Diplomarbeit

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich AGN
(Anwendungen der Informatik in Geistes- und Naturwissenschaften)

Ein IT-Sicherheitskonzept für eine wissenschaftliche Einrichtung

am Beispiel des Fachbereichs Informatik der Universität Hamburg

Teil I
IT-Sicherheitskonzept

Jens Nedon
Fibigerstraße 275
22419 Hamburg

Betreuer:
Prof. Dr. Klaus Brunnstein
Dr. Hans-Joachim Mück

Hamburg
30. September 1999
2. fehlerbereinigte Auflage im Februar 2000

Einleitung

Ziel einer wissenschaftlichen Einrichtung ist es, Forschungsergebnisse zu erschaffen. Für die wissenschaftliche Einrichtung, die Gesellschaft und auch den einzelnen Forscher stellen diese Forschungsergebnisse Werte dar, die es zu schützen gilt. Da auch wissenschaftliche Einrichtungen dabei in zunehmendem Maße auf die Unterstützung durch Informations- und Kommunikationstechnik angewiesen sind, muß auch die Sicherheit der eingesetzten Informationstechnik (IT-Sicherheit) diskutiert werden.

Dabei werden in einer wissenschaftlichen Einrichtung möglicherweise andere Maßstäbe als in einem Unternehmen anzusetzen sein, da die Forschung von einer offenen Kommunikation und dem Austausch von Forschungsergebnissen profitiert. Im Gegensatz dazu wird ein Unternehmen eher darauf zu achten haben, daß möglichst wenig Information aus dem Unternehmen unkontrolliert herausgetragen wird. Hier werden möglicherweise restriktive Maßnahmen ergriffen, die in einer wissenschaftlichen Einrichtung nicht durchsetzbar wären.

Trotz beabsichtigter Offenheit der Kommunikation erfordert die Verarbeitung von Daten in einer öffentlichen Einrichtung, wie z.B. einer Hochschule, die Einhaltung gesetzlicher Vorschriften, z.B. zum Datenschutz oder auch zur Haushalts- und Buchführung, so daß auch hieraus die Notwendigkeit eines Konzeptes zur IT-Sicherheit begründet werden kann.

Es finden sich in der Literatur zahlreiche Quellen und Beispiele darüber, wie die Informationsverarbeitung in einem Unternehmen gesichert werden kann, jedoch wenige Beispiele für IT-Sicherheitskonzepte in wissenschaftlichen Einrichtungen. Es kann daher vermutet werden, daß, gerade in Hochschulen, IT-Sicherheit - wenn überhaupt - nur punktuell praktiziert wird.

Ziel dieser Arbeit soll es sein, zu untersuchen, ob und in welcher Weise sich Vorgehensmodelle zur Erstellung von IT-Sicherheitskonzepten auf wissenschaftliche Einrichtungen anwenden lassen. Dabei werden zunächst Literaturquellen ausgewertet und daraus ein Vorgehensmodell abgeleitet. Dieses soll dann an einem konkreten Beispiel angewendet werden. Als Beispiel dafür dienen die Einrichtungen des Fachbereichs Informatik der Universität Hamburg.

Inhaltsverzeichnis

Tabellenverzeichnis

Kapitel 1

IT-Sicherheitskonzepte in der Literatur

Zu Beginn der Arbeit soll kurz untersucht werden, wie die Begriffe *IT-Sicherheitskonzept*, *IT-Sicherheitspolitik* und auch der Begriff *Policy* in der Literatur verwandt und beschrieben werden. Bereits bei einer ersten Sichtung der Literatur fallen Differenzen auf, die sich z.B. aus einer ungenauen Übersetzung ergeben. Neben einer Klärung der Begriffe sollen dabei auch Vorgehensweisen zum IT-Sicherheitsmanagement untersucht werden.

1.1 IT-Sicherheitsziele und IT-Sicherheitspolitik

Der Begriff der Sicherheitspolitik wird in [Strauß1991] definiert als „ein System gegenseitig und auf die allgemeine Unternehmenspolitik abgestimmten Grundsatzentscheidungen [...], die ein Sicherheitsniveau festlegen, das es zu erreichen gilt, und die sicherheitspolitischen Zielsetzungen bis auf die operationale Ebene einer Unternehmenshierarchie hinunterträgt".

So wird dies auch in [Russell1992] definiert: „A Security Policy is the set of rules and practices that regulate how an organization manages, protects and distributes sensitive information. It's the framework in which a system provides trust." Eine ähnliche Definition wird aus dem Orange Book zitiert: „A security policy states the rules enforced by a system's security features; for example the rules governing whether a particular user is allowed to access a particular piece of information. Obviously, there are more security features in a highly secure system (e.g., a system rated as being B1 or higher) than in a less secure system (e.g., a C1 or C2 system), although at the highest levels there are actually few differences in security features. Instead, there is more *assurance*."

Eine Sicherheitspolitik wird in [Freiss1998] aus dem allgemeinen Begriff der Politik als der „Definition einer Richtung und die Festlegung der Ziele, die man sich setzt" abgeleitet.

Grundlage für eine Sicherheitspolitik sind also Entscheidungen über Ziele, die es hinsichtlich der Sicherheit zu erreichen gilt. Auf diese Ziele gilt es in einem gegebenen Umfeld hinzuwirken. Zu diesem Umfeld gehören Umwelteinflüsse ebenso wie allgemeinpolitische und unternehmenspolitische - höhergeordnete - Zielsetzungen und Handlungen. Die Gesamtheit aus den

Zielentscheidungen und den Maßnahmen zur Zielerreichung, angepaßt auf das aktuelle Umfeld, wird als Sicherheitspolitik verstanden. Diese Sicherheitspolitik ist nach [GMITS1] gültig für alle Untergliederungen der betrachteten Organisation. In diesen Untergliederungen muß die Sicherheitspolitik adaptiert und angepaßt werden. Es können dann Teilpolitiken, im Fall der Informationstechnik diverse IT-System-Sicherheitspolitiken erstellt werden.

In der Literatur finden sich viele Beispiele für IT-Sicherheitspolitiken unterschiedlichen Detailgrades. Wesentlich ist nach [GMITS1], daß Politiken auf höherer Ebene weniger detailliert, dafür adaptierbarer, grundsätzlicher, sein müssen als Politiken auf unterer Ebene. Beispiel hierfür sind die IT-Sicherheitspolitiken auf den unteren Ebenen, die beispielsweise in Firewallumgebungen zu finden sind [Fraser1997, McMillan1998].

Beispiele für Teilpolitiken sind:

1. eine „Dienst-Zugriffs-Politik“ [Goncalves1997]
2. eine „Firewallpolitik“ [Goncalves1997]
3. eine „Beschaffungspolitik, die notwendige oder bevorzugte Sicherheitsmerkmale spezifiziert“ [Fraser1997]
4. „An Access Policy which defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It should provide guidelines for external connections, data communications, connecting devices to an network, and adding new software to systems. It should also specify any required notification messages (e.g., connect messages should provide warnings about authorized usage and line monitoring, and not simply say *Welcome*).“ [Fraser1997]

Nicht in eine IT-Sicherheitspolitik gehören „technische Details“ wie auf ein konkretes, zeitlich befristetes Problem gerichtete Aussagen, die von generalisierenden Aussagen bereits erfaßt sind[1] sowie Fragestellungen, die außerhalb des untersuchten Bereichs liegen, oder - wie [Chapman1997] ausdrückt - die „Probleme anderer Leute.“

1.2 IT-Sicherheitsmanagement und IT-Sicherheitskonzepte

„Ausgangspunkt jeglicher Aktivitäten im Bereich der IT-Sicherheit muß die Erstellung eines IT-Sicherheitskonzeptes sein. Darin werden die schutzbedürftigen Objekte und Werte, die gegen sie gerichteten Bedrohungen und das angestrebte Sicherheitsniveau (IT-Sicherheitsziele) definiert und die organisatorischen Rahmenbedingungen (IT-Sicherheitsrichtlinien) und technischen Maßnahmen (IT-Sicherheitsprozeduren) festgelegt, mit denen die IT-Sicherheitsziele

[1] Viele der zum Datumswechsel 2000 erwarteten Probleme werden generalisierend von Fragen der Verfügbarkeit und Integrität bereits erfaßt.

angestrebt werden."[Kultus1998]

Zunächst müssen die IT-Sicherheitsziele erkundet werden. Dann wird das Umfeld analysiert, um kontraproduktive Einflüsse zu identifizieren und im weiteren Verlauf Maßnahmen zu finden um diese Einflüsse zu verringern und positive Einflüsse zu verstärken. Diese Maßnahmen sind auf ihre Eignung zu bewerten und eine sinnvolle Auswahl zu treffen. Diese Auswahl von Maßnahmen wird als IT-Sicherheitskonzept verstanden.

Der Prozeß der Erstellung, Umsetzung und Weiterentwicklung einer IT-Sicherheitspolitik wird als IT-Sicherheitsmanagement bezeichnet.

1.3 Dokumente zum IT-Sicherheitsmanagement

1.3.1 Die niedergeschriebene IT-Sicherheitspolitik

Die IT-Sicherheitspolitik sollte in einer Weise niedergeschrieben, die eine klare Interpretation der Formulierungen zuläßt und damit die Anwendung der IT-Sicherheitspolitik unterstützt. Sie sollte hierzu nach [McMillan1998][2] die folgenden Charakteristika aufweisen:

1. Sie sollte handhabbar und in einer verständlichen Sprache geschrieben sein (nach [McMillan1998]: „leichtes, verständliches Englisch").

2. Ihre Struktur sollte ein leichtes Auffinden der relevanten Abschnitte ermöglichen.

3. Die einzelnen Abschnitte sollten mit Versionsnummern und Datum versehen sein

4. Um irgendeine Autorität zu besitzen, sollte Sie von den leitenden Personen der betreffenden Organisation als offizielles Referenzdokument angesehen und benutzt werden.

5. Sie sollte nur grundlegende Prinzipien definieren. Es ist zu beachten, daß sich Anforderungen und Ziele auch ändern können. Die IT-Sicherheitspolitik muß dann noch immer Gültigkeit besitzen oder entsprechend angepaßt werden können. Jedoch sollte sie sich im zeitlichen Verlauf nur wenig – besser gar nicht – ändern. Auch [Garfinkel1996] verweist explizit auf diesen Punkt.

6. Die Wortwahl muß sorgfältig erfolgen. Grundlage der IT-Sicherheitspolitik ist es, alle Begriffe präzise zu definieren sowie sicherzustellen, daß die Begriffe auch so verwandt werden, wie sie intendiert sind. Sorgfältig muß die Bezeichnung der Konzepte gewählt werden; jedes Konzept muß präzise genug bezeichnet werden, um dessen Bedeutung verständlich zu machen, aber nicht so präzise, daß bestimmte Technologien damit impliziert oder gar benannt werden.

7. Die IT-Sicherheitspolitik sollte als Teil der Betriebsanweisungen angesehen und erstellt werden.

[2] übersetzt

8. Die IT-Sicherheitspolitik sollte nicht nur definieren, welche Art der Benutzung des IT-Systems akzeptabel ist, sondern auch, welche nicht akzeptiert wird.

9. Die IT-Sicherheitspolitik sollte allen Personen zur Kenntnis gegeben werden, die von ihr betroffen sind. Ein Abschnitt der IT-Sicherheitspolitik sollte die Verteilung regeln.

10. In regelmäßigen Intervallen sowie bei Bedarf sollte die IT-Sicherheitspolitik überarbeitet werden. Auch dies sollte in einem separaten Abschnitt geregelt sein.

11. Die IT-Sicherheitspolitik sollte nicht nur eine Benutzungsanweisung sein, sondern auch die Rechte und Pflichten der Benutzer gegenüber dem Systembetreiber regeln sowie Entscheidungsrichtlinien, Begriffsdefinitionen u.a. enthalten.

1.3.2 Übergeordnete Dokumente

Wird die IT-Sicherheitspolitik aus einer höhergeordneten Politik hergeleitet, so sollten entsprechende Verweise vorhanden und die Dokumente entsprechend zugreifbar sein.

1.3.3 Handbücher

Die in der IT-Sicherheitspolitik festgelegten Verfahren und Handlungsanweisungen sollten in Handbüchern erläutert und ausdetailliert werden. Hier werden dann auch technische Details erläutert, von denen in der IT-Sicherheitspolitik zum Teil abstrahiert wurde.

1.4 Wie entsteht ein IT-Sicherheitskonzept ?

1.4.1 Vorgehensweise nach DIN/ISO/IEC – Leitfaden für das IT-Sicherheitsmanagement

Nach [GMITS2] sind im Rahmen eines Sicherheitsprozesses die folgenden Schritte bzw. Meilensteine anzusetzen:

1. Den ersten Schritt bildet die Entwicklung einer IT-Sicherheitspolitik.

2. Aufgaben und Zuständigkeiten müssen definiert und ein Sicherheitsstab im Unternehmen implementiert werden.

3. Den nächsten Schritt bildet eine Risikoanalyse; hier gibt es als vier Optionen den Ansatz des Grundschutzes, eine informale Analyse, eine detaillierte Risikoanalyse sowie die Kombination daraus. Alle vier Optionen werden in den folgenden Abschnitten erläutert.

4. Nachdem das Risiko und dessen Ursachen identifiziert wurden, können Maßnahmenempfehlungen zur Erreichung eines akzeptablen IT-Sicherheitsniveau ausgesprochen werden. Die Auswahl von Schutzmaßnahmen (engl.: safeguards) richtet sich nach den identifizierten Bedrohungen.

5. Würden die Schutzmaßnahmen implementiert, verbliebe in jedem Fall ein Restrisiko, das ermittelt werden muß. Wenn dieses noch immer nicht tragbar ist, müssen weitere Schutzmaßnahmen ausgewählt werden.

6. Nun müssen IT-System-Sicherheitspolitiken definiert werden, die die IT-Sicherheitspolitik auf das jeweilige IT-Teilsystem anpassen. Hier werden z.B. auch die im vorigen Punkt zum Einsatz vorgeschlagenen Schutzmaßnahmen mit eingebracht.

7. Sind die IT-System-Politiken erarbeitet, wird ein IT-Sicherheitsplan erstellt, in dem alle Aktivitäten verzeichnet und koordiniert werden, die zur Implementation der in den Sicherheitsempfehlungen vorgeschlagenen Schutzmaßnahmen notwendig sind.

8. Nun folgt die Implementationsphase zur Realisierung aller im IT-Sicherheitsplan verzeichneten Schutzmaßnahmen, dies beinhaltet auch die Einarbeitung und Schulung von Personal.

9. Die Nachprüfung soll sicherstellen, daß alle Schutzmaßnahmen korrekt implementiert wurden, mit der Sicherheitspolitik konform sind und daß auch Änderungen am System nicht die Wirksamkeit der Schutzmaßnahmen beeinträchtigen. Die Nachprüfung ist ein dauerhafter Prozeß, der in der Organisation verankert werden muß.

Grundschutz-Ansatz zur Risikoanalyse

Eine Möglichkeit, schnell ein relativ gutes Sicherheitsniveau zu erreichen, ist die pauschale Auswahl geeigneter Sicherheitsmechanismen zur Absicherung gegen die gängigsten Risiken. Die Gründe, sich für dieses Verfahren zu entscheiden, können folgende sein:

- Es werden keine Ressourcen für eine detaillierte Risikoanalyse benötigt; Zeit und Aufwand werden reduziert. Normalerweise werden nur verhältnismäßig geringe Ressourcen für die Auswahl geeigneter Sicherheitsmechanismen benötigt.

- Dasselbe Grundschutzkonzept kann auf eine Reihe von Institutionen und Subeinheiten ohne große Anpassung angewendet werden. Voraussetzung hierfür ist die Ähnlichkeit der Institutionen. Das BSI hat mit dem Grundschutzhandbuch [BSI1998] eine Grundlage geschaffen, auf der nach Identifikation der IT-Systeme nach dem Baukastenprinzip das Schutzkonzept zusammengesetzt werden kann.

Informale Risikoanalyse

Die zweite Möglichkeit der Risikobewältigung ist die Informale Risikoanalyse. Hier können auch externe Sicherheitsberater herangezogen werden. Diese zeigen, basierend auf ihrer Erfahrung, Schwachstellen und Risiken auf und geben Empfehlungen zu Gegenmaßnahmen.

Vorteil dieses Verfahrens ist, daß:

- keine zusätzlichen Fähigkeiten trainiert und keine Verfahren und Konzepte studiert werden müssen, um eine praktikable Absicherung zu realisieren.

Nachteile sind, daß möglicherweise:

- ohne einen strukturierten Ansatz Risiken und Schwachstellen vergessen werden,
- subjektive Meinungen und Sichtweisen, auch Vorurteile erheblich an Bedeutung gewinnen,
- sehr wenig Kritik an Sicherheitsmechanismen geübt wird, die bereits erfolgreich in anderen Kontexten eingesetzt wurden.
- ohne wiederholte gleichartige Risikoanalysen eine zeitliche Anpassung des Systems und der Sicherheitsmechanismen schwer bis unmöglich wird, da eine Analyse kein zweitesmal so wie beim erstem Mal erfolgt.

Detaillierte Risikoanalyse

Eine detaillierte Risikoanalyse ist die aufwendigste Option des Sicherheitsmanagements; hier werden detailliert alle Werte hinsichtlich Schwachstellen und Gefahren untersucht. Als Folge einer detaillierten Risikoanalyse werden, im Gegensatz zur Grundschutzanalyse, Sicherheitsmechanismen in Reaktion auf konkrete Schwachstellen und Risiken ausgewählt.

Diese Methode verursacht einen sehr hohen Aufwand an Zeit, Expertise und Kosten, der Vorteil ist jedoch, daß ein Sicherheitsniveau erreicht wird, das an die wirklichen Bedürfnisse des Systems angepaßt ist. Darüberhinaus profitiert das IT-Sicherheitsmanagement gerade bei sicherheitsrelevanten Systemänderungen von der zusätzlichen Information, die im Rahmen einer detaillierten Risikoanalyse über das System gewonnen wurde.

