Datenaustausch über das Internet möglich.

8.4 Baustein B 5.7 Windows 2000 Client

F6 F11 F14 F13 F23 F24 F38 F39 F40 F41 F42 F43 F44 F45 F46 F50 F51

Windows 2000 ist ein weitverbreitetes Betriebssystem mit sehr vielen Möglichkeiten und Risiken. Durch verschiedene Sicherheitsmaßnahmen kann verhindert werden, dass Unberechtigte das System nutzen oder an Daten auf dem System gelangen. Handelt es sich bei dem betrachteten PC um einen tragbaren PC (Laptop, Notebook), so müssen weitere Punkte beachtet werden. Bei einem tragbaren PC ist das Diebstahlrisiko höher als bei einem PC, der im Büro steht, da dieser in Umgebungen betrieben wird, die nicht den Schutz einer Büroumgebung gewährleisten (z. B. Bahnhof) und zu denen viele Personen Zugang haben. Trotzdem sind auf tragbaren PCs sensible Informationen gespeichert, die einen entsprechenden Schutz benötigen.

*Hinweis***:** Der Baustein B5.7, Windows 2000 Client kann ebenso für einen Computer eingesetzt werden, auf dem Windows XP installiert ist.

Setzen Sie die folgenden Maßnahmen für einen Windows 2000 Rechner um:

M 4.49 - Bei einem Windows 2000 Rechner sollte nicht die Möglichkeit bestehen, das System über einen Wechseldatenträger (z. B. CD-ROM, Diskette) zu booten. Deaktivieren Sie diese Funktion im BIOS. Wenn Sie nicht wissen, wie das geht, wenden Sie sich an einen Dienstleister oder den Lieferanten des IT-Systems.

M 4.57 - Bei Windows-Systemen werden Anwendungen direkt von CD gestartet, wenn eine CD in das Laufwerk eingelegt wird (Autostart). Deaktivieren Sie diese Funktion. Details finden Sie in den Maßnahmen M 4.57 im GSHB.

M 4.136 M 1.149 M 1.50 - Bei der Installation von Windows 2000 müssen Sie verschiedene Sicherheitsaspekte beachten. Stellen Sie sicher, dass sowohl die Hinweise von Microsoft ([MSSEC]) als auch die im GSHB (siehe M 1.136) beachtet werden.

M 2.10 - Vermerken Sie das Betriebssystem und dessen Version auf allen PC-Pässen, die in Frage kommen und notieren Sie die Nummer der Hersteller-Hotline.

M 2.35 - Installieren Sie regelmäßig (mindestens einmal pro Woche) die von Microsoft veröffentlichten Patches auf ihren Systemen. Hierdurch reduzieren Sie das Risiko, welches durch Fehler in der Software existiert.

M 3.4
M 3.5
M 3.28 - Schulen Sie Ihre Mitarbeiter im Umgang mit Windows. Hierbei ist insbesondere darauf zu achten, dass ihnen verständliche Handbücher zur Verfügung stehen.

M 4.2 - Aktivieren Sie auf allen Systemen mit Windows den Bildschirmschoner mit Passwortabfrage. Dieser sollte sich nach spätestens 15 Minuten aktivieren.

Hinweis: Das BSI bietet einen Bildschirmschoner mit Sicherheitshinweisen an. Dieser Bildschirmschoner und eine Installationsanleitung kann unter [BSIBS] erreicht werden.

M 2.25 - Dokumentieren Sie detailliert, wie Windows auf den Computern installiert ist. Notieren Sie hierbei insbesondere während des Installationsprozesses gewählte Auswahlmöglichkeiten.

Ist Windows 2000 auf einem tragbaren PC installiert, müssen Sie zusätzlich die folgende Dinge beachten:

M 1.33 - Lassen Sie das Gerät niemals unbeaufsichtigt. Unberechtigte Personen könnten Zugang zum System erlangen oder das Gerät entwenden.

Hinweis: Wird ein tragbarer PC in einem Kraftfahrzeug aufbewahrt, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein tragbarer PC stellt einen hohen Wert dar, der potentielle Diebe anlockt, zumal tragbare PCs leicht veräußert werden können. Wird der tragbare PC in fremden Büroräumen vor Ort benutzt, so ist dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen. Wird der Raum für längere Zeit verlassen, sollte auch der tragbare PC ausgeschaltet (oder in den Stand-by-Modus versetzt) werden, um über das Bootpasswort die unerlaubte Nutzung zu verhindern.

Einige neuere Geräte bieten zusätzlich die Möglichkeit zum Anketten des Gerätes an einen festen Gegenstand (z. B. Schreibtisch). Der Diebstahl setzt dann den Einsatz von Werkzeug voraus.

Verschlüsseln Sie sensible Daten, die sich auf dem Computer befinden. (vgl. [HDPROT])

M 4.2 - Aktivieren Sie bei Ihrem tragbaren PC die Bildschirmsperre derart, dass eine Deaktivierung nur nach der Eingabe eines Passwortes möglich ist.

M 4.3 - Setzen Sie einen Virenscanner ein und aktualisieren Sie diesen regelmäßig.

M 6.20 M 6.21 M 6.24 M 6.71 - Kopieren Sie die Daten von Ihrem tragbaren PC regelmäßig auf eine CD oder einen Arbeitsplatz-PC in der Büroumgebung. Sollte der tragbare PC gestohlen werden oder defekt sein, können Sie so zumindest noch auf die Daten zugreifen. Und bedenken Sie diese Datensicherung auch bei längerer mobiler Nutzung durchzuführen.

Hinweis: Die meisten tragbaren PC besitzen fest eingebaute Modems und Netzwerkkarten. Auf Reisen ermöglicht ein Modem z. B. eine Verbindung mit dem Internet aufzubauen. Achten Sie hierbei auf folgende Punkte:

- Überprüfen Sie regelmäßig die vom Modem angewählte Rufnummer. In letzter Zeit haben sich sog. „Dialer“ weit verbreitet und die Einwahlrufnummern auf kostenpflichtige Mehrwertnummern geändert.

  Zur Dialer-Problematik hat das BSI unter [DIALER] zusätzliche Informationen zur Verfügung gestellt.

- Speichern Sie keine Passworte für den Zugang zu Online-Diensten auf dem Computer. Häufig ist es zur Vereinfachung möglich, das Zugangspasswort auf dem Computer zu speichern. Diese Möglichkeit sollten Sie nicht nutzen, da es einem Unberechtigten die Möglichkeit gibt, Ihren Zugang zum Online-Dienst zu nutzen.

Für Herrn Anders ist der Laptop ein sehr wichtiger Bestandteil zur Ausübung seiner Arbeit geworden, weil dort u.a. seine Kundendatei gespeichert ist. Er lässt daher den Laptop nie unbeaufsichtigt und sichert die Daten in zweierlei Hinsicht: zum einen werden regelmäßig Sicherungskopien

von seiner Frau gemacht und zum zweiten hat Frau Anders ihm ein Programm installiert, welches die Dateien auf der Festplatte des Laptops verschlüsselt. Selbst im Falle eines Diebstahls wären die Daten schnell wiederherstellbar, für den Dieb aber wertlos. Die Hardware des Laptops selbst ist gegen Diebstahl versichert.

8.5 Baustein B 6.1 Servergestütztes Netz

F6 F11 F12 F13 F23 F24 F46 F47 F48 F49 Unter einem servergestützten Netz wird ein lokales Netz mit mindestens einem Server – welcher z. B. unter Windows 2000 betrieben wird – verstanden. Wesentliche Maßnahmen sind hierbei die durchgängige Dokumentation aller Systeme, Änderung voreingestellter Hersteller-Passwörter und die regelmäßige Datensicherung sowie die Beachtung von Sicherheitshinweisen zum Server-Betriebssystem (vgl. [WIN2KS]).

Achten Sie auf die folgenden Punkte:

M 1.32 - Der Server in Ihrer Institution ist eine zentrale Komponente in Ihrer IT. Wählen Sie den Aufstellort des Geräts derart, dass nur berechtigte Personen Zugang zu diesem Gerät haben.

M 3.10 - Legen Sie fest, wer für die Pflege und Wartung der Systeme verantwortlich ist und tragen Sie die Telefonnummer des Verantwortlichen in den PC-Pass ein.

Hinweis: Sorgen Sie dafür, dass nur kompetente Personen Ihre Systeme administrieren. Sie können sich beispielsweise vertraglich zusichern lassen, dass der für die Administration Ihrer Server verantwortliche Mitarbeiter eines externen Dienstleisters über eine entsprechende Qualifikation verfügt oder fragen Sie den Mitarbeiter einfach direkt! Als Referenz eignet sich z. B. eine MCSE (Microsoft Certified Systems Engineer) Zertifizierung.

Weiterhin sollten Sie beachten, dass die Installation der Systeme detailliert dokumentiert ist.

M 4.7 - Ändern Sie die Standard-Passwörter aller Systeme. Damit wird verhindert, dass ein Unberechtigter, der die Standard-Passwörter kennt, Zugriff zu den Systemen erlangen kann.

Hinweis: Denken Sie auch daran die Passwörter gesichert zu hinterlegen!

M 4.56 - Auf dem Server können sehr sensible Dateien abgelegt werden. Gelöschte Dateien können ggf. wiederhergestellt werden. Um dies zu verhindern, sollten Sie für derartige Dateien ein Werkzeug benutzen, das die Dateien vor der Löschung überschreibt.

M 4.146 - Bei dem Betrieb eines Windows 2000 Servers sind verschiedene Sicherheitsaspekte zu berücksichtigen. Beachten Sie die Hinweise in M 4.146 aus dem GSHB.

Frau Anders hat den Server in einem Abstellraum der Firmenräume ihres Mannes untergebracht. Es handelt sich um einen fensterlosen Raum, der zusätzlich als Lagerraum für Unterlagen genutzt wird. Der Raum wird nicht regelmäßig betreten, so dass er meist verschlossen ist. Einen Schlüssel haben Herr und Frau Anders sowie Frau Bauer. Das Administrator-Passwort für den Server kennen nur Frau und Herr Anders.

8.6 Sicherheitsstatuts

Was habe ich z.Z. für Sicherheitsanforderungen umgesetzt? Wo sind noch Lücken? Wie steht mein Unternehmen z.Z. da?

Um eine erste Einschätzung über den eigenen Sicherheitsstatus zu bekommen, hilft Ihnen eine Fragenliste, die zu jedem Baustein grundlegende Sicherheitsvoraussetzungen abfragt.

Aus der Beantwortung der Fragen, die in Form einer Checkliste in Abschnitt 11.6 enthalten sind, kann man für das Beispiel des kleinen IT-Verbunds eine erste Einschätzung des Sicherheitsniveaus ablesen.

Ergänzen Sie den Fragenkatalog mit eigenen Fragen und streichen Sie ggf. überflüssige Fragen. So können Sie sich für Ihre Institution eine individuelles Hilfsmittel für eine Selbstüberprüfung erstellen.

9 Basis-Sicherheitscheck

Für jeden Baustein muss konkret ermittelt werden, ob alle Maßnahmen umgesetzt sind.

Pro Maßnahme wird im Basis-Sicherheitsscheck ermittelt, ob die Maßnahme „umgesetzt“, „teilweise“, oder „nicht umgesetzt“ ist. Es ist aber auch möglich, dass eine Maßnahme „entbehrlich“ ist, da den entsprechenden Gefährdungen andere Maßnahmen entgegenwirken (z. B. wenn infrastrukturelle Maßnahmen entfallen, da höherwertige technische Maßnahmen realisiert sind) oder wenn die Funktion, zu deren Schutz die Maßnahme dient, nicht vorhanden ist (z. B. wenn der in der Gefährdung betrachtete Dienst auf den Computer nicht vorhanden ist).

Im Abschnitt 11.7 ist ein Formular für den kleinen IT-Verbund das Ihnen hilft, den Umsetzungsstatus aller Maßnahmen zu dokumentieren.

Führen Sie nun den Soll-Ist Vergleich für Ihre Institution durch, in dem Sie ggf. Maßnahmen im Muster-Formular ergänzen oder streichen.

Realisierung der IT-Sicherheitsmaßnahmen und Aufrechterhaltung des Sicherheitsniveaus

In den meisten Fällen gibt es einige Maßnahmen, die noch nicht oder nur teilweise realisiert sind. Der nächste Schritt besteht darin, diese Defizite soweit wie möglich zu beheben.

Frau Anders hat erfahren, dass für das Betriebssystem des Rechners von Frau Bauer ein neues Update verfügbar ist. Das Update beseitigt einige Sicherheitslücken, die bei Nutzung des Rechners im Internet auftreten können. Da Frau Bauer mit dem Firmenrechner auch einen Internetzugang hat, besorgt sich Frau Anders das Update und spielt es ein.

Mit dem einmaligen Durchlauf der IT-Grundschutz-Methodik lässt sich kein dauerhaft sicherer Zustand erreichen. Aktualisieren Sie daher regelmäßig ihre PC-Pässe und gehen Sie den Fragenkatalog durch.