Im Rahmen der detaillierten Risikoanalyse werden zunächst die Werte identifiziert, die es in der Einrichtung zu schützen gilt. Danach werden Schwachstellen und Bedrohungen identifiziert und der mögliche Schaden an den zu schützenden Werten ermittelt.

Bewertet werden Daten und Information, Dokumentation, Goodwill und Reputation, Kreditwürdigkeit und Ansehen, Hardware, Gebäude, Software sowie der Einsatz von Mitarbeitern und deren Erfahrungen.

Bedrohungen sind beispielsweise Diebstahl, unbefugter Zugriff, Kopie und Veröffentlichung sensitiver Daten, Zerstörung oder die Blockade der Diensterbringung.

„Bestimmte gefährdende Ereignisse treten nur selten auf, und in den meisten Fällen werden auch nur einige wenige Konsequenzen dieser Ereignisse aus der Menge aller denkbaren Folgen eintreten. Daher ist es sinnvoll, die Betrachtung der gefährdeten Ereignisse und ihrer möglichen Konsequenzen um eine Wahrscheinlichkeitsbetrachtung zu erweitern. Bei dieser Betrachtung

werden den verschiedenen Ereignissen und ihren denkbaren Folgen subjektive Wahrscheinlichkeiten zugeordnet. Der Begriff *Risiko* beschreibt die Wahrscheinlichkeit des Eintreffens eines gefährdeten Ereignisses innerhalb eines bestimmten Zeitraums und den damit verbundenen potentiellen Schaden“ [Stelzer1992]

Risiken, die nicht tragbar sind, müssen durch Gegenmaßnahmen gesenkt werden.

Zur Ermittlung des Risikos gibt es zwei Ansätze: die quantitative – oder auch kardinale – und die semiquantitative – oder auch ordinale – Risikoanalyse.

Bei der ***Quantitativen (kardinalen) Risikonalayse*** werden sowohl Eintrittswahrscheinlichkeit als auch Schadenswert in kardinalen Zahlenwerten[3] ausgedrückt. Beide Werte werden multipliziert und ergeben dann einen Erwartungswert für das betreffende Risiko. Werden mehrere Einzelrisiken betrachtet, so kann dieser Einzelerwartungswert additiv zu einem Gesamtrisiko verknüpft werden.

$$\text{Risiko} = \sum Eintrittswahrscheinlichkeit * Schadenswert$$

Die Voraussetzungen sind lt. [Stelzer1992]:

- ein klar abgegrenzter Analysebereich
- die Kenntnis und mathematische Beschreibbarkeit der zugrundeliegenden kausalen Zusammenhänge
- eine ausreichende Menge empirisch abgesicherter Daten (vor allem für die Ermittlung der Eintrittswahrscheinlichkeiten)
- ein nur geringer Einfluß menschlichen Handelns (da als unberechenbar anzusehen) sowie
- die exakte Formulierbarbeit der Schadenshöhe und der Schadensfolgekosten.

Daraus ergeben sich Schwierigkeiten. Der kardinale Ansatz „erzwingt eine präzise numerische Formulierung der Risiken, und zwar selbst in den Fällen, in denen keine verläßlichen Angaben für solche Schätzungen vorliegen.“ [Stelzer1992]

Auch im Hinblick auf Eintrittswahrscheinlichkeiten ergeben sich Schwierigkeiten aufgrund fehlender empirischer Daten, die dann nur geschätzt werden können. Es wird eine Exaktheit vorgetäuscht, die in Wirklichkeit gar nicht vorliegt, auch im Hinblick auf die Robustheit der entstehenden Kennzahl.

So wird ein sehr hoher Schadenswert mit sehr geringer Eintrittswahrscheinlichkeit evtl. gleich bewertet mit einem geringen Schadenswert hoher Wahrscheinlichkeit. Trotzdem ist bei geringfügigster Abweichung der Eintrittswahrscheinlichkeit im ersten Fall mit einer deutlichen

[3] z.B. in Geldbeträgen

Risikoänderung zu rechnen. Zudem können zwei der Kennzahl nach gleiche Risiken völlig unterschiedliche Sachverhalte zugrundeliegen, die möglicherweise auch völlig anders von den verantwortlichen Personen gesehen und behandelt werden wollen.

„Die Beschreibung des Risikos durch eine einzige Risikokennziffer ist zwar prägnant, gleichzeitig wird aber auch der zugrundeliegende Informationsgehalt verringert." [Stelzer1992]

Der Kardinale Ansatz erweist sich damit als aufwendig und trotz des hohen Analyseaufwandes instabil, da exakte statistische Daten für Schadenshöhe und Eintrittswahrscheinlichkeit vorliegen müssen. Häufig fehlt diese Datenbasis. Außerdem lassen sich viele Schadenspotentiale nicht in kardinale Metriken einordnen.[4]

In der ***Semiquantitativen (ordinalen) Risikoanalyse*** werden Schadenshöhe und Eintrittswahrscheinlichkeiten nicht exakt formuliert, sondern Klassen zugeordnet. Die Schadenspotentiale können z.B. den Schadenskategorien *unter 50 Euro*, *50 bis 500 Euro*, *über 500 Euro* zugeordnet werden. Analog geschieht dies mit der Eintrittswahrscheinlichkeit. Anschließend werden diese Klassen miteinander verknüpft, z.B. die Ordinalzahl 3 (Schadenskategorie 3) mit der Ordinalzahl 2 (Eintrittswahrscheinlichkeitsklasse 2).

$$\text{Risiko} = \textit{Eintrittshäufigkeitsklasse} \text{ verknüpft mit } \textit{Schadenskategorie}$$

Interessant an diesem Ansatz ist hier, daß nicht mehr kardinale Werte für Schäden angegeben werden müssen, sondern hier auch subjektiv höherwertige Schäden als Schadenskategorie erfaßt werden können (z.B. menschliche Verluste bei einem Unfall)

Voraussetzung ist hier nach [Stelzer1992] die Bildung geeigneter Klassen und deren aussagekräftige Abgrenzung. Zu beachten ist jedoch, daß

- die Klassifikation zu oberflächlichen und undurchdachten Angaben verführen kann,
- unterschiedliche Risiken in ihrer Höhe nur bedingt verglichen werden können und
- die Verknüpfung ordinaler Zahlen grundsätzlich problematisch sein kann; insbesondere in keiner Weise einen Wert zum Ergebnis hat, der als kardinale Zahl in weitere Berechnungen einfließen kann.

Gerade aus dem letzten Punkt ergibt sich die Gefahr der Fehlinterpretation der in der ordinalen Risikoanalyse ermittelten Risikoklasse.

Ein Beispiel für eine Vorgehensweise nach diesem Modell bietet das IT-Sicherheitshandbuch des BSI [ITSHB1992]. das Verfahren ist im Abschnitt 2.4.2 beschrieben.

[4] Ein Beispiel hierfür sind menschliche Verluste

Kombinierter Ansatz zur Risikoanalyse

Grundschutzanalyse, Detaillierte Risikoanalyse und Informale Analyse können nach [GMITS3] kombiniert werden.

Die informale Risikoanalyse wird dabei oft als eine Voranalyse für ein Grundschutzkonzept (z.B. nach [BSI1998]) eingesetzt, das gegen gängige Risiken aus Kostengründen mit Pauschalverfahren schützen soll und besonderen Einsatz und Kosten auf die Abwendung größerer Risiken konzentriert.

In einem ersten Schritt wird das IT-System grob analysiert und die Teilsysteme klassifiziert in solche, für die Grundschutz realisiert werden soll, und jene, für die eine detaillierte Risikoanalyse unternommen wird. Diese Methode reduziert die Kosten, die bei einer detaillierten Risikoanalyse anfallen würden und gestattet gleichzeitig eine grundlegende Absicherung des Systems gegen gängige Risiken.

Vorteile sind nach [GMITS3] auch folgende:

- Die grobe Mini-Risikoanalyse erzeugt eine höhere Akzeptanz bei Entscheidern hinsichtlich der hohen Kosten für detaillierte Analysen; diese werden aufgrund der in der Voranalyse gesammelten Informationen besser begründet.

- Es wird auch ein Organisationsplan in der ersten Phase der Analyse erstellt; dieser kann als eine gute Planungsgrundlage für das Unternehmen dienen.

- Ressourcen und Geld werden dort eingesetzt, wo sie wirklich notwendig sind; insbesondere werden keine überflüssigen Risikoanalysen durchgeführt, die doch nur zum Grundschutzniveau führen würden. Hochschutzbedürftige Systeme können schnell identifiziert und analysiert werden.

Nachteilig ist, daß:

- möglicherweise durch die grobe Risikoanalyse zu Beginn hochschutzbedürftige Systeme nicht als solche erkannt werden und nur mit Grundschutz versehen werden.

- dadurch, daß auf die Anwendung des IT-Grundschutzes in den höheren Schutzklassen gänzlich zugunsten der Risikoanalyse verzichtet wird, dort zwar IT-Sicherheitsmaßnahmen ausgewählt werden, die zu den Bedrohungen passen, in den niedrigeren Schutzklassen jedoch mit der Pauschalmethode möglicherweise schwerere Schutzmaßnahmen installiert werden (die gar nicht nötig wären), paradoxerweise in den niedrigen Schutzklassen ein aufwendigerer Schutz besteht als in den höheren Schutzklassen.

Trotzdem bietet der kombinierte Ansatz nach [GMITS3] das derzeit beste Kosten/ Nutzenverhältnis hinsichtlich des Risikomanagements.

1.4.2 Grundschutzansatz des BSI

Ein Beispiel für den in [GMITS2] beschriebenen kombinierten Ansatz bietet das Grundschutzkonzept [BSI1998] des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Risikobewertung vollzieht sich in zwei Schritten. Für die Abgrenzung eines Grundschutzniveaus werden zunächst die IT-Systeme hinsichtlich des potentiellen Schadens in vier Stufen klassifiziert, dann die in den beiden unteren Stufen eingordneten IT-Systeme mit pauschalen Maßnahmen gesichert (Grundschutz)[5], während höhere Sicherheitsniveaus eine detaillierte Risikoanalyse erzwingen.

Es kann hierbei geschehen, daß die zu treffenden Maßnahmen schließlich nur wenig über dem Grundschutzniveau liegen, jedoch kann nach dem derzeitigen Konzept nur von Grund auf evaluiert, nicht etwa auf dem Grundschutzniveau aufgesetzt werden. Um diese Schwäche des Grundschutzkonzeptes nach [BSI1998] zu überwinden, wird derzeit unter dem Begriff „Grundschutz plus X“ das Verfahren weiterentwickelt, jedoch ist eine derartige Methode bislang nicht einsetzbar.

1.4.3 Vorgehensmodell nach einer Studie zur Sicherheit in Verwaltungs- und Kliniknetzen

In einer Studie des Bayerischen Staatsministeriums für Unterricht, Kultus, Wissenschaft und Kunst [Kultus1998] wird ein Vorgehensmodell vorgeschlagen. Es besteht aus den Schritten

1. Definition der IT-Sicherheitsziele
2. Ableitung von IT-Sicherheitsrichtlinien sowie der
3. Ableitung von IT-Sicherheitsprozeduren

Definition der IT-Sicherheitsziele:
Die Analyse der in die Informationsverarbeitung involvierten Objekte sowie der gegen sie gerichteten Bedrohungen vollzieht sich nach [Kultus1998] nach folgendem Schema:

1. Ermittlung der gegebenenfalls bedrohten, zu schützenden Objekte und Werte
2. Analyse der möglichen Bedrohungen hinsichtlich der Vertraulichkeit[6], Integrität[7], Verfügbarkeit[8], Nachweisbarkeit bzw. Nichtabstreitbarkeit[9] und Ordnungsmäßigkeit[10]

[5] nach dem Baukastenprinzip gibt es für Klassen von IT-Systemen wie Faxgeräte, Netzwerke, Einzelplatz-PCs vorgefertigte Maßnahmenkataloge

[6] Die Daten und ihre Übertragungswege sind zu schützen

[7] Die Daten sind vor Veränderung, Verlust oder Zerstörung zu schützen

[8] Die IT-Systeme und -dienste müssen in der vorgesehenen Leistungsfähigkeit ohne Beeinträchtigung zur Verfügung stehen

[9] Die Urheber jeglicher Aktionen im IT-System müssen zu jeder Zeit identifizierbar und nachweisbar sein

[10] Die Nutzung der IT hat nur durch dazu Autorisierte und nur gemäß der vorgegebenen Bestimmung zu geschehen

3. Risikoabschätzung möglicher Bedrohungen
   (Abschätzung der Eintrittswahrscheinlichkeit sowie der möglichen Schadenshöhe)

4. Kosten/Nutzen-Analyse für den Aufwand an Sicherheitsmaßnahmen.

Definition der IT-Sicherheitsrichtlinien:
„Die IT-Sicherheitsrichtlinien legen die Rahmenbedingungen und Regeln fest, nach denen eine an den definierten Sicherheitszielen orientierte Informationsverarbeitung zu erfolgen hat. Sie beschreiben insbesondere die Rechte, Pflichten und zulässigen Verhaltensweisen der Benutzer sowie der Systemadministratoren der einzelnen IT-Systeme und der diese verbindenden Netze. Sie sorgen darüber hinaus für eine Klassifizierung der anfallenden Daten im Hinblick auf ihre Schutzwürdigkeit und schreiben verbindlich vor, welche Maßnahmen zur Sicherstellung ihrer Integrität und Vertraulichkeit durchzuführen sind. Außerdem enthalten sie ein Konzept für die Reaktion auf eingetretene Sicherheitsvorfälle (Schadensereignisse) sowie eine Vorgehensweise für die kontinuierliche Fortschreibung des IT-Sicherheitskonzepts einschließlich der Sicherheitsüberprüfung und der Beseitigung von Schwachstellen.“ [Kultus1998]

Definition der IT-Sicherheitprozeduren:
„In Abhängigkeit von dem jeweiligen Stand der Informationstechnologie werden konkrete technische Verfahren und Prozeduren zur Umsetzung der Sicherheitsrichtlinien und zur Realisierung des angestrebten Sicherheitsniveaus festgelegt, die vor allem in den folgenden Bereichen zum Einsatz gelangen:

- Authentifizierung: gegenseitiger Nachweis der Identität der in einen konkreten Informationsverarbeitungsprozeß involvierten Personen und Systeme; Kontrolle des eingesetzten Authentifizierungsmediums (z.B. Chipkarte) gegen Mißbrauch, Verlust, Vergeßlichkeit

- Zugangsregelung: zentrale Zugangskontrolle über alle Systeme und Applikationen einer Einrichtung (zentraler Berechtigungsserver und Single-Signon); Zugangsregelung zu Teilen einer Anwendung; Zeitkontrolle bestehender Client/Server-Verbindungen auf Inaktivität

- Zugriffskontrolle: Kontrolle der unterschiedlichen Privilegien für den Zugriff auf Dateien oder einzelne Datenelemente

- Bereitstellung zertifizierter Software: zentrale Auslieferung von zertifizierter und beglaubigter Software („trusted software“)

- Abschottung von Subnetzen: Einsatz von Firewalls zur Absicherung von Subnetzen

- Verschlüsselung und Signierung von Daten: Verschlüsselung besonders schützenswerter oder gefährdeter Daten bei der Speicherung und/oder Übertragung; Erstellung signierter Dokumente (Notariatsfunktion); Ermöglichung von (rechts-)verbindlichen elektronischen Vorgängen; Verwaltung und Distribution der geheimen und öffentlichen Schlüssel (key management)

- Sicherheitsmanagement und -überwachung: laufende Dokumentation und Kontrolle aller relevanten Aktionen im IT-Gesamtsystem; gezielte Überprüfung der Wirksamkeit der getroffenen Sicherheitsmaßnahmen“ [Kultus1998]

1.4.4 Revision nach den Grundsätzen ordnungsmäßiger Datenverarbeitung

Ein interessanter Weg wird in der Revision von IT-Systemen gegangen. Hier sind in der Vergangenheit Grundsätze für eine Ordnungsmäßigkeit entwickelt worden, die eine Methodik für die Begutachtung eines Systems und eine Vergleichbarkeit mit einem Idealbild erlauben. Ein sehr bekanntes Beispiel sind die „Grundsätze ordnungsmäßiger Buchführung“, die in der Buchhaltung eine gesetzliche Grundlage bilden.

[Hahn1990] definiert diese folgendermaßen: „Eine Buchführung kann im allgemeinen als ordnungsmäßig gelten, wenn in ihr die formalen und/oder materiellen Grundsätze befolgt werden:

- Die Buchführung muß vollständig, richtig, zeitgerecht und geordnet sein (§ 239 Abs. 2 HGB);
- sie muß klar und übersichtlich sein (§ 243 Abs. 2 HGB);
- sie darf nicht in chiffrierter Form vorgenommen werden und keine Zeichen enthalten, deren Bedeutung nicht eindeutig festliegt (§ 239 Abs. 1 HGB);
- die verwendete Sprache soll Deutsch sein, die Wertangaben in Deutscher Mark erfolgen (§ 244 HGB);
- der Kassenbestand soll täglich festgehalten werden, Wareneingänge und Warenausgänge müssen (von gewerblichen Unternehmen) gesondert aufgezeichnet werden;
- alle Buchungen müssen aufgrund von vorliegenden Belegen nachvollziehbar sein;
- spätere Veränderungen in der Buchführung müssen den ursprünglichen Inhalt erkennen lassen; deshalb dürfen auch keine Zwischenräume unausgefüllt bleiben, die später in Manipulationsabsicht ausgefüllt werden könnten;
- Aufbewahrungspflicht der Bücher 10 Jahre, der Buchungsunterlagen 6 Jahre über den Schluß des betreffenden Kassenjahres ahinaus (§ 257 Abs. 4 HGB i.V.m. Abs. 1 und 5);“

Diese Grundsätze sind in der Vergangenheit vielfach erweitert und interpretiert worden, bilden jedoch die Grundlage für die Erfüllung der eigentlichen Absicht der Revision, zu ermöglichen, nämlich dem Zweck, „die Buchhaltung so zu gestalten, daß sie einem ’*Sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des*

Unternehmens vermitteln kann' (§ 238 Abs. 1 Satz 2 HGB)" [Hahn1990].