10 Zusammenfassung

Die aufgezeigte Vorgehensweise hat Sie schrittweise an die Erstellung der Sicherheitskonzeption für den IT-Verbund Ihrer Institution herangeführt.

Sie haben nun dokumentiert,

- dass Ihnen Sicherheit wichtig ist und
- welche Maßnahmen Sie hierfür umgesetzt haben.

Der von Ihnen geleistete Aufwand zahlt sich in jedem Fall aus. So beziehen Banken zur Bewertung ihrer Risiken bei einer Kreditvergabe die IT-Risiken der Unternehmen mit ein. Aber auch beim Abschluss einer Versicherung für Ihre IT-Systeme kann sich die vorhandene Sicherheitskonzeption positiv auf die zu zahlenden Beiträge auswirken. Sie können jetzt z. B. leicht nachweisen, dass die Wiederbeschaffung der Daten z. B. im Falle einer defekten Festplatte für Sie kein Problem ist, weil Sie täglich ein Backup erstellen. Die Versicherung könnte sich also auf die reinen Hardwarekosten beschränken.

Herr Anders war am Nachmittag bei einem Kunden, um sich von der Qualität der ausgeführten Arbeiten zu überzeugen. Der Kunde war sehr zufrieden. Während des Gesprächs erzählt ihm der Kunde, dass in der Firma, in der er als Entwicklungsingenieur arbeitet, Hacker versucht hatten, in das Firmennetz einzudringen. Der Kunde berichtet, dass alle Entwicklungsunterlagen der aktuellen und neu entwickelten Produkte auf den Rechnern des mittelständischen Betriebs gespeichert sind. Zum Glück hat der Administrator, der diese Aufgabe nur ‚nebenbei' übernommen hat, den Netzangriff bemerkt. Der Administrator konnte sich aber zunächst nur damit helfen, dass er den Internetzugang der gesamten Firma für mehrere Stunden abschaltete. Die Analyse des Vorgangs bei der Firma ergab, dass grundsätzliche Schutzmaßnahmen nicht beachtet worden waren. Insbesondere war das mit der Auslieferung der Firewall eingestellte Default-Passwort nie geändert worden. Dies hatten die Hacker ausgenutzt.

Herr Anders erwähnt daraufhin, dass er erst kürzlich gemeinsam mit seiner Frau eine pragmatische Vorgehensweise zur Erstellung einer IT-Sicherheitskonzeption durchgeführt hat.

Herr Anders ist sich sicher, dass die von seinem Kunden geschilderten Angriffe in seinem Unternehmen nicht erfolgversprechend wären.

Sie haben gelernt, dass IT-Sicherheit nicht kompliziert ist und Sie die Nutzung einer standardisierten Vorgehensweise schnell ans Ziel geführt hat.

IT Sicherheitsmaßnahmen werden nicht zum Selbstzweck eingeführt. Alle Maßnahmen haben das Ziel, **Ihr Kerngeschäft zu sichern**.

11 Formulare und Anwendungsbeispiele

Auf den nachfolgenden Seiten sind Formulare und Anwendungsbeispiele zusammengestellt, die Sie bei der Erstellung eines Sicherheitskonzepts unterstützen sollen. Neben einer *Beispiel Sicherheits-Leitlinie* ist ein zweiseitiger PC-Pass beigefügt, welchen Sie kopieren, für jedes Ihrer Systeme ausfüllen und zusammen mit der angepassten Sicherheits-Leitlinie in den Ordner für das Sicherheitskonzept heften sollten. Um Ihnen zu verdeutlichen, wie der PC-Pass ausgefüllt wird, ist der ausgefüllte PC-Pass des Chef-PCs unseres beispielhaften IT-Verbundes beigefügt.

Nach den PC-Pässen haben wir eine beispielhafte Definition von Schutzbedarfsklassen beigefügt, die Sie als Grundlage für Ihre Einstufung in Schutzbedarfsklassen nutzen und ebenfalls in den Ordner für das Sicherheitskonzept heften sollten.

Die vollständige Modellierung für den beispielhaften IT-Verbund finden Sie im Anschluss. Sie sollten eine ähnliche Tabelle erstellen und Ihren IT-Verbund modellieren. Auch dieses Ergebnis halten Sie anschließend in Ihrem Ordner für das Sicherheitskonzept fest.

Zum Schluss haben wir noch eine Checkliste für die Selbstüberprüfung beigefügt. Nachdem Sie diese Checkliste bearbeitet und ausgefüllt haben, kommt auch sie in den Ordner für das Sicherheitskonzept. Vergessen Sie nicht, die Checkliste regelmäßig neu auszufüllen, um Änderungen an Ihrem IT-Verbund und daraus erforderliche neue Maßnahmen zu erkennen.

11.1 Beispiel Sicherheits-Leitlinie

Das nachfolgende „Sicherheits-Leitlinie-Beispiel“ soll Ihnen helfen, eine eigene Sicherheits-Leitlinie für Ihre Institution zu erstellen. Prüfen Sie die in <*kursiv*> enthaltenen Textstellen und passen Sie diese ggf. an Ihre Bedürfnisse an.

Sicherheits-Leitlinie zur Sicherheit <in der Institution>

Wir als <Institutsleitung> verabschieden hiermit folgende IT-Sicherheits-Leitlinie als Bestandteil unserer <Institutspolitik>:

Die IT unterstützt unseren Geschäftszweck insbesondere bei <tragen Sie hier Bereiche ein, in denen Sie IT einsetzen>.

Ein Ausfall soll insgesamt kurzfristig kompensiert werden können, wobei der Geschäftsablauf durch Sicherheitsmängel nicht stark beeinträchtigt werden darf. Die Maßnahmen zur Gewährleistung der Sicherheit orientieren sich an der Minimierung der im Schadensfall entstehenden Kosten – verursacht durch Schäden und/oder durch deren Vermeidung.

Unsere Daten, die unserer <Kunden/Mandanten> und unsere IT-Systeme in allen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). An die Sicherstellung der Vertraulichkeit von Firmendaten stellen wir die höchsten Ansprüche.

Zu diesem Zweck wurden Verantwortlichkeiten zur IT-Sicherheit definiert. Als Verantwortliche für die IT-Sicherheit sind der <Institutsleiter> und ein Administrator benannt sowie Vertretungsregeln erstellt worden. Die Mitarbeiter wurden und werden auch in Zukunft in der korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen geschult, sowie hinsichtlich der Gefährdungen für die IT sensibilisiert.

Wir tragen den Anforderungen der Datenschutzgesetze Rechnung und streben ein dem Geschäftszweck und der Bedeutung der personenbezogenen Daten bzw. Datenverarbeitung angemessenes Datenschutzniveau an. Die organisatorischen Voraussetzungen sind auf die Sicherstellung der Ordnungsmäßigkeit der Datenschutzgesetze ausgerichtet.

Eine kontinuierliche Revision der Regelungen und deren Einhaltung soll das angestrebte Sicherheits- und Datenschutzniveau sicherstellen. Abweichungen werden mit dem Ziel analysiert, die IT-Sicherheitssituation <in der Institution> zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnologie zu halten.

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

Datum *Unterschrift*

11.2 PC-Pass

Der PC-Pass soll dem IT-Verantwortlichen einen Überblick über die vorhandenen Computer verschaffen und ein schnelles effektives Reagieren bei Problemen ermöglichen. Somit kann sich der IT-Verantwortliche einen Überblick über die vorhandenen Systeme und deren Schutzbedürftigkeit verschaffen. Denken Sie bei Änderungen an einem IT-System daran ggfs. die Einträge im PC-Pass anzupassen.

P C - P a s s — Seite 1

System

Service-Rufnummern

Serien-/Inventarnummer

Betriebssystem inkl. eingespielte Service-Pakete und Patches

Virenscanner; Einstellungen, Aktualisierungsintervall	**letzte Aktualisierung**

Raum(nummer)		**Schutzbedarf** Verfügbarkeit	Vertraulichkeit	Integrität
	Schutzbedarf des Raumes	☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch

Notizen

P C - P a s s **Seite 2**

Anwendungen/Programme/ Daten	**Hotline**	Personen-bez Daten	**Schutzbedarf** Verfüg-barkeit	Vertrau-lichkeit	Integrität
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
Abgeleiteter Schutzbedarf des Systems			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch

Systeminstallation/-konfiguration/Notizen

11.3 Exemplarischer PC-Pass für den Chef-PC

PC-Pass Seite 1

System

Chef-PC

Service-Rufnummern

Fleissig und Partner 0123-456789

PC-Notruf 0123-987654

Serien-/Inventarnummer

PC001

Betriebssystem inkl. eingespielte Service-Pakete und Patches

Windows XP, Service Pack 123 vom 01.01.2004

Virenscanner; Einstellungen, Aktualisierungsintervall	letzte Aktualisierung
SuperScan 2004-1.2. tägliche Aktualisierung	2.3.2004

Raum(nummer)		Schutzbedarf: Verfügbarkeit	Vertraulichkeit	Integrität
Chef-Zimmer (R1)	Schutzbedarf des Raumes	☒ normal ☐ hoch	☒ normal ☐ hoch	☒ normal ☐ hoch

Notizen

Bei Windows XP ist der automatische Download von Patches aktiviert. Der Virenscanner aktualisiert sich ebenfalls täglich.

PC-Pass Seite 2

Anwendungen/Programme/ Daten	Hotline	Personenbez. Daten	Schutzbedarf Verfügbarkeit	Vertraulichkeit	Integrität
MS-Office		✓	☒ normal ☐ hoch	☒ normal ☐ hoch	☒ normal ☐ hoch
Spezialsoftware		✓	☒ normal ☐ hoch	☒ normal ☐ hoch	☒ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
			☐ normal ☐ hoch	☐ normal ☐ hoch	☐ normal ☐ hoch
Abgeleiteter Schutzbedarf des Systems			☒ normal ☐ hoch	☒ normal ☐ hoch	☒ normal ☐ hoch

Systeminstallation/Konfiguration/Notizen

Die Installation des PCs ist handschriftlich dokumentiert. Das Dokument (Installation Chef-PC) befindet sich im Anhang des Ordners für das Sicherheitskonzept. Ebenso befindet sich dort eine Aufstellung der einzelnen Hardwarekomponenten.

11.4 Definition von Schutzbedarfsklassen

Mit Hilfe der nachfolgenden Tabelle können Sie die Schutzbedarfskategorien in Ihrer Institution definieren. Hierzu müssen Sie die *kursiv* hervorgehobenen Textbestandteile auf die Gegebenheiten Ihre Institution anpassen. Die jeweils für *normalen/hohen* Schutzbedarf gültigen Formulierungen sind durch ein „/“ voneinander getrennt.

Beeinträchtigung des informationellen Selbstbestimmungsrechts	
Normal/ Hoch	- Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als *tolerabel/bedeutend* eingeschätzt werden. - Ein möglicher Missbrauch personenbezogener Daten hat *geringe/erhebliche* Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
Beeinträchtigung der Aufgabenerfüllung	
Normal/ Hoch	- Die Beeinträchtigung würde von den Betroffenen als *tolerabel/nicht tolerabel* eingeschätzt werden. - Die tolerierbare Ausfallzeit beträgt maximal z. B. *24/1 bis 24 Stunden*.
Verstoß gegen Gesetze/Vorschriften/Verträge	
Normal/ Hoch	- Verstöße gegen Vorschriften und Gesetze haben *geringfügige/erhebliche* Konsequenzen - Vertragsverletzungen haben *geringe/hohe* Konventionalstrafen zur Folge.
Beeinträchtigung der persönlichen Unversehrtheit	
Normal/ Hoch	- Eine Beeinträchtigung der persönlichen Unversehrtheit kann *wahrscheinlich/nicht absolut* ausgeschlossen werden.
Negative Außenwirkung	
Normal/ Hoch	- Es ist eine *geringe bzw. nur interne/breite* Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.
Finanzielle Auswirkungen	
Normal/ Hoch	- Es entstehen der Institution finanzielle Schäden in Höhe von *50 bis 250*/*250 bis 5000 EUR*.

Hinweis: Die Schutzbedarfskategorien sind nur ein Beispiel und können je nach Institution anders aussehen (z. B. Banken oder Rechenzentren). Diese Schutzbedarfsfeststellung bietet die Grundlage einer Risikoanalyse Ihrer Institution.

11.5 Modellierung des beispielhaften IT-Verbundes

Die nachfolgende Tabelle modelliert den beispielhaften IT-Verbund aus Kapitel 3. Die in der ersten Spalte angegebene Nummer bezieht sich auf die Nummer des Bausteins im GSHB. Die Fragen beziehen sich auf die Checkliste in Abschnitt 11.6.