Aus diesem Begriff der Ordnungsmäßigkeit in der Buchführung wird von [Schuppenhauer1998] ein Begriff der Ordnungsmäßigkeit in der Datenverarbeitung hergeleitet. Hier werden die oben zitierten Grundsätze ordnungsmäßiger Buchhaltung in einer Form abgebildet und weiterentwickelt, daß sie in der DV-Welt anwendbar sind. Allgemein formuliert sind dies die folgenden Anforderungen nach [Schuppenhauer1998]:

- Ordnungsmäßige DV-Buchführung – Grundsatz der Auftragsbindung
- Ordnungsmäßige Führung digitaler Beleg- und Buchnachweise – Grundsatz der Urschrifttreue
- Ordnungsmäßige DV-Arbeitsabwicklung – Grundsatz der Kontrollierbarkeit
- Ordnungsmäßige DV-Dokumentation – Grundsatz der Transparenz
- Ordnungsmäßige Organisation des DV-Bereiches – Grundsatz der Funktionssicherheit

Der letzte der angesprochenen Grundsätze – der Grundsatz der Funktionssicherheit – definiert ein Idealbild für die IT-Sicherheit, das Anforderungen an IT-Systeme definiert, die nach [Schuppenhauer1998] aus den folgenden Sicherheitsmerkmalen bestehen:

- Verfügbarkeit:
  sichere räumliche Unterbringung
  ständige Betriebsbereitschaft
  volle Betriebssicherheit
- Risikoabdeckung:
  ausreichender Versicherungsschutz
- Manipulationssicherheit:
  klare personelle Funktionstrennung
  Bedienungssicherheit
  klare Arbeitsanweisungen
- Datensicherung:
  Datenbeständeschutz (auch im Katastrophenfall)
  schnelle Rekonstruierbarkeit
- Sicherheitskontrolle:
  Überwachung der Dokumentations- Kontroll- und Sicherheitsmaßnahmen durch unabhängige Stellen

Aus diesem Idealbild heraus ist eine Methodik für eine DV-Prüfung entwickelt worden. Diese basiert u.a. auf der Prüfung anhand umfangreicher Fragenkataloge und Checklisten sowie der

anschließenden Bewertung der Ergebnisse.

Für ein IT-Sicherheitskonzept in einer wissenschaftlichen Einrichtung könnte diese Prüfmethodik angewendet werden, um einen Überblick über bestehende IT-Sicherheitsmerkmale an dieser Einrichtung zu erhalten.

Kapitel 2

Vorgehensmodell für die Erstellung von IT-Sicherheitskonzepten in wissenschaftlichen Einrichtungen

In diesem Abschnitt soll nun ein Vorgehensmodell für die Erstellung von IT-Sicherheitskonzepten in wissenschaftlichen Einrichtungen abgeleitet werden, das in den darauffolgenden Kapiteln auf den Fachbereich Informatik der Universität Hamburg angewendet wird. Damit soll gezeigt werden, wie ein IT-Sicherheitskonzept in einer wissenschaftlichen Einrichtung entstehen würde und welche Konsequenzen sich aus der Anwendung der im vorigen Kapitel beschriebenen Verfahren ergeben.

Das Vorgehensmodell wird aus den in den folgenden Abschnitten beschriebenen Phasen bestehen.

2.1 Abgrenzung der Einrichtung

Zunächst muß die betrachtete Einrichtung beschrieben und abgegrenzt werden. Informal müssen die Einrichtung, ihr Zweck, ihre Arbeit und ihre Umweltbeziehungen beschrieben werden.

2.2 Implementation eines IT-Sicherheitsmanagement-Teams in der Einrichtung

Ein IT-Sicherheitsmanagement- Team hat nach [BSI1998] die hauptsächliche Aufgabe, „die IT-Sicherheitsziele festzulegen und Verfahren (IT-Sicherheitspolitik) zu definieren, um diese Ziele zu erreichen, für die Implementation der Sicherheitsmaßnahmen zu sorgen sowie die Umsetzung zu überwachen“. Dem IT-Sicherheitsmanagement-Team sollten nach [BSI1998] angehören:

- ein Mitglied mit Expertenwissen im Bereich IT-Sicherheit sowie Erfahrung mit Organisation und Verwaltung

- der IT-Sicherheitsbeauftragte
- ein Vertreter aus dem IT-Koordinierungsausschuß sowie
- ein Vertreter der Nutzer

2.3 Bestimmung der IT-Sicherheitsziele

Als erster Schritt zur Bestimmung der IT-Sicherheitsziele soll eine Befragung der Verantwortlichen in den Fachbereichseinrichtungen über die in ihrem Bereich anliegenden Sicherheitsziele stattfinden, um herauszufinden, welchen Stellenwert die IT-Sicherheit in der entsprechenden Fachbereichseinrichtung hat, welche Anforderungen hinsichtlich der Sicherheitsmerkmale Vertraulichkeit, Integrität und Verfügbarkeit bestehen, ob es bereits eine IT-Sicherheitspolitik gibt und welche technischen Maßnahmen zur Umsetzung dieser IT-Sicherheitspolitik ergriffen werden.

In Anlehnung an den Fragenkatalog des BSI-Grundschutzhandbuches [BSI1998] werden Fragen aus den folgenden Kategorien gestellt, der Fragenkatalog befindet sich im Anhang.

1. **Welches sind die IT-Sicherheitsziele?**
   Hier soll zunächst evaluiert werden, welche Bedeutung die befragte wissenschaftliche Einrichtung der eingesetzten Informationstechnik beimißt. Dazu gehören die Ziele, die mit dem IT-Einsatz verfolgt werden, woraus sich danach Anforderungen an Sicherheitskriterien herausarbeiten lassen.
   (a) Welche Bedeutung hat der Einsatz der IT für die wissenschaftliche Einrichtung ?
   (b) Welche Ziele verfolgt die wissenschaftliche Einrichtung mit dem Einsatz der IT ?
2. **Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist ?**
   Vertraulichkeit ist ein Sicherheitsmerkmal, dessen Schutzbedarf zu ermitteln und zu begründen ist. Hierzu werden Fragen zu gesetzlichen Auflagen gestellt sowie solche nach der betrieblichen Notwendigkeit oder Politik der Vertraulichkeit.
3. **Hängen wesentliche Entscheidungen von der Richtigkeit und Aktualität – Integrität – von Informationen ab, die mit IT verarbeitet werden ?**
   Die Abstufung der Sicherheitsanforderungen hinsichtlich der Integrität von Daten, deren Verarbeitung und Aufbereitung soll mit den folgenden Fragen erörtert werden. Auch hier soll die Integritätsforderung aus gesetzlichen, vertraglichen, wirtschaftlichen sowie politischen Anforderungen begründet werden.
4. **Gibt es wichtige und/oder sehr wichtige Aufgaben in der wissenschaftlichen Einrichtung, die nur mit Unterstützung von IT erledigt werden können? Gibt es Massenaufgaben in der wissenschaftlichen Einrichtung, deren Erledigung**

nur mit IT-Einsatz möglich ist?
Hier soll die Anforderung an die Verfügbarkeit, ggf. Wiederherstellbarkeit der Informationsverarbeitung erörtert werden.

Das BSI [BSI1998] empfiehlt hier, zunächst von den Aufgaben der gesamten Organisation auszugehen und die dafür eingesetzten IT-Systeme zu klassifizieren sowie ein anzustrebendes Schutzniveau auszuloten, das dann bei Bedarf detaillierter untersucht werden kann.

2.4 Risikoanalyse

In Anlehnung an [GMITS3] wird zunächst eine informale Analyse durchgeführt und die IT-Anwendungen in Sicherheitsniveaus eingeordnet. Es werden hier die IT-Anwendungen nach ihren Sicherheitsanforderungen klassifiziert. Für die höherklassifizierten Anwendungen wird dann eine detaillierte Risikoanalyse, wie im Kapitel 1.4.1 beschrieben, durchgeführt. Hierzu kann als Leitfaden das IT-Sicherheitshandbuch des BSI [ITSHB1992] dienen.

Für die restlichen Anwendungen sollte ein Grundschutz realisiert werden. Dazu kann als Leitfaden das Grundschutzhandbuch des BSI [BSI1998] verwendet werden.

2.4.1 Grundschutzanalyse

Definition von IT-Sicherheitsniveaus
Es ist notwendig, den Schutzbedarf für die evaluierten Einrichtungen festzustellen, um die weitere Betrachtung der Einrichtungen und IT-Systeme hierauf abzustimmen.

Die Schwierigkeiten bei der Festlegung dieser IT-Sicherheitsniveaus sind, wie bereits beschrieben, folgende:

- Wenn dieser Schwellwert zu hoch angesetzt wird, werden Sicherheitsmechanismen in Anwendungen implementiert, die einer Bedrohung im Ernstfall nicht standhalten würden, es würde also eine Unterdeckung eintreten.
- Ist der Schwellwert zu niedrig angesetzt, so werden unnötig viele Anwendungen detailliert untersucht, obwohl sie dieses eventuell gar nicht benötigen.

Es ist also notwendig, diese IT-Sicherheitsniveaus sorgfältig auszuwählen. Als Beispiel hierfür sind im BSI-Grundschutzhandbuch [BSI1998] die folgenden vier IT-Sicherheitsniveaus angegeben:

1. **Niedriges Sicherheitsniveau**
   „Vertraulichkeit von Informationen ist nicht gefordert. Fehler können toleriert werden, solange sie die Erledigung der Aufgabe nicht völlig unmöglich machen. Dauernder Ausfall ist zu vermeiden, längere Ausfallzeiten sind jedoch hinnehmbar.
   Insgesamt gilt: Schäden haben nur eine unwesentliche Beeinträchtigung der wissenschaftlichen Einrichtung zur Folge.“

2. **Mittleres Sicherheitsniveau**
   „Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muß gewährleistet sein. Kleinere Fehler können toleriert werden, Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein. Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.
   Insgesamt gilt: Schäden haben Beinträchtigungen der wissenschaftlichen Einrichtung zur Folge.“

3. **Hohes Sicherheitsniveau**
   „Der Schutz vertraulicher Informationen muß hohen gesetzlichen Anforderungen genügen und in sicherheitskritischen Bereichen stärker ausgeprägt sein. Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein. In zentralen Bereichen der wissenschaftlichen Einrichtung laufen zeitkritische Vorgänge oder es werden dort Massenaufgaben wahrgenommen, die ohne IT-Einsatz nicht zu erledigen sind; es können nur kurze Ausfallzeiten toleriert werden.
   Insgesamt gilt: Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der wissenschaftlichen Einrichtung ein; Schäden haben erhebliche Beeinträchtigungen der wissenschaftlichen Einrichtung selbst oder betroffener Dritter zur Folge.“

4. **Maximales Sicherheitsniveau**
   „Der Schutz vertraulicher Informationen muß gewährleistet sein und in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen genügen. Die Informationen müssen im höchsten Maße korrekt sein. Die zentralen Aufgaben der wissenschaftlichen Einrichtung sind ohne IT-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel.
   Insgesamt gilt: Der Ausfall der IT führt zum totalen Zusammenbruch der wissenschaftlichen Einrichtung oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.“

Nach dem Grundschutzhandbuch würden für niedriges und mittleres Schutzniveau eine Grundschutzanalyse und für die darüberliegenden hohen und maximalen Schutzniveaus eine detaillierte Risikoanalyse durchzuführen sein.

Die Auswahl von Sicherheitsmaßnahmen vollzieht sich dabei mit pauschalen Methoden nach einem Verfahren des BSI, bei dem für Objekte (z.B. Telefon, Fax, PC) und auch für die Organisation selbst jeweils eine pauschale Liste von Schutzmethoden definiert wird.

2.4.2 Detaillierte Risikoanalyse

Für die IT-Systeme, für die hoher oder maximaler Schutzbedarf gesehen wird, würde dann eine Detaillierte Risikoanalyse durchzuführen sein. Eine solche Detaillierte Risikoanalyse, z.B. nach dem IT-Sicherheitshandbuch des BSI [ITSHB1992], ist ein vierstufiges Verfahren. Die vier Stufen, die selbst noch weiter ausdetailliert werden, sind:

1. **Ermittung der Schutzbedürftigkeit**
   Hier findet eine Abgrenzung des zu untersuchenden IT-Systems statt. Es werden die IT-Anwendungen und die vom IT-System verarbeiteten Informationen erfaßt und hinsichtlich ihres Schadenspotentials bewertet. Schließlich wird festgestellt, welche IT-Anwendungen oder Informationen überhaupt schutzbedürftig sind. Die Bewertung vollzieht sich anhand einer fünfteiligen Werteskala (unbedeutend bis existenzgefährdend), die bei Bedarf auch um eine sechste Klasse (lebensgefährdende oder menschheitsgefährdende Katastrophe) erweitert werden kann.

2. **Bedrohungsanalyse**
   Es werden alle möglichen und vorstellbaren Bedrohungen ermittelt, die auf die schutzbedürftigen Anwendungen und Informationen einwirken könnten. Dazu werden die IT-Anwendungen und alle dazu notwendigen Objekte untersucht. Hinsichtlich der Bedrohungen hilft das IT-Sicherheitshandbuch mit einer Checkliste, auch alle denkbaren Bedrohungen zu beachten. Es wird zwischen Grundbedrohungen und konkreten Bedrohungen unterschieden.
   Als Grundbedrohungen werden die Bedrohung der Verfügbarkeit, der Integrität und der Vertraulichkeit untersucht. Eine Untersuchung der Verbindlichkeit oder der Nichtabstreitbarkeit findet hier nicht statt.
   Nachdem die Grundbedrohungen den Objekten zugeordnet wurden, werden Schwachstellen und bisherige Schutzmaßnahmen im IT-System untersucht und unter diesem Eindruck reale Bedrohungen und Objekte einander zugeordnet und bewertet. Konkrete Bedrohungen beziehen sich auf die acht Bereiche Infrastruktur, Hardware, Datenträger, Paperware, Software, Anwendungsdaten, Kommunikation und Personen.

3. **Riskoanalyse**
   Es wird sodann untersucht, in welcher Weise sich die Bedrohungen auf die Objekte und damit die IT-Anwendungen und Informationen auswirken. Dazu werden Schadenswerte und vermutete Eintrittshäufigkeiten gegenübergestellt. Es muß entschieden werden, welche Schadenswerte und Häufigkeiten ein tragbares und welche ein untragbares Risiko darstellen.

4. **Erstellung des Sicherheitskonzepts**
   Die untragbaren Risiken sind dann mittels geeigneter Schutzmaßnahmen zu senken bzw. es sind für den Schadensfall Vorkehrungen zu treffen. Dies wird im Abschnitt 2.5 erläutert.

In der ersten Stufe findet eine Überschneidung mit dem Grundschutzansatz statt, da dort bereits diese Untersuchung geleistet wurde. Es sollen hier die IT-Anwendungen und Informationen detailliert untersucht werden, die in der Grundschutzanalyse mit einem hohen Schutzbedarf gekennzeichnet worden sind.

Die in der dritten und vierten Stufe erreichten Ergebnisse und die im Rahmen der Grundschutzanalyse erreichten Ergebnisse müssen nun wieder zusammengebracht werden. Dies geschieht in den nachfolgenden Abschnitten.

2.5 Risikobewertung

Welches Risiko ist akzeptabel und welche Werte sind bereits angemessen geschützt?
Auf welches Niveau soll das gesenkt werden, welche Werte sollen besonders geschützt werden?

Diese beiden Fragen müssen im Rahmen der Risikobewertung beantwortet werden. Manche Risiken müssen oder können akzeptiert werden, das Risiko wird dann meist bereits als Kosten eingeplant, Betriebe können hierfür Rückstellungen bilden, wissenschaftliche Einrichtungen in der Regel nicht. Existenzielle Risiken jedoch müssen gesenkt, besser noch ausgeschlossen werden.

Die Bewertung muß ganzheitlichen Charakter haben, da hier nicht nur ein isoliertes IT-System betrachtet werden soll, sondern Gefährdungen und Risiko hinsichtlich der gesamten IT der Organisation untersucht werden sollen.

2.6 Maßnahmenkatalog

In einem Maßnahmenkatalog sollen als Empfehlung eine Auswahl von Schutzmaßnahmen (engl.: safeguards) aufgeführt werden, die aufgrund der Risikoanalyse und -bewertung als geeignet angesehen werden, diejenigen Risiken zu senken, die als untragbar angesehen werden.

Da das Risiko sowohl von der Eintrittswahrscheinlichkeit als auch dem Schadenswert abhängt, ergeben sich hier zwei Möglichkeiten der Beeinflussung. Die Eintrittswahrscheinlichkeit eines Schadens kann oftmals mit technischen Maßnahmen (z.B. Zugriffskontrolle) beeinflußt werden. Die Schadenshöhe erfordert neben technischen (z.B. Redundanz, Verschlüsselung) oftmals zusätzlich organisatorische Maßnahmen. Durch eine Verschlüsselung der Daten kann z.B. im Falle eines Einbruchs der Schadenswert begrenzt werden, sofern ein externes (ebenfalls verschlüsseltes) Backup vorhanden ist. Der Einbruch selbst ist dadurch nicht verhindert worden, die Eintrittswahrscheinlichkeit hierfür könnte jedoch durch technische Maßnahmen gesenkt werden (Türsicherung). Die Trennlinie zwischen Schadenswertbegrenzung und Eintrittswahrscheinlichkeitssenkung ist jedoch fließend.