Nr.	Baustein	anzuwenden auf	Fragen
Übergeordnete Komponenten			
B 3.0	IT-Sicherheitsmanagement	gesamten IT-Verbund	F1,F2,F3
B 3.1	Organisation	gesamten IT-Verbund	F4,F5,F6,F7
B 3.2	Personal	gesamten IT-Verbund	F8,F9,F10,F14
B 3.4	Datensicherungskonzept	gesamten IT-Verbund	F11,F12,F18
B 3.6	Computer-Virenschutzkonzept	gesamten IT-Verbund	F13,F14,F15,F16
B 3.9	Hard- und Software-Management	gesamten IT-Verbund	F18,F19,F20
B 9.1	Standardsoftware	gesamten IT-Verbund	F22,F23,F24
Infrastruktur			
B 4.1	Gebäude	Büroumgebung	F25,F26,F27
B 4.2	Verkabelung	Büroumgebung	F28,F29
B 4.3.1	Büroräume	Chef-Zimmer, Sekretariat, Flur, Abstellraum	F20,F30,F31
IT-Anwendungen			

B 7.4	E-Mail	Outlook	F10,F32,F33,F34
B 9.2	Datenbanken	Datenbank für die Spezialsoft-ware	F6,F11,F13, F19,F24,F37
IT-Systeme			
B 5.3	Tragbarer PC	Laptop	F6,F13,F14,F38, F39,F40,F41,F42, F43,F44,F50,F51
B 5.7	Windows 2000 Client (Windows XP Client)	Laptop, Sek.-PC (Chef-PC)	F6,F11,F14,F13, F23,F24,F45,F46
B 6.1	Servergestütztes Netz	Intranet	F6,F11,F12,F13, F23,F24,F47,F48
B 6.9	Windows 2000 Server	Server	F46,F48,F49
B 7.3	Firewall	DSL-Router	F13,F14,F23,F47, F48,F52,F53,F54
B 8.4	LAN-Anbindung eines IT-Systems über ISDN	DSL-Router	F13,F14,F23,F47, F48,F52,F53,F54
B 8.1	TK-Anlage	Telefonanlage	F13,F20,F27,F48, F55
B 8.2	Faxgerät	Faxgerät	F7,F13,F48,F56, F57,F58
B 8.3	Anrufbeantworter	Anrufbeantworter	F13,F48,F59
B 8.6	Mobiltelefon	Handy	F60,F61,F62

Tabelle 1: Bausteine des GSHB, die auf den beispielhaften IT-Verbund anwendbar sind

Hinweis: Das GSHB hat für Windows XP Clients noch keinen Baustein vorgesehen. Wegen der großen Ähnlichkeit zwischen einem Windows 2000 und einem XP Client wird bei der Modellierung der Baustein des Windows 2000 Clients angewendet.

Finden Sie im GSHB nicht den exakt passenden Baustein, dann orientieren sie sich an ähnlichen Bausteinen, die sie dann sinngemäß anwenden können!

11.6 Checkliste

Nr.	Frage
F1	Sind in Ihrer Sicherheitsleitlinie folgende Punkte definiert?
☐	- Stellenwert der Sicherheit und Bedeutung der IT für Ihr Unternehmen
☐	- Definition der Sicherheitsziele
F2	Sind Ihre Mitarbeiter ausreichend zum Thema IT-Sicherheit sensibilisiert?
☐	
F3	Haben Sie in den vergangenen 12 Monaten die Sicherheits-Leitlinie, die Schutzbedarfsfeststellung und die PC-Pässe aktualisiert oder sind Sie gerade dabei?
☐	
F4	Haben Sie im PC-Pass schon den Ansprechpartner und die Hotline-Nummern für alle IT-Systeme ausgefüllt?
☐	
F5	Haben Sie einen festen Ansprechpartner, wenn es zu Problemen mit den Computern oder den Programmen/Anwendungen kommt, und ist dessen Telefonnummer (Hotline-Rufnummer) im PC-Pass notiert?
☐	
F6	Haben Sie Ihren Mitarbeitern mitgeteilt, dass ein Passwort
☐	- regelmäßig gewechselt werden muss,
☐	- mindestens 8 Stellen lang
☐	- nicht leicht zu erraten sein darf (z. B. Vorname des Ehemanns, Kfz-Kennzeichen etc.) und
☐	- in einem verschlossenen Umschlag hinterlegt sein muss?
F7 ☐	Haben Sie in Ihrer Institution einen Aktenvernichter aufgestellt?
F8	Weisen Sie neue Mitarbeiter auf die Sicherheitsleitlinie und deren Inhalte hin?
☐	
F9	Haben Sie eine Checkliste erstellt, die Sie bei
☐	Einstellung und
☐	Ausscheiden
	eines Mitarbeiters abarbeiten?
F10	Existiert eine Vertretungsregelung (Urlaub/Krankheit) von Mitarbeitern, die für die IT zuständig sind?
☐	Ist hierin sichergestellt, dass die E-Mails eines abwesenden Mitarbeiters bearbeitet werden?
☐	

F11 ☐	Haben Sie festgelegt, welche Daten regelmäßig gesichert werden, welche Person für die Datensicherung (Medienwechsel) zuständig ist, und überprüfen Sie regelmäßig, ob Ihre Datensicherung funktioniert?
F12 ☐	Werden die Datensicherungsmedien (Bänder, CDs etc.) sicher aufbewahrt? (z. B. in einem Bankschließfach; Tresor)
F13	Werden Ihre Mitarbeiter bei der Einführung neuer Programme und Geräte in deren Nutzung eingewiesen und geschult?
☐	Virenschutz
☐	Datenbank
☐	Laptopnutzung
☐	Betriebssystem (Windows 2000/XP etc.)
☐	Telefon-Anlage / TK-Anlage
☐	Fax-Gerät
☐	Anrufbeantworter
F14 ☐	Haben Sie Ihren Mitarbeitern untersagt, eigene Software auf den Computern zu installieren?
F15 ☐	Setzen Sie Virenschutzprogramme ein, und werden diese regelmäßig automatisch aktualisiert?
F16	Wissen Sie und Ihre Mitarbeiter, wie die Virenschutzprogramme
☐	bedient werden und was zu tun ist, wenn ein Virus gemeldet wird?
☐	Informieren Sie sich regelmäßig über neue Viren?
F17 ☐	Werden Datenträger (z. B. CDs, Disketten) auf Viren überprüft, bevor sie weitergegeben werden?
F18 ☐	Sind die Datenträger (Disketten, CDs, etc.) in Ihrer Institution eindeutig gekennzeichnet?
F19	Wissen Sie und Ihre Mitarbeiter, wo die Handbücher der Pro-
☐	gramme stehen, die sie täglich nutzen?
☐	Insbesondere die der Datenbanken/Spezialsoftware!
F20 ☐	Werden Besucher Ihrer Institution während des Aufenthalts ständig durch einen Ihrer Mitarbeiter begleitet und beaufsichtigt?
F21 ☐	Wissen Sie, wo Ihre Sekretärin wichtige Dokumente abgelegt hat, und könnten Sie diese ohne Ihre Sekretärin finden (z. B. wenn diese plötzlich erkrankt)?

F22	Haben Sie im PC-Pass notiert, welche Software in welcher Version □ auf den einzelnen Computern installiert ist, □ wie die Rufnummer der Hotline lautet und □ ob die Software vollständig geliefert wurde?
F23	Haben Sie sich in den letzten vier Wochen über Aktualisierungen (Patches/Updates) der in Ihrer Institution eingesetzten Software informiert? □
F24	Wird die Installation und Deinstallation von Software und Betriebssystem schriftlich dokumentiert und □ ist diese im Ordner für die Sicherheitskonzeption abgelegt?
F25 □	Haben Sie in Ihrer Institution Rauchmelder installiert?
F26	Wissen Sie und Ihre Mitarbeiter, □ wo sich die Notausgänge befinden und □ wie die Fluchtwege verlaufen, □ wo sich die Feuerlöscher befinden und ist bekannt, □ wie die Feuerlöscher bedient werden und □ dass feuergefährliche Geräte eine Brandgefahr darstellen?
F27	Haben Sie Ihre Mitarbeiter angewiesen, Fenster und Türen nach Dienstende zu schließen und feuergefährliche Geräte auszuschalten? □
F28	Ist sichergestellt, dass Besucher keine Möglichkeit haben, Kabel in Ihrer Büroumgebung zu manipulieren? □
F29	Sind alle Stromleitungen durch einen Elektro-Fachbetrieb verlegt worden und sind diese vor Kurzschließen gesichert? □
F30	Haben Sie festgelegt, zu welchen Zeiten das Betreten der Institution durch die Mitarbeiter zulässig ist? □
F31	Verschließen Ihre Mitarbeiter sensible Daten nach Feierabend und halten Sie ihren Arbeitsplatz ordentlich? □
F32	Weisen Sie Ihre Mitarbeiter regelmäßig über die Risiken von E-Mail-Anhängen (Viren, Würmer) hin? □
F33	Haben Sie festgelegt, welche Informationen **NICHT** per E-Mail versandt werden dürfen? □
F34	Nutzen Sie ein Verschlüsselungsprodukt, wenn sensible Daten per E-Mail versandt werden? □

F35 ☐	Ist die Konfiguration Ihrer speziellen Bürosoftware schriftlich dokumentiert, und werden Änderungen nachgehalten?
F36 ☐	Ist sichergestellt, dass z. B. Ihre Sekretärin nicht auf Daten zugreifen kann, auf die sie nicht unbedingt zugreifen muss?
F37 ☐	Besitzt die von Ihnen eingesetzte Datenbank die Möglichkeit, unterschiedliche Rechte beim Zugriff auf die Daten in der Datenbank zu definieren?
F38 ☐	Haben Sie das Notebook ständig im Auge, wenn Sie es außerhalb des Büros nutzen?
F39 ☐	Haben Sie auf dem Notebook einen Bildschirmschoner mit Passwortschutz installiert?
F40 ☐	Ist auch auf dem Notebook ein Virenscanner installiert, der regelmäßig aktualisiert wird?
F41 ☐	Wird das Betriebssystem des Notebooks regelmäßig aktualisiert?
F42 ☐	Werden die Daten auf der Festplatte verschlüsselt?
F43 ☐	Können Sie die Daten Ihres Notebooks wiederherstellen, wenn dessen Festplatte kaputt geht?
F44 ☐	Kopieren Sie die Daten des Notebooks regelmäßig auf den Server oder brennen Sie diese auf eine CD?
F45 ☐	Ist sichergestellt, dass das Starten des Systems über Wechselmedien (z. B. CD-ROM, Diskette, etc.) durch ein Passwort geschützt ist oder verhindert wird?
F46 ☐	Wurde Ihr Windows 2000 System sicher installiert?
F47 ☐	Haben Sie sich vertraglich von Ihrem Dienstleister zusichern lassen, das nur geschultes Personal (z. B. MCSE zertifiziertes) Ihre Systeme administriert?
F48 ☐	Haben Sie Ihren Server und die TK-Geräte so aufgestellt, dass diese nicht für unberechtigte (z. B. Besucher) zugänglich sind?
F49 ☐	Setzen Sie zum Löschen von Dateien mit vertraulichem Inhalt ein spezielles Programm ein, welches eine Wiederherstellung verhindert?
F50 ☐	Haben Sie die Speicherung der Passwörter in der Kommunikationssoftware deaktiviert?

F51 □	Haben Sie die Rufnummer, die vom Modem gewählt wird, überprüft?
F52 □	Ist der Zugang zum Internet durch eine Firewall abgesichert?
F53 □ □	Haben Sie die Konfiguration der Firewall (insbesondere deren Filterlisten) schriftlich dokumentiert und wird sichergestellt, dass der Zugriff auf Ihre Systeme aus dem Internet verhindert wird?
F54 □	Ist die Nutzung aktiver Inhalte (insbesondere ActiveX) an Ihren WWW-Browsern deaktiviert?
F55 □	Wird die TK-Anlage von geschulten Personen gewartet und sind Anbieter und Telefonnummer notiert?
F56 □	Haben Sie festgelegt, welche Informationen nicht per Fax versandt werden dürfen?
F57 □	Verwenden Sie ein Fax-Vorblatt, welches mindestens Rufnummer des Faxgerätes, Name des Absenders, Telefonnummer eines Ansprechpartners, Name des Empfängers und der Seitenzahl einschließlich Fax-Vorblatt enthält?
F58 □	Prüfen Sie regelmäßig die Empfangsprotokolle und Zielwahlnummern auf Plausibilität?
F59 □	Ist die Fernabfragefunktion des Anrufbeantworters deaktiviert oder durch einen individuellen Code abgesichert?
F60 □	Haben Sie sich die Hotline-Nummer Ihres Mobilfunkanbieters notiert, so dass Sie Ihr Handy bei Diebstahl sperren können?
F61 □	Haben Sie eine individuelle und nicht einfach zu erratende PIN gewählt?
F62 □	Bewahren Sie die PIN und PUK für Ihr Mobiltelefon und die SIM bei den hinterlegten Passwörtern auf?
F63 □ □ □	Sind Ihre Systeme vor Diebstahl geschützt und gegen Diebstahl versichert? Insbesondere sollten Sie an Laptops und Mobiltelefone denken!
F64	...