Um das angestrebte IT-Sicherheitsniveau bzw. die angestrebten IT-Sicherheitsziele zu erreichen, müssen als Reaktion auf die festgestellten Bedrohungen Maßnahmen ergriffen werden, die diesen Bedrohungen entgegenwirken. Diese Maßnahmen dienen entweder dazu, die Schadenshäufigkeit oder das Schadenspotential zu senken. Jede Maßnahme wird mit Kosten verbunden sein, die in Relation zu ihrem Nutzen bzw. zur möglichen Schadenshöhe gesetzt werden müssen. Aus den möglichen Maßnahmen werden nun die effektivsten ausgewählt. Diese Maßnahmen werden dann in einem Maßnahmenkatalog zusammengefaßt.

Die ausgewählten Maßnahmen können z.B. die folgenden Bereiche umfassen:

1. **Kaufrichtlinien** enthalten notwendige und bevorzugte Sicherheitsmerkmale von Hard-

ware und Software

2. **Richtlinien und Maßnahmen zum Schutz von Email und privaten Daten**, z.B. auch Monitoring-, Log- und Auditdaten

3. **Zugriffspolitik**
   Rechte und Verantwortlichkeiten der wissenschaftlichen Einrichtung und der Benutzer, z.B. in Bezug auf die Ressourcennutzung (CPU, Software, Sourcecode), den Zugriff auf Daten, die Verwendung von und Verschwiegenheit bei kritischen Daten, Copyright und -left, Rechte an privaten Daten und Email sowie Ausnahmen, unter denen auf diese Daten von z.B. Operateuren, Management zugegriffen werden kann. Das betrifft auch externe Verbindungen, Email, FTP, Telnet, ... von innen nach außen und umgekehrt sowie die Installation und Änderung von Geräten und Software.

4. **Authentifikation** - Paßwort-Restriktionen, Remote-Login-Authentikation und Hilfsmittel

5. **Verfügbarkeit** - Definition von Backup und Recovery-Maßnahmen, Administrationszeiten mit verminderter Verfügbarkeit sowie Kontaktinformation bei Problemen

6. **Wartung und Pflege** sowie Kontrolle, z.B. bei Fernwartung

7. **Fehlermeldung, Angriffserkennung** - Was muß wem gemeldet werden? Ist eine anonyme Meldung möglich?

8. **Notfallmaßnahmen** - Notfallerkennung, Meldung und Maßnahmen zur Benachrichtigung, zur Backup- und Logdatei-Rettung und zur Netzisolation; jedoch auch die Definition von Zuständigkeiten und Richtlinien zur Beweissicherung und Einleitung der Strafverfolgung, falls ein Angreifer identifiziert werden kann.

9. **Weitergehende, unterstützende Information** - Gesetzliche Vorschriften, Handlungsanweisungen und Prozeduren für Benutzer, Operateure sowie das Management

Unterstützung bieten hier sowohl das IT-Grundschutzhandbuch [BSI1998] als auch das IT-Sicherheitshandbuch [ITSHB1992] des BSI mit umfangreichen Handlungsvorschlägen. Zu beachten ist in jedem Fall auch die Höhe der Kosten, die bei Umsetzung der Maßnahmen entstehen würden. Sie müssen in angemessenem Verhältnis zur Schadenshöhe stehen, vor deren Eintritt sie schützen sollen.

2.7 Ermittlung des Restrisikos

Es ist zu untersuchen, wie hoch nach Umsetzung der vorgeschlagenen Maßnahmen das Restrisiko wäre. Ist es nun akzeptabel und tragbar? Falls ja, können die Maßnahmen jetzt umgesetzt werden. Falls nein, müssen weitere Maßnahmen zur Risikosenkung ergriffen werden.

2.8 Erarbeitung von IT-System-Sicherheitskonzepte

Nun müssen Teil-Sicherheitskonzepte erarbeitet werden, die auf das jeweilige IT-Teilsystem zugeschnitten sind und sich dennoch in ein Gesamtkonzept einfügen. Die Teil-Sicherheitskonzepte besitzen einen höheren Detailgrad als die grundlegende Sicherheitspolitik. Hier fließen die im vorigen Punkt vorgeschlagenen IT-Sicherheitsmaßnahmen ein.

2.9 Erarbeitung eines IT-Sicherheitsplans

Alle Aktivitäten, die zur Implementation der in den Sicherheitsempfehlungen vorgeschlagenen Schutzmaßnahmen notwendig sind, werden in einem IT-Sicherheitsplan verzeichnet und koordiniert.

2.10 Implementation

Die vorgeschlagenen IT-Sicherheitsmaßnahmen müssen dann gemäß der Aktivitätenliste im IT-Sicherheitsplan realisiert werden, dies beinhaltet auch die Einarbeitung und Schulung von Personal.

2.11 Nachprüfung

Die Nachprüfung soll sicherstellen, daß alle IT-Sicherheitsmaßnahmen korrekt implementiert wurden, mit den IT-Sicherheitszielen konform sind und daß auch Änderungen am System nicht die Wirksamkeit der Maßnahmen beeinträchtigen. Die Nachprüfung ist ein dauerhafter Prozeß, der in der Organisation verankert werden muß.

2.12 Zusammenfassung

In diesem Kapitel wurde ein Vorgehensmodell vorgeschlagen, mit Hilfe dessen in einer wissenschaftlichen Einrichtung ein IT-Sicherheitskonzept erstellt werden könnte. Dieses Vorgehensmodell wurde abgeleitet nach dem in [GMITS2] vorgeschlagenen Modell und wird dort als em Kombinierter Ansatz bezeichnet. Das Modell bietet die Möglichkeit, nach Bestimmung eines IT-Sicherheitsniveaus für die wissenschaftliche Einrichtung und Teileinrichtungen die niedrigen bis mittleren IT-Sicherheitsniveaus durch die pauschale Anwendung von Grundschutzmaßnahmen, z.B. nach [BSI1998], zu erreichen, andererseits bei höher schutzbedürftigen IT-Systemen und Daten das angestrebte Schutzniveau durch Maßnahmen zu erreichen, die aus einer detaillierten Risikoanalyse, z.B. nach [ITSHB1992], hervorgehen.

Kapitel 3

Anwendung des Vorgehensmodells am Fachbereich Informatik

Aus den in Kapitel 1 untersuchten Modellen wurde in Kapitel 2 eine Vorgehensweise für die Erstellung eines IT-Sicherheitskonzeptes in einer wissenschaftlichen Einrichtung abgeleitet. Im Rahmen dieser Arbeit soll diese Vorgehensweise am Beispiel des Fachbereichs Informatik der Universität Hamburg auf ihre Anwendbarkeit untersucht werden. Die aufgezeigten Schritte sollen dabei im folgenden nachvollzogen werden.

3.1 Abgrenzung des Fachbereichs Informatik und der untersuchten Fachbereichseinrichtungen

Der Fachbereich Informatik der Universität Hamburg, besteht aus 9 Arbeitsbereichen und 3 Arbeitsgruppen, beide zusammen unterteilt in insgesamt 4 Schwerpunkte. Weitere Teilbereiche des Fachbereiches sind das Rechenzentrum, die Bibliothek und die Verwaltung. Dem Fachbereich angegliedert sind Drittmittelprojekte, z.B. die DFN Policy Certification Authority (PCA), und das DFN CERT, das seit Januar 1999 als GmbH auftritt.

Eine Sicherheitspolitik würde fachbereichsweit gelten müssen, die Einbeziehung der fachbereichsexternen Organisationen wie der DFN-CERT GmbH, die zwar organisatorisch unabhängig, räumlich jedoch dem Fachbereich zuzuordnen ist, muß jedoch überlegt werden.

Im Rahmen dieser Arbeit wird das Vorgehensmodell exemplarisch auf einige wichtige Fachbereichseinrichtungen angewandt. Andere, hier nicht untersuchte Fachbereichseinrichtungen, würden dann ebenso untersucht werden können – die Anwendungstauglichkeit des Vorgehensmodells vorausgesetzt, die ja untersucht werden soll.

Die untersuchten Fachbereichseinrichtungen betreffen die Bereiche

- **Zentrale Einrichtungen**

Als zentrale Einrichtungen des Fachbereichs werden die Fachbereichs-Bibliothek, die Fachbereichs-Verwaltung und das Fachbereichs-Rechenzentrum untersucht.

- **Arbeitsbereiche und Arbeitsgruppen**
  Exemplarisch werden die Arbeitsbereiche AGN (Anwendungen der Informatik in Geistes- und Naturwissenschaften) sowie SWT (Softwaretechnik) untersucht.

- **Angegliederte Einrichtungen**
  Die DFN CERT GmbH ging 1999 aus dem DFN-Projekt DFN CERT hervor und nutzt Räumlichkeiten am Fachbereich Informatik. Die DFN CERT GmbH ist das Computer-Notfall-Team des Deutschen Forschungsnetzes DFN.

3.2 Implementation eines IT-Sicherheitsmanagement-Teams

Ein IT-Sicherheitsmanagement-Team hat, wie in Abschnitt 2.2 beschrieben, die Aufgabe, die IT-Sicherheitsziele festzulegen und Verfahren (IT-Sicherheitspolitik) zu definieren, um diese Ziele zu erreichen. Außerdem soll das IT-Sicherheitsmanagement-Team für die Implementation der Sicherheitsmaßnahmen sorgen sowie die Umsetzung überwachen.

3.2.1 Aufgaben des Teams

Die Aufgaben des IT-Sicherheitsmanagement-Teams sind in [BSI1998] detailliert dargestellt:

- ▷ IT-Sicherheitsziele festzulegen und eine Politik zu entwickeln, diese Ziele zu erreichen,
- ▷ die Pflichten des IT-Sicherheitsbeauftragten festzulegen,
- ▷ bei der Erstellung des IT-Sicherheitskonzepts beratend zu unterstützen, sowie zu überprüfen, ob die IT-Sicherheitsziele erreicht werden,
- ▷ einen Realisierungsplan der im IT-Sicherheitskonzept ausgewählten Sicherheitsmaßnahmen zu entwickeln,
- ▷ die Implementierung dieser Sicherheitsmaßnahmen zu überwachen,
- ▷ die Sensibilisierung für IT-Sicherheit in der gesamten Institution zu fördern,
- ▷ die Effektivität von Sicherheitsmaßnahmen im laufenden Betrieb zu kontrollieren,
- ▷ den IT-Koordinierungsausschuß und das Management in IT-Sicherheitsfragen zu beraten, sowie
- ▷ die Ressourcen (Personen, Geld, Wissen etc.) festzulegen, die im IT-Sicherheitsprozeß verbraucht werden dürfen.

3.2.2 Angehörige des Teams

Dem IT-Sicherheitsmanagement- Team sollten nach [BSI1998] angehören:

- ein Mitglied mit Expertenwissen im Bereich IT-Sicherheit sowie Erfahrung mit Organisation und Verwaltung
- der IT-Sicherheitsbeauftragte
- ein Vertreter aus dem IT-Koordinierungsausschuß sowie
- ein Vertreter der Nutzer

Die Einbeziehung von jeweils nur einem Mitarbeiter ist am Fachbereich Informatik zu überdenken, da verschiedene Gründe für die Einbeziehung weiterer Personen sprechen, die den entsprechenden Rollen zugeordnet werden können. Die Gründe sind nachfolgend dargestellt.

Expertise im Bereich IT-Sicherheit

Am Fachbereich Informatik liegt die Kernkompetenz im Bereich IT-Sicherheit in drei Quellen: zum einen wird im Fachbereichs-Rechenzentrum im Rahmen der täglichen Arbeit IT-Sicherheit praktiziert und damit entsprechendes Know-How vorgehalten, zweitens gibt es einen Arbeitsbereich (AGN), der sich mit IT-Sicherheit beschäftigt und über entsprechendes Know-How verfügt und drittens ist mit der DFN CERT GmbH Expertise über IT-Sicherheit und IT-Sicherheitsmanagement im Hause. Letztere ist möglicherweise, da nicht mehr organisatorisch mit der Universität verbunden sondern als eigenständiges Unternehmen agierend, nicht in derselben Weise in das IT-Sicherheitsmanagement-Team zu integrieren wie die ersteren zwei.

IT-Sicherheitsbeauftragter

Am Fachbereich Informatik sind die Aufgaben hier zweigeteilt. Zum einen gibt es einen Datenschutzbeauftragten des Fachbereichs, zum anderen ist für den Bereich der IT-infrastrukturellen Sicherheit ein Mitarbeiter des Fachbereichs-Rechenzentrums zuständig. In diesem Fall sollten beide diesem Team angehören.

Vertreter aus dem IT-Koordinierungsausschuß

Die Rolle eines IT-Koordinierungsausschusses nimmt am Fachbereich Informatik der Wirtschaftsausschuß wahr. Dieser sollte aus seinen Reihen einen Vertreter benennen.

Vertreter der Nutzer

Die Nutzer am Fachbereich sind in verschiedene Nutzerklassen einzuteilen: Studierende, Verwaltung, Professoren und FB-Mitarbeiter sowie Mitarbeiter in Drittmittelprojekten. Andererseits existiert mit dem Fachbereichsrat ein Gremium, das am Fachbereich die Interessen der FB-Angehörigen koordinieren soll. Die Statusgruppen der Professoren, Dozenten, Mitarbeiter (incl. Mitarbeiter aus Drittmittelprojekten), Studierenden und der Verwaltungsmitarbeiter sind hier

mit Sitz und Stimme vertreten. Aus diesem Grund sollte es Aufgabe des Fachbereichsrates sein, einen oder mehrere Vertreter in das IT-Sicherheitsmanagement-Team zu entsenden. Es kann hier sinnvoll sein, mehrere Vertreter zu entsenden, da zum einen es personelle Überschneidungen gibt mit den drei vorgenannten Rollen und es andererseits so möglich ist, Vertreter mehrerer Statusgruppen an den Entscheidungen des IT-Sicherheitsmanagement-Teams zu beteiligen.

3.3 Bestimmung der IT-Sicherheitsziele am Fachbereich Informatik

Zur Bestimmung der IT-Sicherheitsziele haben folgende Befragungen stattgefunden:

- Interview mit Herrn Dr. H.-J. Mück (Leiter des Fachbereichs-Rechenzentrums) zum Fachbereichs-Rechenzentrum am 23. März 1999,
- Interview mit Herrn Dr. H.-J. Mück (Geschäftsführer der DFN CERT GmbH) zur DFN CERT GmbH, zum DFN-Projekt *Firewalls in Hochgeschwindigkeitsnetzen* sowie zum DFN-Projekt *Policy Certification Authority* am 23. März 1999,
  desweiteren eine Nachbesprechung mit Mitarbeitern der DFN CERT GmbH am 30. August 1999,
- Interview mit Herrn T. Schwinghammer (Fachbereichs-Planer) zur Fachbereichs-Verwaltung am 30. März 1999,
- Interview mit Frau E. Criegee (Leiterin der Fachbereichs-Bibliothek) und Frau M. Obernesser (Bibliothekarin) zur Fachbereichs-Bibliothek am 8. Juni 1999,
- Interview mit Frau Dr. K. Schier (Wissenschaftliche Mitarbeiterin am AB AGN) zum Arbeitsbereich AGN am 7. April 1999,
- Interview mit Herrn U. Zimmer (Wissenschaftlicher Mitarbeiter am AB SWT) zum Arbeitsbereich SWT am 8. Juni 1999.

Der Fragenkatalog und die jeweiligen Antworten sind im Teil II dieser Arbeit zu finden.

3.3.1 Ergebnisse der Befragung

Fachbereichsverwaltung

Die Selbstbeschreibung der Fachbereichsverwaltung [Studienführer1997] ist:
„Die Fachbereichsverwaltung ist zuständig für allgemeine studentische und verwaltungstechnische Angelegenheiten, insbesondere Mittelbewirtschaftung, Personalverwaltung und Gremienbetreuung.“

Darüber hinaus wird Unterstützung für die wissenschaftlichen Arbeiten am Fachbereich geleistet. Die Befragung[1] ergab die folgenden Ergebnisse:

[1] Zu den Antworten auf die einzelnen Fragen siehe Teil II dieser Arbeit.

1. **Welche Bedeutung hat der Einsatz der IT für die Fachbereichsverwaltung ?**
   In der Verwaltungstätigkeit wird der IT eine hohe Bedeutung beigemessen, z.B. im Kassenwesen (Buchung, Rechnungen) und der geplanten Stellenverwaltung.
   Im Wissenschaftsservice hat die Bedeutung in den letzten Jahren durch Emailverkehr zwischen der Verwaltung und den Fachbereichseinrichtungen zugenommen, die gesamte Kommunikation läuft jetzt über Email, die Preisermittlung für Bestellvorgänge läuft teilweise über WWW. Dazu kommen die Prognoseberechnungen über die eingesetzten Finanzmittel, die unabhängig von der Zentralverwaltung und unabhängig vom Verwaltungsnetz durchgeführt werden.

2. **Welche Ziele verfolgt der Fachbereich Informatik mit dem Einsatz der IT in der Fachbereichsverwaltung ?**
   Die Beschleunigung der Arbeitsprozesse ist das Kernziel des Einsatzes der IT in der Fachbereichverwaltung.

3. **Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist ?**
   Aus den Antworten wird deutlich, daß in der FB-Verwaltung personenbezogene Daten vorgehalten werden, die gemäß BDSG vertraulich zu behandeln sind. Darüber hinaus ist bei mißbräuchlicher Veröffentlichung der Daten mit Regreßforderungen von Geschädigten zu rechnen. Es kann politische oder gesellschaftliche Verunsicherung ausgelöst werden, wenn die Veröffentlichung bekannt wird, mindestens entstünde Zweifel an der amtlichen Verschwiegenheit.