11.7 Maßnahmen

Die nachfolgenden Tabellen enthalten eine Auswahl von Maßnahmen zu den in Kapitel 8 behandelten Bausteinen des GSHB. Die linke Spalte der Tabelle verweist jeweils auf die entsprechende Nummerierung im GSHB. Dort finden Sie ggfs. auch weitere Details zu den Maßnahmen. Wenn Sie diese Tabellen durcharbeiten können Sie in den rechten Spalten markieren, ob sie die Maßnahme vollständig (JA), teilweise (T) oder nicht (N) umgesetzt haben. Wenn die Maßnahme nach Ihrer Bewertung entbehrlich ist, markieren sie dies in der Spalte (E).

	Datensicherungskonzept B 3.4	JA	E	T	N
2.41	Verpflichtung der Mitarbeiter zur Datensicherung				
2.137	Beschaffung eines geeigneten Datensicherungssystems				
6.33	Entwicklung eines Datensicherungskonzepts				
6.34	Erhebung der Einflussfaktoren der Datensicherung				
6.35	Festlegung der Verfahrensweise für die Datensicherung				
6.36	Festlegung des Minimaldatensicherungskonzeptes				
6.37	Dokumentation der Datensicherung				
6.41	Übungen zur Datenrekonstruktion				

	Windows 2000 Server B 6.9	JA	E	T	N
1.29	Geeignete Aufstellung eines IT-Systems				
2.3	Datenträgerverwaltung				
2.4	Regelungen für Wartungs- und Reparaturarbeiten				
2.9	Nutzungsverbot nicht freigegebener Hard- und Software				
2.10	Überprüfung des Hard- und Software-Bestandes				
2.13	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln				
2.22	Hinterlegen des Passwortes				
2.25	Dokumentation der Systemkonfiguration				
2.26	Ernennung eines Administrators und eines Vertreters				
2.30	Regelung für die Einrichtung von Benutzern / Benutzergruppen				
2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile				
2.32	Einrichtung einer eingeschränkten Benutzerumgebung				
2.34	Dokumentation der Veränderungen an einem bestehenden System				
2.35	Informationsbeschaffung über Sicherheitslücken des Systems				
2.227	Planung des Windows 2000 Einsatzes				
2.228	Festlegen einer Windows 2000 Sicherheitsrichtlinie				
2.231	Planung der Gruppenrichtlinien unter Windows 2000				
3.4	Schulung vor Programmnutzung				

	Windows 2000 Server B 6.9	JA	E	T	N
3.5	Schulung zu IT-Sicherheitsmaßnahmen				
3.10	Auswahl eines vertrauenswürdigen Administrators und Vertreters				
3.11	Schulung des Wartungs- und Administrationspersonals				
3.28	Schulung zu Windows 2000 Sicherheitsmechanismen für Benutzer				
4.2	Bildschirmsperre				
4.3	Regelmäßiger Einsatz eines Viren-Suchprogramms				
4.4	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern				
4.15	Gesichertes Login				
4.17	Sperren und Löschen nicht benötigter Accounts und Terminals				
4.30	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen				
4.44	Prüfung eingehender Dateien auf Makro-Viren				
4.48	Passwortschutz unter Windows NT/2000				
4.49	Absicherung des Boot-Vorgangs für ein Windows NT/2000 System				
4.52	Geräteschutz unter Windows NT/2000				
4.57	Deaktivieren der automatischen CD-ROM-Erkennung				
4.75	Schutz der Registrierung unter Windows NT/2000				
4.84	Nutzung der BIOS-Sicherheitsmechanismen				
4.93	Regelmäßige Integritätsprüfung				
4.136	Sichere Installation von Windows 2000				

	Windows 2000 Server B 6.9	JA	E	T	N
4.148	Überwachung eines Windows 2000 Systems				
4.149	Datei- und Freigabeberechtigungen unter Windows 2000				
4.150	Konfiguration von Windows 2000 als Workstation				
4.200	Umgang mit USB-Speichermedien				
6.20	Geeignete Aufbewahrung der Backup-Datenträger				
6.22	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen				
6.27	Sicheres Update des BIOS				
6.32	Regelmäßige Datensicherung				
6.77	Erstellung von Rettungsdisketten für Windows 2000				
6.78	Datensicherung unter Windows 2000				

	Servergestütztes Netz B 6.1	JA	E	T	N
1.28	Lokale unterbrechungsfreie Stromversorgung				
1.29	Geeignete Aufstellung eines IT-Systems				
1.32	Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern				
2.3	Datenträgerverwaltung				
2.4	Regelungen für Wartungs- und Reparaturarbeiten				
2.9	Nutzungsverbot nicht freigegebener Hard- und Software				
2.10	Überprüfung des Hard- und Software-Bestandes				
2.13	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln				
2.22	Hinterlegen des Passwortes				
2.25	Dokumentation der Systemkonfiguration				
2.26	Ernennung eines Administrators und eines Vertreters				
2.30	Regelung für die Einrichtung von Benutzern / Benutzergruppen				
2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile				
2.32	Einrichtung einer eingeschränkten Benutzerumgebung				
2.34	Dokumentation der Veränderungen an einem bestehenden System				
2.35	Informationsbeschaffung über Sicherheitslücken des Systems				
2.38	Aufteilung der Administrationstätigkeiten				
2.138	Strukturierte Datenhaltung				

	Servergestütztes Netz B 6.1	JA	E	T	N
2.204	Verhinderung ungesicherter Netzzugänge				
3.4	Schulung vor Programmnutzung				
3.5	Schulung zu IT-Sicherheitsmaßnahmen				
3.10	Auswahl eines vertrauenswürdigen Administrators und Vertreters				
3.11	Schulung des Wartungs- und Administrationspersonals				
4.1	Passwortschutz für IT-Systeme				
4.2	Bildschirmsperre				
4.3	Regelmäßiger Einsatz eines Viren-Suchprogramms				
4.7	Änderung voreingestellter Passwörter				
4.15	Gesichertes Login				
4.16	Zugangsbeschränkungen für Accounts und / oder Terminals				
4.17	Sperren und Löschen nicht benötigter Accounts und Terminals				
4.24	Sicherstellung einer konsistenten Systemverwaltung				
4.44	Prüfung eingehender Dateien auf Makro-Viren				
4.65	Test neuer Hard- und Software				
5.6	Obligatorischer Einsatz eines Netzpasswortes				
5.7	Netzverwaltung				
5.8	Monatlicher Sicherheitscheck des Netzes				
5.9	Protokollierung am Server				
5.10	Restriktive Rechtevergabe				

	Servergestütztes Netz B 6.1	JA	E	T	N
5.13	Geeigneter Einsatz von Elementen zur Netzkopplung				
6.20	Geeignete Aufbewahrung der Backup-Datenträger				
6.21	Sicherungskopie der eingesetzten Software				
6.22	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen				
6.25	Regelmäßige Datensicherung der Server-Festplatte				
6.31	Verhaltensregeln nach Verlust der Systemintegrität				
6.32	Regelmäßige Datensicherung				