4. **Hängen wesentliche Entscheidungen von der Richtigkeit und Aktualität – Integrität – von Informationen ab, die mit IT verarbeitet werden ?**
   Die Prüfungsordnung sowie die Grundsätze ordnungsmäßiger Buchführung verlangen die integre Datenverarbeitung der Prüfungsdaten sowie fiskalischer Daten. Im Prüfungswesen kann eine fehlerhafte Datenverarbeitung zu falschen amtlichen Entscheidungen bis hin zur Exmatrikulation von Studierenden führen. Im Kassenwesen kann ein Schaden durch Umlenken von Zahlungen entstehen. Eine fehlerhafte Personalprognose kann bewirken, daß Personen nicht eingestellt werden können, weil vermeintlich keine Mittel hierfür vorhanden sind oder umgekehrt zuviele Mitarbeiter eingestellt werden und der Fachbereich in Zahlungsunfähigkeit gerät.
   Manipulationen würden entdeckt werden, z.B. im Rahmen der Mittelzuweisung innerhalb der Uni aufgrund der statistischen Kennzahlen, die im FB ermittelt werden. Hier drohen Ansehensverluste innerhalb der Universität.

5. **Gibt es wichtige und/oder sehr wichtige Aufgaben in der Fachbereichsverwaltung, die nur mit Unterstützung von IT erledigt werden können? Gibt es Massenaufgaben in der Fachbereichsverwaltung, deren Erledigung nur mit IT-Einsatz möglich ist?**
   Innerhalb einer bestimmten Frist müssen Steuern und Sozialversicherungsbeiträge abgeführt und Rechnungen beglichen werden. Ebenso müssen Klausurdaten innerhalb von

wenigen Tagen nach der Klausur veröffentlicht werden (Prüfungsordnung). Als zeitkritisch und nicht manuell lösbar wird aber nur die Mittelbewirtschaftung[2] angesehen.

Arbeitsbereich AGN - Anwendunge der Informatik in Geistes- und Naturwissenschaften

Im Arbeitsbereich AGN[3] gibt es eine inoffizielle Sicherheitspolitik:
„Es gibt ethische Leitlinien für die Erstellung von WWW-Seiten. Es gibt eine moralische Richtlinie in Bezug auf die Verbreitung der Kenntnis über Sicherheitslücken. Keine(r) soll Viren schreiben oder verbreiten. Jede(r) soll Verantwortung mit seinem (ihrem) Spezialwissen wahrnehmen. Mit sensitiven Informationen soll vertraulich umgegangen werden." (Interview mit Dr. K. Schier)

1. **Welche Bedeutung hat der Einsatz der IT für den Arbeitsbereich AGN?**
   Die IT am Arbeitsbereich dient der Unterstützung von Lehre, Forschung und der Arbeitsbereichsverwaltung.

2. **Welche Ziele verfolgt der Fachbereich Informatik mit dem Einsatz der IT im Arbeitsbereich AGN?**
   Die IT wird zum Herausfinden von Sicherheitslücken genutzt – der Arbeitsbereich nutzt damit die IT zur Untersuchung von IT.

3. **Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist ?**
   Datenbanken mit personenbezogenen Daten gibt es am Arbeitsbereich selbst bis auf eine Ausnahme nicht, jedoch werden Informationen über Studenten, z.B. Adreßdaten, in den Sekretariatsrechnern gespeichert. Aus ethischen Gründen werden Informationen über Computerviren und deren Code als sensitiv eingestuft.

   Im Drittmittelprojekt BADO[4] werden sensitive personenbezogene Daten verarbeitet. Hier ergibt sich hoher Schutzbedarf.

4. **Hängen wesentliche Entscheidungen von der Richtigkeit und Aktualität – Integrität – von Informationen ab, die mit IT verarbeitet werden ?**
   Im Rahmen des Drittmittelprojektes BADO ergeben sich sowohl vertragliche als auch gesetzliche Verpflichtungen aus dem BDSG [BDSG] zur Einhaltung der Datenintegrität. Die Virendatenbank soll aufgrund einer internen Vorschrift seitens der Arbeitsbereichsleitung konsistent gehalten werden. Eine Verfälschung der Virentestergebnisse würde einen Ansehensverlust nach sich ziehen.

[2] Verwaltung der dem Fachbereich zugeteilten finanziellen Mittel
[3] Zu den Antworten auf die einzelnen Fragen siehe Teil II dieser Arbeit.
[4] Drittmittelprojekt *Basisdaten-Dokumentation*

Aus der Verfälschung von Daten, die auf den Mitarbeiterrechnern gespeichert sind, kann sich erheblicher Schaden ergeben, z.B. bei der Verfälschung von Gutachten. Der Schaden kann sich fortpflanzen, z.B. kann aus verfälschten Prüfungsgutachten ein unrechtmäßiger Verwaltungsakt seitens des Prüfungsamtes folgen.

5. **Gibt es wichtige und/oder sehr wichtige Aufgaben im Arbeitsbereich AGN, die nur mit Unterstützung von IT erledigt werden können? Gibt es Massenaufgaben im Arbeitsbereich AGN, deren Erledigung nur mit IT-Einsatz möglich ist?**
   Der Antivirentest und die Virendatenbank können nur mithilfe der IT bestehen, ebenso wird im Rahmen des Drittmittelprojektes BADO die Verfügbarkeit der IT zu einem bestimmten Zeitpunkt der Datenauswertung vertraglich vorausgesetzt. Weitere Verfügbarkeitsverpflichtungen ergeben sich nicht aus vertraglichen oder gesetzlichen Grundlagen. Der ständige IT-Zugriff im Rahmen der täglichen Arbeit wird jedoch erwartet, insbesondere der Emailzugriff durch den Leiter der Einrichtung.

Fachbereichsbibliothek

Die Selbstbeschreibung der Bibliothek [Studienführer1997] ist:
„Die Bibliothek versorgt als zentrale Einrichtung alle Angehörigen und Studierenden des Fachbereichs mit Literatur. Darüber hinaus werden ihre Bestände und Dienste von fachbereichsfremden Interessenten stark genutzt. Der i.d.R. ausleihbare Bestand umfaßt ca. 60.000 Bücher, Reports und Zeitschriftenbände. Etwa 250 Zeitschriften sind abonniert. Der gesamte Bestand der Bibliothek ist im Campus-Katalog nachgewiesen, einem gemeinsamen Online-Katalog der Staats- und Universitätsbibliothek und der Bibliotheken der Universität. Die Bibliothek bietet über ihre Homepage neben dem Campus-Katalog andere ausgewählte Bibliothekskataloge an sowie wichtige Recherche- und Dokumentlieferdienste und weitere Informationsmöglichkeiten zum Fach Informatik."
Die Bibliothek bietet daneben die Möglichkeit des entfernten Zugriffs der Benutzer auf ihre Ausleihdaten sowie die Bestellmöglichkeit via Internet (WWW sowie Telnet und SSH) im Rahmen des Systems OPAC.

Die Befragung[5] ergab die folgenden Antworten:

1. **Welche Bedeutung hat der Einsatz der IT für die Fachbereichsbibliothek ?**
   Aus den Antworten der Befragung wird deutlich, daß ohne den Einsatz von Informationstechnik die Bibliothek nicht mehr sinnvoll arbeiten kann. Einige Schlüsselfunktionen der Bibliothek sind fast vollständig auf das IT-System abgebildet.

2. **Welche Ziele verfolgt der Fachbereich Informatik mit dem Einsatz der IT in der Fachbereichsbibliothek ?**
   Neben der Arbeitserleichterung (Schnelligkeit, Vollständigkeit) für die MitarbeiterInnen

[5] Zu den Antworten auf die einzelnen Fragen siehe Teil II dieser Arbeit.

der Bibliothek und die BenutzerInnen sind vor allem eine zeitgemäße Informationsvermittlung und Recherche sowie die Präsentation der Rechercheergebnisse von Bedeutung.

3. **Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist ?**
   In der Bibliothek werden personenbezogene Ausleihdaten erzeugt und verarbeitet, hierzu zählen auch Gebührendaten. Besondere Anforderungen stellt deshalb das Bundesdatenschutzgesetz [BDSG].

4. **Hängen wesentliche Entscheidungen von der Richtigkeit und Aktualität – Integrität – von Informationen ab, die mit IT verarbeitet werden ?**
   Ausleihdaten führen zu Gebührenvorgängen. Sind diese Daten fehlerhaft, so werden den Studierenden möglicherweise unrechtmäßig Gebühren belastet oder erlassen. Fehler sind hier nicht nachvollziehbar, so begründet sich ein hohes Sicherheitsniveau bezüglich der Integrität der Daten. Eine weitere Begründung ist die drohende Handlungsunfähigkeit der Bibliothek, wenn der Bestandskatalog Fehler enthält.

5. **Gibt es wichtige und/oder sehr wichtige Aufgaben in der Fachbereichsbibliothek, die nur mit Unterstützung von IT erledigt werden können? Gibt es Massenaufgaben in der Fachbereichsbibliothek, deren Erledigung nur mit IT-Einsatz möglich ist?**
   Recherchemöglichkeiten werden noch wichtiger eingestuft als die Verfügbarkeit des Ausleihsystems. Fallen diese Systeme aus, so kann die Bibliothek ihre Aufgabe nicht mehr erfüllen.

Arbeitsbereich SWT - Softwaretechnik

Die Befragung[6] ergab die folgenden Ergebnisse:

1. **Welche Bedeutung hat der Einsatz der IT für den Arbeitsbereich SWT?**
   Anliegen des Arbeitsbereiches Softwaretechnik ist es, sowohl den Mitarbeitern als auch den Studierenden eine Grundausstattung an EDV zur Verfügung zu stellen.

2. **Welche Ziele verfolgt der Fachbereich Informatik mit dem Einsatz der IT im Arbeitsbereich SWT?**
   Einzelne Wissenschaftler müssen arbeiten können - Promotion, Habilitation, Forschung; dazu gehört die wissenschaftliche Kommunikation mit der ganzen Welt.
   Ein Lehrbetrieb, der größtenteils auf IT basiert, muß aufrechterhalten werden; d.h. die technische Ausstattung ist Lehrmittel und Lehrgegenstand zugleich.
   Darüberhinaus müssen Sekretariatsdienste ermöglicht werden, z.B. Email, Internetbanking und Briefverkehr.

3. **Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist ?**

[6] Zu den Antworten auf die einzelnen Fragen siehe Teil II dieser Arbeit.

Prüfungsrelevante Daten und Klausurdaten werden auf den Rechnern von SWT verarbeitet, dies sind personenbezogene Daten, die als vertraulich eingestuft werden. Forschungsergebnisse, Studienarbeiten, Diplomarbeiten, Dissertationen und andere Papers werden bis zu ihrer Veröffentlichung als vertraulich angesehen, danach als öffentlich. Aus der vorzeitigen Veröffentlichung könnten im schlimmsten Falle Personen psychisch geschädigt werden, wenn z.B. Daten veröffentlicht würden, die der betroffenen Person unangenehm sind. Bei Projekten mit industriellen Partnern wird Vertraulichkeit vereinbart und vorausgesetzt.

4. **Hängen wesentliche Entscheidungen von der Richtigkeit und Aktualität – Integrität – von Informationen ab, die mit IT verarbeitet werden ?**
   Hier hat die Befragung keine besonderen Anforderungen im Arbeitsbereich ergeben.

5. **Gibt es wichtige und/oder sehr wichtige Aufgaben im Arbeitsbereich SWT, die nur mit Unterstützung von IT erledigt werden können? Gibt es Massenaufgaben im Arbeitsbereich SWT, deren Erledigung nur mit IT-Einsatz möglich ist?**
   Es wird mit einer maximalen Ausfallzeit von 1-2 Tagen gerechnet, während der sich Studierende im extremsten Fall ihre Übungsaufgaben nicht vom Netz laden können. Besondere Anforderungen an die Verfügbarkeit gibt es nicht.

DFN CERT GmbH

Aus der Befragung[7] wird folgendes deutlich:

1. **Welche Leistungen erbringt das DFN CERT gegenüber dem DFN ?**
   Die DFN CERT GmbH ist die zentrale Anlaufstelle für Notfälle, insbesondere Angriffe im Bereich des Deutschen Forschungsnetzes (DFN). Es wird Hilfe bei der Aufklärung von Angriffen und Unfällen angeboten. Basisdienste sind Informationsangebote zu Rechnersicherheit und Netzsicherheit, dazu Beratung und Warnmeldungen. Darüber hinaus wird Notfallunterstützung angeboten, Informationsaustausch mit anderen CERTs und innerhalb der FIRST[8] betrieben sowie Veranstaltungen, wie z.B. der CERT-Workshop, organisiert. Zusätzlich bietet die DFN CERT GmbH noch folgende Dienstleistungen an: Risikoanalysen, Gutachten, Sicherheitskonzepte; Produktevaluation; individuelle Fortbildungsmaßnahmen; Unterstützung vor Ort; Aufbau von Notfallteams und Zertifizierungsinstanzen.

2. **Welche Leistungen erbringt das DFN CERT gegenüber dem Fachbereich/ der Uni ?**
   Es gibt einen Informationsfluß zwischen FB-Rechenzentrum und CERT. Das CERT war auch ins Verwaltungs-EDV-Projekt eingebunden.

[7] Zu den Antworten auf die einzelnen Fragen siehe Teil II dieser Arbeit.
[8] Forum of Incident Response Teams

3. **Aus welchen Einheiten besteht das DFN CERT und was wird in diesen gemacht**
   Das DFN CERT ist seit Januar 1999 eine eigenständige GmbH und erbringt die oben beschriebenen Leistungen.

   Die DFN PCA (Policy Certification Authority) hat als Aufgaben die Erstellung und Pflege der Policy(s) zur Zertifizierung von anderen Zertifizierungsinstanzen (CAs) des DFN sowie der öffentlichen Schlüssel von Benutzern. Die DFN PCA nimmt auch selbst Zertifizierungen vor.

   Das Firewallabor ist ein Drittmittelprojekt an der Universität. Aufgabe sind die Erforschung von Konzepten für Firewalls in Hochgeschwindigkeitsnetzen sowie Tests und Lastmessungen.

4. **Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist?**
   In der DFN CERT GmbH sind die Logdaten von Vorfällen (traceroutes, Hacking-Angriffe, Portscans) zu schützen, da die gesammelte Information direkt zu Angriffen genutzt werden kann. Die eingehenden Sicherheitswarnungen sind ebenfalls zu schützen. Alle Daten, die im CERT sind, werden als sensibel angesehen. Die Policy des DFN-CERT besagt, daß keine Daten herausgegeben werden, solange der Datenlieferant keine Zustimmung gibt.

   Im Bereich der PCA ist die Vertraulichkeit des privaten Signaturschlüssels essentielle Voraussetzung für die Arbeit der PCA, da hiervon die Zertifizierungsinfrastruktur des DFN abhängig ist.. Hier besteht ein entsprechender Schutzbedarf. Es gibt eine High-Level- und eine Medium-Level-Policy der PCA, die im Internet verfügbar ist.

   Auch im Firewalltestlabor gibt es kritische Daten und Inventar; z.B. bei Meßreihen muß u.U. auf den Quellcode zurückgegriffen werden; der darf lt. Vertrag nicht herausgegeben werden.

5. **Hängen wesentliche Entscheidungen von der Richtigkeit und Aktualität – Integrität – von Informationen ab, die mit IT verarbeitet werden ?**
   Sicherheitswarnungen müssen auf Echtheit überprüfbar sein, da sie auch Empfehlungen enthalten, wie die betreffenden Schwachstellen beseitigt werden können. Die Gefahr bestünde ansonsten, daß Angreifer selbst solche Empfehlungen erzeugen und damit Anwender verleiten, Sicherheitslücken zu erzeugen.

   Der Signaturschlüssel der PCA muß integer sein, da ansonsten die Signaturen ungültig wären. Die Verfälschung des privaten Schlüssels wird jedoch leicht erkannt, weil die Signaturen dann nicht mehr stimmen.

6. **Gibt es wichtige und/oder sehr wichtige Aufgaben in der DFN CERT GmbH bzw. der DFN PCA und im Firewallabor, die nur mit Unterstützung von IT erledigt werden können? Gibt es Massenaufgaben, deren Erledigung nur mit IT-Einsatz möglich ist?**
   Verfügbarkeit wird als wichtig eingestuft, jedoch nicht an erster Stelle. Ein Angriff auf die Verfügbarkeit des CERT kann jedoch andere Angriffe verschleiern, die das CERT dann nicht beobachten kann.

   Email und Webserver werden als Schnittstelle nach Außen verwendet. Sie dienen der Kommunikation von Schwachstellen und dem Austausch von Informationen über Angriffe. Wenn diese Dienste nicht verfügbar sind, bedeutet dies eine erhebliche Leistungseinschränkung. Die Notfallhotline geschieht per Email, da die Vertraulichkeit und Integrität hier besser als bei einem Telefonat zu wahren ist.

   Telefon und Fax dienen als Schnittstelle zwischen Anwendern und CERT; deren Verfügbarkeit ist sehr wichtig, da sonst keine IT-Sicherheitsberatung stattfinden kann.

   Darüberhinaus gibt es in der DFN CERT GmbH ein Workflowmanagementsystem, in dem alle relevanten Daten verzeichnet sind, so daß bei Mitarbeiterausfall auch andere Mitarbeiter die Aufgabe übernehmen könnten

Fachbereichs-Rechenzentrum

Eine Befragung[9] des Rechenzentrumsleiters hat am 2. März 1999 gemäß Fragenkatalog, Teil 6 stattgefunden. Geklärt werden sollte nicht nur die Frage des Sicherheitsniveaus, sondern es sollte auch ein Eindruck des vorherrschenden Sicherheitsbewußtseins gewonnen werden. Aus bereits getroffenen Vorkehrungen sollen Rückschlüsse auf die Priorisierung der Sicherheitsziele gewonnen werden.

In einer Selbstbeschreibung charakterisiert sich das Rechenzentrum wie folgt:
„Das Informatik-Rechenzentrum stellt im Fachbereich Informatik zentrale Rechnerleistung für die Lehre und Forschung - insbesondere für die Ausbildung im Grundstudium - bereit, betreibt Workstation- und PC-Pools für die Lehre und koordiniert die Vernetzung aller Rechner des Fachbereiches.
Im Rahmen ihrer Ausbildung (Übungen zu Vorlesungen, Praktika, Projekte, Studien- und Diplomarbeiten ...) wird den Studierenden der Informatik viel Gelegenheit gegeben, die Informatik-Rechenanlagen kennenzulernen und zu benutzen.“ [Studienführer1997]

1. **Werden mit der eingesetzten IT Informationen verarbeitet, deren Vertraulichkeit besonders zu schützen ist ?**
   Das Rechenzentrum betreibt den Emailserver für den Fachbereich, Emails können als vertraulich angesehen werden, sollten daher gegen Fremdzugriff geschützt werden.

[9] Zu den Antworten auf die einzelnen Fragen siehe Teil II dieser Arbeit.

2. **Hängen wesentliche Entscheidungen von der Richtigkeit und Aktualität – Integrität – von Informationen ab, die mit IT verarbeitet werden ?**
   Hier gibt es keine besonderen Anforderungen.

3. **Gibt es wichtige und/oder sehr wichtige Aufgaben im Fachbereichs-Rechenzentrum, die nur mit Unterstützung von IT erledigt werden können? Gibt es Massenaufgaben im Fachbereichs-Rechenzentrum, deren Erledigung nur mit IT-Einsatz möglich ist?**
   Kommunikation, insbesondere Internetzugriff und Email, haben Priorität hinsichtlich der Verfügbarkeit.

3.3.2 Klassifikation der IT-Systeme der Fachbereichseinrichtungen nach ihrem Schutzbedarf

Fachbereichs-Verwaltung

Das System zur Mittelbewirtschaftung MBV[10] erfordert ein hohes Sicherheitsniveau aufgrund der genannten Anforderungen an Verfügbarkeit und Integrität.
Einen hohen Vertraulichkeits- und Integritätsbedarf haben die künftigen Systeme zur Stellenverwaltung und zum Prüfungswesen. Das System zur Stellenverwaltung begründet den Vertraulichkeitsbedarf auf Vorgaben des Datenschutzes, den Integritätsbedarf jedoch aus wirtschaftlichen Erfordernissen. Hierzu gibt es eine Studie [LIT1998] der Universität und des Landesamtes für Informationstechnik (LIT) Hamburg mit dem Ziel integrer und sicherer Datenkommunikation.
Das System zum Prüfungswesen muß Vertraulichkeits- und Integritätsvorgaben nach dem BDSG beachten. hier hat auch der Datenschutzbeauftragte des Fachbereichs bereits eine Risikoanalyse angeordnet. Im Bereich des Wissenschaftsservice besteht für Kontoangaben und Personaldaten ein Vertraulichkeitsbedarf, im Sinne des mittleren Schutzniveaus, das den Vertraulichkeitsanspruch interner Informationen beschreibt.

Arbeitsbereich AGN - Anwendunge der Informatik in Geistes- und Naturwissenschaften

Hoher Schutzbedarf für die Virendatenbank, da diese vom Arbeitsbereich als sensitiv eingestuft wird. Im Drittmittelprojekt BADO werden sensitive personenbezogene Daten verarbeitet. Hier ergibt sich hoher Schutzbedarf. Mittlerer Schutzbedarf besteht für Gutachten und Dateien auf Mitarbeiterrechnern. Laborechner für Studenten genießen niedrigen Schutzbedarf, da hier weder besondere Anforderungen an Integrität, Vertraulichkeit noch Verfügbarkeit gestellt werden.

Arbeitsbereich SWT - Softwaretechnik

Niedriger Schutzbedarf allgemein, mittlerer Schutzbedarf für personenbezogene Daten. Lediglich für Drittmittelprojekte, z.B. im Krankenhausbereich, sollte ein hohes Schutzniveau

[10] MBV steht für ein Softwareprojekt mit dem Namen *Mittelbewirtschaftungsverfahren*

angestrebt werden; dies ist auch mit den Drittmittelgebern aus Sicht der Vertraulichkeit so vereinbart. Zudem wird die Universität die Verfügbarkeit von IT im Rahmen von Drittmittelprojekten zusagen. Hier ist einem Rechtsanspruch der Drittmittelgeber Genüge zu tun.

Fachbereichs-Bibliothek

Hoher Schutzbedarf besteht aufgrund der Sensitivität der Benutzerdaten, die eine hohe Vertraulichkeit erfordert, der Integrität des Bestandskatalogs und der Verfügbarkeit von Recherchemöglichkeiten, Bestandskatalog und Ausleihsystem.

Fachbereichs-Rechenzentrum

Aus der Befragung wurde deutlich, daß für die Leistungen des Rechenzentrums grundsätzlich keine Verfügbarkeitsgarantien ausgesprochen werden. Zum anderen konnte auch festgestellt werden, daß bestimmte IT-Systeme des Rechenzentrums, z.B. Netzkomponenten, implizit höheren Verfügbarkeitsansprüchen genügen sollten, da sie Grundlage für das Funktionieren der Fachbereichs-IT sind. Den Verfügbarkeitsbedarf des FB-Netzes, des Emailverkehrs und des Internetzugriffs würde ich deshalb als hoch ansehen.

Ansprüche an die Vertraulichkeit von Daten bestehen dagegen im Bereich der Emailkommunikation, da diese durch das Fernmeldegeheimis vor unbefugter Einsichtnahme zu schützen sind, andererseits sind Unzulänglichkeiten hinsichtlich der Vertraulichkeit bekannt, deshalb sehe ich mittleren Schutzbedarf. Ebenso sind personenbezogene Daten, die nach dem BDSG [BDSG] zu Verwaltungszwecken mit Einverständnis der Benutzer erhoben werden können und aus Sicherheitsgründen (Sicherheitsaudits zur Einbruchserkennung) auch erhoben werden müssen, vor unbefugtem Zugriff zu schützen. Die Vertraulichkeit der benutzerspezifischen Daten soll auf Betriebssystemmechanismen belassen werden.

Die Integrität der Daten wird als wichtig für die Aufgabenerfüllung des Rechenzentrums angesehen. Es soll jedoch kein maximal möglicher Schutz der Integrität der Daten vom Rechenzentrum angeboten werden, deshalb wird hier der Integritätsbedarf in mittleres Schutzniveau eingeordnet.

DFN CERT GmbH

Aus der Befragung wurde deutlich, daß ein hoher Bedarf an Vertraulichkeit der gespeicherten und eingehenden Informationen besteht. Es werden alle Daten als sensibel angesehen und nur mit Zustimmung des Betroffenen weitergegeben. Verfügbarkeitsansprüche bestehen in Bezug auf das Workflowmanagement sowie die Kommunikationseinrichtungen. Hohe Integritätsansprüche bestehen vor allem an die Angriffsdaten, die kommuniziert werden, und die Daten, die vorgehalten werden. Insgesamt besteht in der DFN CERT GmbH hoher Schutzbedarf bezüglich aller drei Sicherheitseigenschaften.

Drittmittelprojekte DFN PCA und Firewallabor beim Fachbereichs-Rechenzentrum

In der DFN PCA besteht hoher Bedarf an die Vertraulichkeit und die Integrität des privaten Signaturschlüssels der DFN PCA, da hiervon die Integrität der Zertifizierungsinfrastruktur abhängig ist.

Im Firewallabor besteht mittlerer Schutzbedarf hinsichtlich der erzielten Ergebnisse des Drittmittelprojektes sowie des untersuchten Quellcodes.

3.3.3 Erarbeitung einer IT-Sicherheitskonzeptes für den Fachbereich Informatik

Grundsicherung

Basierend auf den Ergebnissen der Befragung wird vorgeschlagen, nach der Vorgehensweise des BSI [BSI1998] einen generellen Grundschutz für alle untersuchten Einrichtungen zu realisieren, da mindestens Anforderungen an die Verfügbarkeit bestimmter Komponenten gestellt werden, die eine Klassifikation in niedriges oder mittleres Sicherheitsniveau rechtfertigen.

Genaue Betrachtung

Für die folgenden Systeme sollte eine detaillierte Risikoanalyse nach [ITSHB1992] oder [GMITS2] durchgeführt werden, da sie in hohes Sicherheitsniveau oder darüber klassifiziert wurden.

- ▷ Verwaltung - MBV (Mittelbewirtschaftungsverfahren)
- ▷ Verwaltung - Stellenverwaltung
- ▷ Verwaltung - Prüfungswesen
- ▷ AGN - Virendatenbank
- ▷ AGN - Drittmittelprojekt BADO
- ▷ Bibliothek - Bestandskatalog und Ausleihsystem
- ▷ FB-Rechenzentrum - Emailverkehr und Netzbetrieb
- ▷ DFN CERT GmbH – alle Daten
- ▷ DFN PCA – Vertraulichkeit und Integrität des Signaturschlüssels der DFN PCA

Für diese IT-Systeme sollte eine detaillierte Risikoanalyse nach [GMITS2] oder [ITSHB1992] durchgeführt werden. Eine Ausnahme bilden die drei Systeme *Bibliothek-Recherche*, das *SWT-Drittmittelprojekt Krankenhausdaten* und der *Wissenschaftsservice* der Verwaltung. In diesen Systemen ergab die Befragung der jeweiligen Fachbereichseinrichtung, daß ein hoher Schutzbedarf vorliegt, folgende Argumente sprechen jedoch dafür, auch hier Grundschutz, ggf. ergänzt um weitere Maßnahmen, zu realisieren.

Besonderheiten

Die **Bibliotheksrecherche** unterliegt hohen Verfügbarkeitsanforderungen, jedoch weniger Vertraulichkeits- und Integritätsanforderungen. Da die Anfragen in verschiedenen Medien durch die Bibliothek selbst erfolgen bzw. keiner Anmeldung bedürfen, findet eine Anonymisierung dahingehend statt, daß der einzelne Anfragende im Nachhinein nicht mehr identifiziert werden kann und muß. Die Integritätsanforderungen beziehen sich auf die ermittelten Recherchedaten. Dabei handelt es sich im Wesentlichen um Referenzen auf Bücher, Zeitschriften, Reports, etc. Stimmen die angegebenen Referenzen aufgrund inkonsistenten Datenbestandes (Veralterung etc.), so tritt das Problem der nichtintegren Bestandsdaten auf, das gesondert untersucht wird. Stimmen die Referenzen aufgrund eines internen Fehlers in Hard- oder Software einzelner Klienten nicht, so fällt dies unmittelbar bei der Bestellung der Literatur auf und kann ggf. über das Ausleihsystem nochmals recherchiert werden. Dies wird, zusammen mit dem Bestandskatalog, ebenfalls gesondert untersucht. Ebenso kann bei Nichtverfügbarkeit einzelner Klienten oder Suchmedien auf andere Klienten oder Ersatzmedien ausgewichen werden. Eine detaillierte Risikoanalyse ist demzufolge entgegen den hohen Sicherheitsanforderungen, die die Bibliothek hier angegeben hat, für die Bibliotheksrecherche nicht erforderlich. Zum Grundschutzkonzept wäre die Verfügbarkeit entsprechender Ersatzklienten und -medien zu beachten.

Beim **Drittmittelprojekt Krankenhausdaten** des Arbeitsbereichs Softwaretechnik handelt es sich um ein Softwareprojekt, in dem allerdings keine realen Patientendaten in der Universität verarbeitet werden. Insofern hat das Projekt, bzw. die fertige Software beim Einsatz entsprechenden Anforderungen des Datenschutzes zu genügen, jedoch findet dieser Einsatz dann beim Drittmittelgeber und nicht im Hoheitsbereich der Universität statt. Deshalb sollte das Drittmittelprojekt einer Grundschutzabsicherung unterzogen werden, nicht jedoch einer detaillierten Risikoanalyse.

Verwaltung - Wissenschaftsservice
Die Verwaltung verarbeitet nach eigenen Angaben personenbezogene Daten, die zum einen zum Schriftverkehr benötigt werden, und andererseits Daten, die zu Prognosezwecken verwendet werden, aber außerhalb des Stellenverwaltungssystems und des Mittelbewirtschaftungssystems verarbeitet werden. Diese Daten unterliegen Vertraulichkeitsanforderungen. Da diese jedoch nur wenig über den Anforderungen mittleren Schutzniveaus liegen, sollte auch hier Grundschutz realisiert werden, der, ähnlich wie im Fall des Bibliotheksrecherchesystems, um Maßnahmen zur Erhöhung der Vertraulichkeit, ergänzt werden muß.

Weiteres Vorgehen

Da im Rahmen dieser Arbeit die genannten Systeme nicht alle detailliert untersucht werden können, sollen hier beispielhaft die drei IT-Systeme

- Fachbereichs-Bibliothek – Bestandskatalog und Ausleihsystem –
- Fachbereichs-Rechenzentrum – Emailverkehr und Netzbetrieb – sowie

- AGN – Virendatenbank –

betrachtet werden.

Kapitel 4

Bedrohungs- und Risikoanalysen

4.1 Fachbereichs-Bibliothek

4.1.1 Ergebnisse der Grundschutz-Analyse

Im Rahmen des IT-Grundschutzes nach [BSI1998] werden IT-Komponenten identifiziert, für die dann pauschal Gefährdungen angenommen werden. Ebenso pauschal werden dann in Kapitel 5 Maßnahmen vorgeschlagen. Die Gefährdungen, die lt. IT-Grundschutzhandbuch aus den identifizierten Komponenten hergeleitet werden, sind detailliert im Teil III aufgeführt.
Als Ergebnis der Grundschutzanalyse[1] wird die Anwendung der Grundschutz-„Bausteine“ für folgende IT-Komponenten der Bibliothek vorgeschlagen:

Übergeordnete Komponenten

Hier werden Gefährdungen betrachtet, die sich pauschal auf den gesamten Betrieb erstrecken und nicht einzelnen IT-Anwendungen zuordnen lassen. Dazu gehören:

Organisation:
Gefährdungen, auf die Organisation und Regelung der Arbeitsabläufe zurückzuführen sind .

Personal:
Gefährdungen, die aus der Abhängigkeit der Bibliothek von Beschäftigten bestehen.

Notfallvorsorge-Konzept:
Der mögliche Ausfall des IT-Systems als Gefährdung für die Bibliothek.

Datensicherungskonzept:
Der mögliche Verlust gespeicherter Daten als Gefährdung für die Abläufe in der Bibliothek.

[1] Die detaillierte Analyse befindet sich im Teil II dieser Arbeit

Infrastruktur

Gebäude:
Für die Bibliothek werden die Gebäude Haus A und Haus B sowie der Übergang zwischen beiden betrachtet.

Verkabelung:
In der Bibliothek ist das Ethernet in der Bibliothek, die Verkabelung zwischen Bibliothek und Fachbereichsrechenzentrum und jene zwischen Bibliothek und Regionalem Rechenzentrum sowie die Stromversorgung mit 230 V zu untersuchen.

Büroräume
Als Büroräume werden hier die Räumlichkeiten der Bibliothek sowie die Mitarbeiterbüros der Bibliothek in der Bibliothek und im Flur des Hauses A betrachtet.

Nicht vernetzte Systeme

PC unter Windows 95:
Betrachtet wird ein unter dem Betriebssystem Windows 95 laufender PC in der Bibliothek, der in der 34. Kalenderwoche 1999 auf Windows NT 4.0 umgerüstet werden soll. Da davon auszugehen ist, daß zum Zeitpunkt der Fertigstellung des IT-Sicherheitskonzeptes dieser PC dann wie die anderen unter Windows NT betrieben wird, wird er hier nicht mehr separat betrachtet sondern im folgenden Punkt mitbehandelt.

PC unter Windows NT:
Betrachtet werden einzelne, nicht vernetzte PCs , die unter dem Betriebssystem Windows NT 4.0 betrieben werden. Die PCs können mit einem Diskettenlaufwerk ausgestattet sein. Auf sicherheitsspezifische Aspekte von einzelnen Windows NT-Anwendungen wird nur am Rande eingegangen. Die Bibliothek hat kürzlich alle (bis auf einen) Rechner mit Windows NT 4.0 ausgestattet.

Vernetzte Systeme

Servergestütztes Netz:
Betrachtet wird ein lokales Netz mit mindestens einem Server. Die Clients können PCs mit oder ohne Festplatte sein, aber auch Unix-Workstations oder Terminals. Dieses ist jedoch unabhängig vom Netzbetriebssystem bzw. den Betriebssystemen der Clients. Dafür sind die weiterführenden Abschnitte (z.B. Server-Betriebssysteme) zu beachten.

Windows NT-Netz:
Betrachtet wird ein Windows NT Netzwerk, daß als Client-Server-System unter dem Betriebssystem Windows NT 4.0 betrieben wird. Die betrifft den NT-Server der Bibliothek, der vom Regionalen Rechenzentrum betrieben und gewartet wird, auch in dessen Räumlichkeiten untergebracht ist.

Datenübertragungseinrichtungen

Email:
Die Bibliothek hält für ihre Mitarbeiter einen Emailzugang über den POP3-Server des Fachbereichsrechenzentrums vor; als Klienten wird Pegasus Mail eingesetzt.

Telekommunikation

TK-Anlage:
Die Bibliothek nutzt die Telekommunikationsanlage des Fachbereichs.

Faxgerät:
Die Bibliothek hält ein Faxgerät vor; auch bei der Informationsübermittlung werden Gefährdungen angenommen.

Sonstige IT-Komponenten

Standardsoftware:
Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten wird und im allgemeinen über den Fachhandel, z.B. über Kataloge, erworben werden kann. Sie zeichnet sich dadurch aus, daß sie vom Anwender selbst installiert werden soll und daß nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist. Die Bibliothek nutzt die folgende Standardsoftware: Windows NT, Netscape, Teraterm (Telnet/ SSH), MS Office, Pegasus, FTP.

Datenbanken:
Die Bibliothek nutzt in geringem Umfang die Datenbanksysteme Access und Oracle, letzteres auslaufend. Deshalb ist auch hier der entsprechende Grundschutz–„Baustein“ anzuwenden.