	E-Mail B 7.4	JA	E	T	N
2.30	Regelung für die Einrichtung von Benutzern / Benutzergruppen				
2.42	Festlegung der möglichen Kommunikationspartner				
2.46	Geeignetes Schlüsselmanagement				
2.118	Konzeption der sicheren E-Mail-Nutzung				
2.119	Regelung für den Einsatz von E-Mail				
2.120	Einrichtung einer Poststelle				
2.121	Regelmäßiges Löschen von E-Mails				
2.122	Einheitliche E-Mail-Adressen				
2.123	Auswahl eines Mailproviders				
2.274	Vertretungsregelungen bei E-Mail-Nutzung				
2.275	Einrichtung funktionsbezogener E-Mailadressen				
3.4	Schulung vor Programmnutzung				
3.5	Schulung zu IT-Sicherheitsmaßnahmen				
3.10	Auswahl eines vertrauenswürdigen Administrators und Vertreters				
3.11	Schulung des Wartungs- und Administrationspersonals				
4.33	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung				
4.34	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen				
4.44	Prüfung eingehender Dateien auf Makro-Viren				
4.64	Verifizieren der zu übertragenden Daten vor Weiter-				

	E-Mail B 7.4	JA	E	T	N
	gabe / Beseitigung von Restinformationen				
4.65	Test neuer Hard- und Software				
4.199	Vermeidung gefährlicher Dateiformate				
5.22	Kompatibilitätsprüfung des Sender- und Empfänger-systems				
5.32	Sicherer Einsatz von Kommunikationssoftware				
5.53	Schutz vor Mailbomben				
5.54	Schutz vor Mailüberlastung und Spam				
5.55	Kontrolle von Alias-Dateien und Verteilerlisten				
5.56	Sicherer Betrieb eines Mailservers				
5.57	Sichere Konfiguration der Mail-Clients				
5.63	Einsatz von GnuPG oder PGP				
5.67	Verwendung eines Zeitstempel-Dienstes				
5.108	Kryptographische Absicherung von E-Mail				
5.109	Einsatz eines E-Mail-Scanners auf dem Mailserver				
5.110	Absicherung von E-Mail mit SPHINX (S/MIME)				
6.23	Verhaltensregeln bei Auftreten eines Computer-Virus				
6.38	Sicherungskopie der übermittelten Daten				
6.90	Datensicherung und Archivierung von E-Mails				

Anhang A Glossar

BIOS	Basic Input/Output System. Das BIOS ist ein permanentes Basis-Betriebssystems, das für die Ein- und Ausgabe von Daten in einem PC verantwortlich ist. Das BIOS kontrolliert den Datenaustausch zwischen Festplatte, Grafikkarte, Tastatur und Maus.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
Computerwurm	Selbstständiges, selbstreproduzierendes Programm, das sich in einem System (vor allem in Netzen) ausbreitet.
GSHB	IT-Grundschutzhandbuch des BSI.
Intranet	Firmeninternes Netzwerk, in der Regel mit Anbindung an das Internet.
IT	Informationstechnologie.
IT-Anwendung	Programm, das einem bestimmten Zweck, einer Anwendung dient. Ein Anwendungsprogramm ist beispielsweise ein Textverarbeitungs- oder ein Bildbearbeitungsprogramm.
IT-Sicherheitskonzeption	Die IT-Sicherheitskonzeption ist das "zentrale" Dokument im IT-Sicherheitsprozess einer Institution. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Eine IT-Sicherheitskonzeption enthält zunächst die Beschreibung des aktuellen Zustandes eines IT-Verbunds und der auf ihr verarbeiteten Informationen. Der aktuelle Zustand eines IT-Verbunds umfasst neben der Beschreibung der technischen Komponenten, der dort betriebenen IT-Anwendungen und dabei zu verarbeitenden Informationen auch eine Auflistung der vorhandenen

	Schwachstellen, möglicher Bedrohungen und bereits umgesetzter Maßnahmen.
IT-System	Unter einem IT-System werden allgemein Geräte verstanden, mit denen Informationen/Daten verarbeitet werden. Hierunter fallen nicht nur PCs, sondern auch Geräte wie Kopierer, Faxgeräte oder Telefone.
IT-Verbund	Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Netzwerk innerhalb einer Abteilung) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.
LAN	Abkürzung für Local Area Network.
Maximum-Prinzip	Die IT-Anwendung, die bzgl. der Verletzung der Grundwerte die höchsten Schäden verursachen kann. Der Schaden mit den schwerwiegendsten Auswirkungen bestimmt den Schutzbedarf eines IT-Systems, auf dem diese Anwendung läuft.
Patch	Ein Patch (engl.: Flicken) ist ein meist kurzfristig erstelltes Programm, das Fehlfunktionen von bereits veröffentlichter Software beheben soll. Meistens wird der Patch auf der Website des Softwareherstellers zum Download angeboten und ermöglicht es den Anwendern, den Mangel des Programms zu beheben.
Trojanisches Pferd	Nach dem Vorbild aus der griechischen Mythologie benannte Programme. Es handelt sich um Programme, die eine schädliche Funktion enthalten, auf den ersten Blick jedoch völlig harmlos erscheinen.

Anhang B Referenzen

[ITGSHB] IT-Grundschutzhandbuch, http://www.bsi.de/gshb/

[GSHBPROF1] Firmenprofile mittlerer IT Verbund, BSI

[GSHBPROF2] Firmenprofile großer IT Verbund, BSI

[LEITFADEN] Leitfaden IT-Sicherheit, BSI
http://www.bsi.de/gshb/Leitfaden

[BSISIPOL] Musterrichtlinien und Beispielkonzepte, BSI

http://www.bsi.de/gshb/deutsch/musterrichtlinien

[WWW1] http://www.bsi.de/literat/faltbl/sinet.htm

[WWW2] http://www.mittelstand-sicher-im-internet.de/topologien-details.php?22

[WINPT] http://winpt.sourceforge.net/de/index.php

[CRYPT] http://www.tecchannel.de/internet/398/

[MSSEC] http://www.microsoft.com/germany/ms
/security/guidance/modules/secmod225.mspx

[BSIBS] http://www.bsi-fuer-buerger.de/Bildschirmschoner/liesmich.htm

[HDPROT] http://www.cipherbox.de/sicherheit-hdprotect.html

[WIN2KS] http://www.freenet.de/freenet/computer_und_technik/betriebssysteme/windows_2000/win_2000_security/

[DIALER] http://www.bsi.de/av/dialer.htm