4.1.2 Ergebnisse der detaillierten Analyse des Bestandskatalog- und Ausleihsystems PICA

Ermittlung der Schutzbedürftigkeit

In einem ersten Schritt werden die IT-Anwendungen und der zu verarbeitenden Informationen erfaßt, die mit dem Ausleihsystem und dem Bestandskatalog in Zusammenhang stehen.

IT-Anwendungen:
1. PICA-Klient (Ausleihsystem, das durch die BibliotheksmitarbeiterInnen genutzt wird)
2. Webzugang für die Benutzer in den Bibliotheksräumen
3. Terminalzugang für die Benutzer - Telnet oder SSH

Verarbeitete Informationen:
4. Benutzerdaten
5. Bestandskatalogdaten

6. Benutzernummer/ Barcode
7. Buchnummer/ Barcode

Die IT-Anwendungen und die zu verarbeitenden Informationen werden hinsichtlich ihrer Schutzbedürftigkeit nach dem oben aufgeführten Klassifikationsschema bewertet.

Verfügbarkeit und die Integrität
An die Verfügbarkeit und die Integrität des PICA-Klienten sowie dazugehörig die Benutzer- und Bestandskatalogdaten werden hohe Anforderungen gestellt. Ein großes Schadenspotential (Schadenswert 3) resultiert daraus, daß die Bibliothek ihr Ausleihsystem fortan elektronisch führt und dann auch nur bei Vorhandensein des Ausleihsystems (in Form der PICA-Software) arbeitsfähig ist. Die Integritätsanforderungen an den Katalogdatenbestand sind aus Sicht der Bibliothek höher als die Integritätsanforderungen an die Benutzerdaten zu bewerten, da der Zugriff auf den Bibliotheksbestand nur noch darüber erfolgt. Die Arbeitsfähigkeit der Bibliothek hängt davon ab und es würde sehr hohen finanziellen Aufwand verursachen, die Bestände erneut zu katalogisieren. Bei nichtintegren Benutzerdaten droht demgegenüber die vergleichsweise geringere Höchstentschädigungssumme aus dem BDSG [BDSG] von 50.000 DM pro Einzelfall bei falschen Daten bzw. der Wert der Literatur, falls nicht mehr nachvollzogen werden kann, wer die Literatur ausgeliehen hat.

Vertraulichkeit
Die Vertraulichkeit der Benutzerdaten ist im Bundesdatenschutzgesetz [BDSG] gefordert - wiederum maximal mit der Höchstentschädigungssumme von 50.000 DM pro Einzelfall zu bewerten.

Die Tabelle 4.1 gibt diese Überlegungen wieder und dient als Voraussetzung für die weiteren Schritte der Risikoanalyse nach [ITSHB1992], die im Anhang detailliert ausgeführt sind.

Tabelle 4.1: Risikoanalyse Bibliotheks-Ausleihsystem - Bewertung der IT-Anwendungen und Informationen

	Verfügbarkeit	**Integrität**	**Vertraulichkeit**
1. PICA-Client	3	3	1
2. Webzugang für die Benutzer in den Bibliotheksräumen	1	2	1
3. Terminalzugang für die Benutzer - Telnet oder ssh	1	2	0
4. Benutzerdaten	3	2	2
5. Bestandskatalogdaten	3	3	0
6. Benutzernummer/ Barcode	0	2	0
7. Buchnummer/ Barcode	0	2	0

Erfassung der Risikobereitschaft

In Zusammenarbeit mit der Bibliothek sind die tragbaren (T) und untragbaren (U) Risiken, wie in der Tabelle 4.2 aufgeführt, diskutiert worden[2]. Dies fließt in die Auswahl der Maßnahmen zur Begrenzung des Risikos auf ein tragbares Maß ein.

Zeilen: Schadenswert (0 ... 4+)
Spalten: Häufigkeitswert (0- ... 4)

Tabelle 4.2: Risikoanalyse Bibliotheks-Ausleihsystem - Erfassung der Risikobereitschaft

	0–	0	1	2	3	4
4+ katastrophal	U	U	U	U	U	U
4 existenzgefährdend	T	U	U	U	U	U
3 großer Schaden	T	U	U	U	U	U
2 mittlerer Schaden	T	T	U	U	U	U
1 geringer Schaden	T	T	T	U	U	U
0 unbedeutend	T	T	T	T	U	U

Für die Klassifikation der Häufigkeitswerte wurden folgende Werte zugrundegelegt:
0- = nach menschlichem Ermessen ausgeschlossen
0 = sehr selten bis
4 = sehr häufig

Auffällig ist die im Verhältnis zu anderen Fachbereichseinrichtungen geringe Risikobereitschaft der Bibliothek, die vor allem in finanzieller Hinsicht aus dem geringen Budget der Bibliothek

[2]Interview am 16.8.1999 mit Frau Criegee

für die IT-Infrastruktur resultiert.

Ergebnisse der Bedrohungs- und der Risikoanalyse

Die Detaillierte Risikoanalyse des Bibliotheks-Ausleih- und Katalogsystems PICA ergab das Vorliegen folgender Bedrohungen, bei deren Eintreten die Folgen für die Bibliothek als nicht tragbar einzustufen sind:

- Verlust der Integrität und Verfügbarkeit der Stromversorgung durch Stromausfall, einen Technischen Fehler oder Blitzeinschlag
- Verlust der Integrität der Gebäude und der Bibliotheksräume samt Infrastruktur durch unkontrollierten Zugang fremder Personen tagsüber und des Reinigungspersonals (frühmorgens) zu den Räumen.
- Verlust von Verfügbarkeit und Integrität der Sicherungseinrichtungen und der Netzkomponenten durch technischen Fehler
- Technisches Versagen der Hardware in Benutzer-PCs, PICA-PCs und Netzkomponenten
- Verlust von Verfügbarkeit und Integrität der PICA-PCs, der Benutzer-PCs und der Barcodescanner durch Bedienungs- oder Wartungsfehler.
- Verlust der Integrität der PICA-PCs, Barcodescanner und Ethernet-Netzwerk durch Manipulation.
- Bedrohung der Vertraulichkeit der PICA-PCs durch die Möglichkeit des Mitlesens der Ein- und Ausgabe durch Unberechtigte.
- Bedrohung der Integrität der Bedienungsanleitungen für die PICA-PCs und der PICA-Ausdrucke durch Fehler, Unvollständigkeit, unbefugte Änderungen oder böswilligen Austausch.
- Bedrohung der Verfügbarkeit, Integrität und Vertraulichkeit der PICA-Software und der Netscape-Software durch Softwarefehler.
- Bedrohung der Verfügbarkeit, Integrität der PICA-Software durch Fehler im Betriebssystem.
- Bedrohung der Verfügbarkeit, Integrität und Vertraulichkeit der PICA-Software, der Netscape-Software und der Telnet-Software durch Fehlen oder Überwinden der Zugangskontrolle oder durch Fahrlässigkeit der Benutzer.
- Bedrohung von Verfügbarkeit, Integrität und Vertraulichkeit der PICA-Software durch Mißbrauch.

- Bedrohung von Verfügbarkeit, Integrität und Vertraulichkeit der Anwendungssoftware (PICA, Netscape, Telnet), des Betriebssystems, der Benutzerdaten und der Bestandskatalogdaten durch unkontrolliertes Einbringen von Software, durch fehlerhafte Software und Einbringen von Computerviren.
- Bedrohung der Verfügbarkeit, Integrität und Vertraulichkeit der Anwendungssoftware und des Betriebssystems durch Bedienungs- oder Wartungsfehler.
- Bedrohung der Verfügbarkeit und Integrität der PICA-Software, der Benutzerdaten und der Bestandskatalogdaten durch Hardwarefehler.
- Bedrohung der Bestandsdaten durch fehlerhafte manuelle Eingabe, absichtliches oder unabsichtliches unbefugtes Löschen.
- Bedrohung der Vertraulichkeit der Benutzerdaten durch Mitlesen an den PICA-PCs, unberechtigtes Kopieren oder Auswerten von Daten an den Benutzer-PCs (z.B. Netscape-Logdaten).
- Bedrohung der Integrität und Vertraulichkeit der Benutzerdaten, Bestandskatalogdaten und PICA-Steuerungsdaten bei der Übertragung durch unbefugten Zugang zum Netz oder Manipulation an Netzkomponenten.
- Bedrohung der Verfügbarkeit des Netzes durch Fehlverhalten oder technischen Defekt.
- Bedrohung der Verfügbarkeit Integrität und Vertraulichkeit der Benutzerdaten, Bestandskatalogdaten und PICA-Steuerungsdaten bei der Übertragung durch Angriffe gegen die Kommunikationsverbindungen.
- Bedrohung des Bibliotheksbetriebes durch Ausfall von Bibliothekarinnen und MitarbeiterInnen.
- Bedrohung des Bibliotheksbetriebes durch Ausfall der RZ-Mitarbeiter im Fehlerfall.

4.2 Fachbereichs-Verwaltung

4.2.1 Grundschutzanalyse des Wissenschaftsservice

Als Ergebnis der Grundschutzanalyse wird die Anwendung der Grundschutz-„Bausteine“ für folgende IT-Komponenten der Fachbereichs-Verwaltung vorgeschlagen:

Übergeordnete Komponenten

Hier werden, wie im Beispiel der Fachbereichs-Bibliothek, die folgenden Komponenten betrachtet:
Organisation:
Gefährdungen, auf die Organisation und Regelung der Arbeitsabläufe zurückzuführen sind .

Personal:
Gefährdungen, die aus der Abhängigkeit der Fachbereichs-Verwaltung von ihren Beschäftigten bestehen.

Notfallvorsorge-Konzept:
Der mögliche Ausfall des IT-Systems als Gefährdung für die Fachbereichs-Verwaltung.

Datensicherungskonzept:
Der mögliche Verlust gespeicherter Daten als Gefährdung für die Abläufe in der Fachbereichs-Verwaltung.

Infrastruktur

Gebäude:
Für die Fachbereichsverwaltung ist das Gebäude Haus A zu betrachten.

Verkabelung:
In der Verwaltung betrifft dies das Ethernet in der Verwaltung, die Verkabelung zwischen Verwaltung und Fachbereichsrechenzentrum sowie die Stromversorgung mit 230 V. Die Verkabelung wird vom Fachbereichsrechenzentrum bzw. der Haustechnik betrieben.

Büroräume:
Büroräume sind im Haus A, 1.und 2. Stock, zu betrachten.

Datenträgerarchiv:
In der Fachbereichs-Verwaltung werden Datenträger in einem Stahlschrank gelagert.

Raum für technische Infrastruktur:
Es gibt in der Fachbereichsverwaltung einen Raum für Verkabelung, Drucker und Betriebsmittel.

In Räumen für technische Infrastruktur sind in der Regel solche Geräte und Einrichtungen untergebracht, die keine oder nur eine seltene Bedienung durch einen Menschen benötigen.

Schutzschränke:
Am Fachbereich Informatik wird ein Stahlschrank zur Aufbewahrung von Datenträgern und Dokumenten eingesetzt.

Nicht vernetzte Systeme

PC unter Windows 95:
Betrachtet wird ein Rechner unter dem Betriebssystem MacOS8, der durch die Simulationssoftware „Softwindows“ die Arbeit unter dem Betriebssystem Windows 95 erlaubt.

PC unter Windows NT:
Betrachtet werden PCs, die unter dem Betriebssystem Windows NT 4.0 betrieben werden und als Klient in einem Windows NT-Netzwerk arbeiten. Die PCs können mit einem Diskettenlaufwerk ausgestattet sein. Auf sicherheitsspezifische Aspekte von einzelnen Windows NT-Anwendungen wird nur am Rande eingegangen. Die Fachbereichs-Verwaltung hat ihre Arbeitsplatzrechner mit Windows NT 4.0 (bis auf drei Ausnahmen) ausgestattet.

Unix-System:
Ein SUN-Arbeitsplatzrechner arbeitet unter einem Unix-Betriebssystem.

Allgemeines System:
Es gibt Rechner unter MacOS8, die hier betrachtet werden sollen.

Vernetzte Systeme

Servergestütztes Netz:
Betrachtet wird ein lokales Netz mit mindestens einem Server. Die Clients können PCs mit oder ohne Festplatte sein, aber auch Unix-Workstations oder Terminals. Dieses ist jedoch unabhängig vom Netzbetriebssystem bzw. den Betriebssystemen der Clients. Dafür sind die weiterführenden Abschnitte (z.B. Server-Betriebssysteme) zu beachten.

Windows NT-Netz:
Betrachtet wird ein Windows NT Netzwerk, das als Client-Server-System unter dem Betriebssystem Windows NT 4.0 betrieben wird. Dies betrifft den NT-Server der Verwaltung, der vom Fachbereichs-Rechenzentrum betrieben und gewartet wird, auch in dessen Räumlichkeiten untergebracht ist. Außerdem ist der folgende Baustein zu betrachten:

Datenübertragungseinrichtungen

Email:
Die Fachbereichs-Verwaltung hält für ihre Mitarbeiter einen Emailzugang über den POP3-

Server des Fachbereichs-Rechenzentrums vor.

Telekommunikation

TK-Anlage:
Die Fachbereichs-Verwaltung nutzt die Telekommunikationsanlage des Fachbereichs.

Faxgerät:
Die Fachbereichs-Verwaltung hält ein Faxgerät vor. Für den IT-Grundschutz werden auch bei der Informationsübermittlung per Fax Gefährdungen angenommen.

Sonstige IT-Komponenten

Standardsoftware:
Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten wird und im allgemeinen über den Fachhandel, z. B. über Kataloge, erworben werden kann. Sie zeichnet sich dadurch aus, daß sie vom Anwender selbst installiert werden soll und daß nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist. Die Fachbereichs-Verwaltung nutzt bei Ihrer Arbeit u.a. Standardsoftware.

Datenbanken:
Die Fachbereichs-Verwaltung nutzt die Datenbanksysteme Access und Oracle, letzteres zunehmend weniger.

4.3 Fachbereichs-Rechenzentrum

4.3.1 Grundschutzanalyse des Rechenzentrumsbetriebs

Es soll Grundschutz nach dem Grundschutzhandbuch 1998 des BSI realisiert werden. Dazu werden die typischen Gefährdungen erfaßt und Maßnahmen zusammengestellt, um ein Grundschutzniveau zu erreichen. Als Ergebnis der Grundschutzanalyse wird die Anwendung der Grundschutz-„Bausteine“ für folgende IT-Komponenten der Bibliothek vorgeschlagen:

Übergeordnete Komponenten

Hier werden, wie im Beispiel der Fachbereichs-Bibliothek und der Verwaltung, die folgenden Komponenten betrachtet:
Organisation:
Gefährdungen, auf die Organisation und Regelung der Arbeitsabläufe zurückzuführen sind .

Personal:
Gefährdungen, die aus der Abhängigkeit des Fachbereichs-Rechenzentrums von ihren Beschäftigten bestehen.

Notfallvorsorge-Konzept:
Der mögliche Ausfall des IT-Systems als Gefährdung für das Fachbereichs-Rechenzentrum.

Datensicherungskonzept:
Der mögliche Verlust gespeicherter Daten als Gefährdung für die Abläufe im Fachbereichs-Rechenzentrum.

Infrastruktur

Gebäude:
Für das Fachbereichs-Rechenzentrum ist als Gebäude das Haus D zu betrachten.

Verkabelung:
Die Verkabelung von IT-Systemen umfaßt alle Kabel und Komponenten der Netze vom Übergabepunkt aus einem Fremdnetz (WIN-Anschluß) bis zu den Anschlußpunkten der Netzteilnehmer. Die Verkabelung wird im Rahmen einer detaillierten Risikoanalyse untersucht und deshalb hier nicht betrachtet.

Büroräume:
Als Büroräume werden die Mitarbeiterbüros im Haus D betrachtet.

Serverraum:
Es gibt im Fachbereichsrechenzentrum keinen isolierten Serverraum. Die Server stehen verteilt im Operatorraum, in Kellerräumen sowie in weiteren Räumen. Sinngemäß soll trotzdem dieser

Baustein auf die betreffenden Räume sowie die fachbereichsöffentlichen Rechnerräume (Poolräume) angewandt werden, da dieser Baustein dem Charakter der Laborräume, Poolräume und Operatorräume am Nächsten kommt.

Datenträgerarchiv:
Es gibt im Fachbereichsrechenzentrum zwei Datenarchive: ein Archiv für die Aufbewahrung der Backupmedien für das tägliche Backup und ein großes Archiv im Keller des Hauses D.

Raum für technische Infrastruktur: Der Operatorraum im Haus D sowie einige Kellerräume dienen als Schnittstelle zur externen Infrastruktur (Einspeisungspunkte, etc.) sowie als Verteilpunkt für die hausinterne Infrastruktur. Deshalb wird dieser Baustein hier angewandt.

Schutzschränke:
Es gibt einen Stahlschrank im Keller von Haus D, der gegen Einbruch und Feuer gesichert ist und mittels Alarmgebern abgesichert sein soll.

Nicht vernetzte Systeme

UNIX-System:
Betrachtet wird ein Unix-System als Klientsystem. Das Fachbereichs-Rechenzentrum hält UNIX-Workstations in Rechner-Pools zur Benutzung durch die Studenten sowie in den Mitarbeiterbüros und Administrationsräumen vor.

Tragbarer PC:
Im Rechenzentrum werden - u.a. zur Ausleihe an Lehrveranstalter - Laptops bereitgehalten.

PC unter Windows NT:
Betrachtet werden PCs, die unter dem Betriebssystem Windows NT 4.0 betrieben werden und als Klient in einem Windows NT-Netzwerk arbeiten. Das Fachbereichs-Rechenzentrum hält einen Pool von Windows NT-PCs zur Benutzung durch die Studenten vor.

Allgemeines nicht vernetztes System:
Dieser Baustein bietet einen Überblick über Gefährdungen und IT-Sicherheitsmaßnahmen, die für nicht vernetzte IT-Systeme typisch sind. Dieser Überblick ist unabhängig vom eingesetzten Betriebssystem und wird deshalb hier angewandt. Desweiteren sind die betriebssystemspezifischen Bausteine zu betrachten.

Vernetzte Systeme

Servergestütztes Netz:
Betrachtet wird ein lokales Netz mit mindestens einem Server. Die Clients können PCs mit oder ohne Festplatte sein, aber auch Unix-Workstations oder Terminals. Das Fachbereichs-Rechenzentrum hält mehrere Serversysteme vor. Deshalb wird dieser Grundschutz-Baustein

hier betrachtet. Zusätzlich werden noch spezifische Gefährdungen der einzelnen Server-Betriebssysteme betrachtet.

Windows NT-Netz:
Betrachtet wird ein Windows NT Netzwerk, daals Client-Server-System unter dem Betriebssystem Windows NT 4.0 betrieben wird. Dies betrifft den NT-Server des Fachbereichs-Rechenzentrums, mit dem der u.a. auch Klienten in der Fachbereichsverwaltung vernetzt sind. Außerdem gibt es einen Windows-NT-(Netz-)Poolraum im Rechenzentrum.

Vernetzte UNIX-Systeme:
Das Rechenzentrum hält Unix-Systeme (Server) von SUN vor, die unter dem Bestriebssystem Solaris laufen.

Heterogene Netze:
Im Fachbereichsrechenzentrum werden verschiedene Netze miteinander gekoppelt. Die Netzkomponenten werden in einer detaillierten Risikoanalyse untersucht. Deshalb wird dieser Baustein hier nicht angewandt.

Datenübertragungseinrichtungen

Modem:
Den Mitarbeitern stehen Modems zur Einwahl in das Fachbereichsrechenzentrum zur Arbeit und zu administrativen Zwecken zur Verfügung.

Firewall:
Zum Schutz vor äußeren Angriffen wird das Fachbereichsnetz mit einem Firewallsystem gesichert, das vom Fachbereichsrechenzentrum betrieben wird.

Email:
Die Datenübertragungseinrichtungen werden in einer detaillierten Risikoanalyse separat betrachtet. Deshalb wird dieser Baustein hier nicht angewandt.

Telekommunikation

TK-Anlage:
Das Fachbereichs-Rechenzentrum nutzt die Telekommunikationsanlage des Fachbereichs.

Faxgerät:
Das Fachbereichs-Rechenzentrum hält ein Faxgerät vor. Deshalb kommt dieser Baustein zur Anwendung.

Anrufbeantworter:
Es wird der Anrufbeantworter der DFN CERT GmbH mitbenutzt. Da dieser im Rahmen einer hochschutzbedürftigen Absicherung dieser Einrichtung bereits erfaßt ist, wird dieser Baustein

hier nicht angewandt.

LAN-Anbindung eines IT-Systems über ISDN:
Ein Modem des Rechenzentrums ist ein ISDN-Modem, insofern kommt dieser Baustein zur Anwendung.

Sonstige IT-Komponenten

Standardsoftware:
Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten wird und im allgemeinen über den Fachhandel, z. B. über Kataloge, erworben werden kann. Sie zeichnet sich dadurch aus, daß sie vom Anwender selbst installiert werden soll und daß nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

Datenbanken:
Dieser Baustein wird angewendet, da im Rechenzentrum Datenbanken, z.B. Oracle, laufen.

4.3.2 Detaillierte Analyse des Emailverkehrs und des Netzbetriebs

Ermittlung der Schutzbedürftigkeit

In einem ersten Schritt werden die IT-Anwendungen und der zu verarbeitenden Informationen erfaßt, die mit Emailverkehr und Netzbetrieb im Fachbereichs-Rechenzentrum in Zusammenhang stehen.

IT-Anwendungen sind:
1. Mailserver
2. Internetanbindung
3. Internes Fachbereichsnetz
4. Netzoperating, Netzüberwachung

Verarbeitete Informationen:
5. Emails
6. Nutzdaten, die übers Netz gehen
7. Netzwerksteuerungsdaten
8. Logdaten

Bewertung der IT-Anwendungen und der zu verarbeitenden Informationen

Die Verfügbarkeit und Integrität der Internetanbindung und des Mailservers sind im Interview explizit als erste bzw. zweite Priorität genannt worden. Die Internetanbindung sowie die Verfügbarkeit des internen Netzes sind dabei Voraussetzung für den Betrieb des Mailservers. Die Nichtverfügbarkeit würde zu Beanstandungen, jedoch zu keinen finanziellen Forderungen seitens der Nutzer führen. Insofern ist hier maximal ein mittleres Schadenspotential anzunehmen. Emails werden als vertraulich angesehen, ebenso Logdaten, mit denen sich Benutzerverhalten

Tabelle 4.3: Risikoanalyse Emailverkehr und Netzbetrieb - Bewertung der IT-Anwendungen und Informationen

	Verfügbarkeit	**Integrität**	**Vertraulichkeit**
1. Mailserver	2	2	0
2. Internetanbindung	3	3	0
3. Internes Fachbereichsnetz	2	3	0
4. Netzoperating, Netzüberwachung	2	2	0
5. Emails	2	2	3
6. Nutzdaten, die übers Netz gehen	0	2	1
7. Netzwerksteuerungsdaten	2	2	0
8. Logdaten	2	3	3

nachvollziehen läßt. Ohne integre Netzwerksteuerungsdaten und Logdaten läßt sich kein Netzwerkoperating durchführen. Die Integrität dient dabei vor allem der Nachweisbarkeit. Mehr als mittleres Schadensniveau wird nicht angenommen, da der Rechenzentrumsbetrieb nach eigenen Angaben keine Verfügbarkeitsgarantien und Funktionsgarantien zu erfüllen hat (siehe Interview im Teil II). Die Bewertung ist in der Tabelle 4.3 zusammengefaßt dargestellt.

Erfassung der Risikobereitschaft

Der maximal tragbare Schaden wird vom Rechenzentrum[3] mit einem Betrag von 100.000 DM im Jahr angegeben. Daraus resultiert die Tabelle 4.4, die für die jeweilige Kombination von Schadenswert und Häufigkeitswert angibt, ob dieses Risiko tragbar (T) oder untragbar (U) wäre.

Zeilen: Schadenswert (0 ... 4+)
Spalten: Häufigkeitswert (0- ... 4)

Ergebnisse der Bedrohungs- und der Risikoanalyse

Es sind wenige Risiken für den Netzverkehr und den Emailbetrieb im Fachbereichs-Rechenzentrum identifiziert worden. Dies ist darauf zurückzuführen, daß bereits viele Maßnahmen ergriffen worden sind, die in die Analyse mit einfließen. Als untragbare Risiken ergeben sich für den Netzverkehr und den Emailbetrieb die folgenden:

Die Verfügbarkeit des Netzes wird durch häufigen Blitzeinschlag bedroht. Ebenso bedroht ist dadurch der Emailserver. Es werden jedoch bereits Maßnahmen ergriffen, so die Verkabelung

[3]nach Angabe des Leiters des Fachbereichs-Rechenzentrums

Tabelle 4.4: Risikoanalyse Emailverkehr und Netzbetrieb - Erfassung der Risikobereitschaft

	0–	0	1	2	3	4
4+ katastrophal	U	U	U	U	U	U
4 existenzgefährdend	T	U	U	U	U	U
3 großer Schaden	T	T	U	U	U	U
2 mittlerer Schaden	T	T	T	U	U	U
1 geringer Schaden	T	T	T	T	U	U
0 unbedeutend	T	T	T	T	T	U

mittels Glasfaser, die insofern schadensmindernd wirkt, daß ein Blitzeinschlag in Netzkomponenten nicht in die angrenzenden Gebäude weitergeleitet werden kann. Der Schaden bliebe auf ein Teilnetz beschränkt, stellt dann jedoch trotzdem einen Sachschaden dar, der als untragbar angesehen wird.

Durch Blitzeinschlag ist zudem die Stromversorgung gefährdet. Dies betrifft die Stromzufuhr zu allen Netzkomponenten und zum Emailserver. Es gibt derzeit Schutzsteckdosenleisten, jedoch kein integriertes Blitzschutzkonzept.

Neben der Gefahr von Blitzeinschlägen sind vor allem Verfügbarkeit und Integrität der Router, des ATM-Switches, der Netzwerkkabel und -dosen sowie des Firewallrechners durch spontane Fehler oder Ausfall bedroht.

4.4 Arbeitsbereich AGN

4.4.1 Ergebnisse der Grundschutzanalyse des Arbeitsbereichs AGN

Als Ergebnis der Grundschutzanalyse wird die Anwendung der Grundschutz-„Bausteine“ für folgende IT-Komponenten der Bibliothek vorgeschlagen:

Übergeordnete Komponenten

Hier werden, wie im Beispiel der Fachbereichs-Bibliothek und der Verwaltung, die folgenden Komponenten betrachtet:

Organisation:
Gefährdungen, auf die Organisation und Regelung der Arbeitsabläufe zurückzuführen sind .

Personal:
Gefährdungen, die aus der Abhängigkeit des Arbeitsbereichs AGN von ihren Beschäftigten bestehen.

Notfallvorsorge-Konzept:
Der mögliche Ausfall des IT-Systems als Gefährdung für den Arbeitsbereich AGN.

Datensicherungskonzept:
Der mögliche Verlust gespeicherter Daten als Gefährdung für die Abläufe im Arbeitsbereich AGN.

Infrastruktur

Gebäude:
Der Arbeitsbereich AGN ist hauptsächlich im Gebäude Haus C, Erdgeschoß, untergebracht. Es befindet sich zudem im 1. Stockwerk ein gemeinsam mit einem anderen Arbeitsbereich genutzter Kopierer.

Verkabelung:
Von Seiten der Hausverwaltung wurde die Verkabelung mit 230 V Netzspannung besorgt. Die Verkabelung mit Datenkabeln ist größtenteils vom AB selbst vorgenommen worden.

Büroraum:
Der Büroraum ist ein Raum, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort der Erledigung ihrer Aufgaben evtl. auch IT-unterstützt nachzugehen. Diese Aufgaben können aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.

Wird jedoch ein Büroraum überwiegend zur Archivierung von Datenträgern genutzt, ist zusätzlich der Abschnitt Datenträgerarchiv zu beachten. Ist in einem Büroraum ein Server (LAN, TK-Anlage, o.ä.) aufgestellt, ist zusätzlich der Abschnitt Serverraum zu beachten.
Für die Mitarbeiter und für Studierende in der Studienabschlußphase stehen Büroräume im Arbeitsbereich AGN zur Verfügung.

Serverraum:
Der Serverraum dient in erster Linie zur Unterbringung eines Servers, z.B. eines LAN-Servers, eines Unix-Zentralrechners oder eines Servers für eine TK-Anlage. Als Serverräume sind im Arbeitsbereich AGN die Laborräume des AVTC und das VTC/NTC-Labor zu betrachten.

Datenträgerarchiv:
Das Datenträgerarchiv dient der Lagerung von Datenträgern jeder Art. Im Rahmen des IT-Grundschutzes werden an den Archivraum hinsichtlich des Brandschutzes keine erhöhten Anforderungen gestellt. Der Brandschutz kann entsprechend den Bedürfnissen des IT-Betreibers durch die Behältnisse, in denen die Datenträger aufbewahrt werden, realisiert werden.
Im Arbeitsbereich AGN werden Datenträger zum einen in einem feuersicheren Safe gelagert, zum anderen in normalen Holzschränken im Laborraum AVTC.

Raum für technische Infrastruktur:
In Räumen für technische Infrastruktur sind in der Regel solche Geräte und Einrichtungen untergebracht, die keine oder nur eine seltene Bedienung durch einen Menschen benötigen. Das VTC/NTC-Labor hat u.a. diese Funktion.

Schutzschränke:
Es existiert ein Safe der Sicherheitsklasse F90, der im Arbeitsbereich untergebracht ist. Darüberhinaus gibt es keine Schutzschränke, insbesondere keine Serverschutzschränke im Arbeitsbereich AGN.

Nicht vernetztes System

Unix-System:
Zu betrachten ist zum einen eine SUN-Workstation in einem Büro, desweiteren Testrechner unter dem Betriebssystem Linux als Klienten im Testnetz.

Tragbarer PC:
Betrachtet wird ein Laptop des AB-Leiters, der u.a. für Lehrezwecke eingesetzt wird. Darüberhinaus sind einige private Laptops am Arbeitsbereich, die jedoch nicht der Kontrolle und Sicherung durch den AB unterliegen. Hier ist eher darauf zu achten, daß davon keine Gefahr für den Arbeitsbereich ausgeht.

DOS-PC (mehrere Benutzer):
Zum Virentest sowie zu anderen Testzwecken werden u.a. DOS-Rechner eingesetzt. Diese wer-

den in diesem Abschnitt betrachtet. Die Virendatenbank und das AVTC-Netz wird jedoch extra in einer detaillierten Analyse untersucht.

PC mit Windows 95:
Am Arbeitsbereich wird nicht mehr Windows 95, sondern Windows 98 eingesetzt. Da hierfür noch kein Grundschutz-Baustein vorhanden ist, wird der Grundschutzbaustein für Windows 95-Rechner angewandt, da dieser den betrachteten Systemen am Nächsten kommt. Am Arbeitsbereich werden in den Büros und Labors Windows 98-Rechner eingesetzt.

Allgemeines nicht vernetztes IT-System:
Zu betrachten sind weitere Rechner, u.a. 2 Commodore Amiga-Rechner und PCs unter dem Betriebssystem OS/2. Für den IT-Grundschutz wird hierfür dieser allgemeine Baustein angewandt.

Vernetzte Systeme

Servergestütztes Netz:
Betrachtet wird ein lokales Netz mit mindestens einem Server. Dieser Abschnitt bietet einen Überblick über Gefährdungen, die für lokale Netze typisch sind. Dieser Überblick ist jedoch unabhängig vom Netzbetriebssystem bzw. den Betriebssystemen der Clients. Hierfür sind die weitergehenden betriebssystemspezifischen Abschnitte zu betrachten.

Vernetzte Unix-Systeme:
Es werden mehrere Rechner als Linux-Server eingesetzt, u.a. „Vertigo“ als Firewall, „Archeron“ und „Blomquist“ als Samba-Server.

Windows NT Netz:
Neben dem NT-Server des AVTC, der gesondert untersucht wird, wird der Webserver unter Windows NT betrieben. Hierfür findet dieser Baustein Anwendung.

Datenübertragungseinrichtungen

Datenträgeraustausch:
Zur Datenübertragung werden Disketten, CDs und Magnetbänder eingesetzt.

Modem:
Die Mailbox des Antivirus-Projektes ist per Modem von außen zu erreichen.

Firewall:
Zum Schutz vor äußeren Angriffen dient der Firewallrechner „Vertigo“ des Arbeitsbereiches.

E-Mail:
Email steht über den POP-Server des Fachbereichs-Rechenzentrums zur Verfügung und kann via Firewall im Arbeitsbereichsnetz gelesen werden.

Telekommunikation

TK-Anlage:
Es ist die TK-Anlage des Fachbereichs zu betrachten.

Fax-Gerät:
Am Arbeitsbereich wird im Sekretariat ein Faxgerät vorgehalten.

Sonstige IT-Komponenten

Standardsoftware:
An Standardsoftware werden das Officepaket Microsoft Office 97 Professional, Internet-Explorer, Netscape Navigator u.a. eingesetzt. Deshalb findet dieser Grundschutzbaustein hier Anwendung.
Datenbanken:
Die Datenbank des Drittmittelprojekts BADO ist in eine hohe Schutzkategorie eingeteilt, wird jedoch in der vorliegenden Arbeit nicht detailliert untersucht. Deshalb soll an dieser Stelle wenigstens mittlerer Schutz realisiert werden.

4.4.2 Ergebnisse der detaillierten Analyse der Virus-Datenbank

Die detaillierten Analyse der Virus-Datenbank hat ergeben, daß Risiken bestehen, die als untragbar einzustufen sind. Als Schwachstellen sind zunächst u.a. identifiziert worden:

- Es gibt eine ungeschützte Übertragungsleitung zum Drucker, die zudem durch ein fremdes Büro führt. Ein Datenabzug über die Druckerschnittstelle ist möglich.
- Reinigungspersonal hat jeden Morgen unbeaufsichtigt Zutritt zum Raum, in dem der Server mit der Virus-Datenbank steht.
- Es treten im Bereich der Stromversorgung Spannungsschwankungen auf.
- Erhöhte Temperaturen in C 116, vor allem im Sommer, könnten den NT-Server und die Test-PCs gefährden.
- Es besteht keine Möglichkeit zu schneller Ersatzbeschaffung, da hierfür kein Budget vorhanden ist.
- Backup-Bänder werden sehr nah am IT-System aufbewahrt. Es gibt kein aktuelles externes Backup. Nur manchmal, wenn der Safe nicht mehr zugreifbar ist, nimmt der Administrator über Nacht ein Backup mit nach Hause.
- Backup-Bänder liegen teilweise unbeaufsichtigt im AVTC-Raum. Da viele Bänder benutzt werden, kann tagsüber trotz Aufsicht leicht eines abhanden kommen oder gestohlen werden. Verstärkt wird die Schwachstelle dadurch, daß das Backup unverschlüsselt erfolgt.

- Es besteht eine Möglichkeit zum Abhören oder Verfälschen der Kommunikation zwischen LAN und Drucker in einem unkontrollierbaren (fremden) Büroraum, durch den das Kabel läuft.
- Es gibt keine Dokumentation der Serverkonfiguration. Nur 1 Administrator weiß, wie alles geht. Bei Ausfall des Hauptadministrators sind Informationen über die konkrete Serverkonfiguration und notwendige Skripte nicht mehr vorhanden. Ein neuer Administrator muß sich dann erst einarbeiten - Verzögerung - und ggf. einiges umkonfigurieren.
- Unvorhergesehenes und unnachvollziehbares Verhalten (z.B. Kopieren der Virendatenbank) von Teammitgliedern ist nicht auszuschließen.
- Es gibt gelegentliche Inkonsistenzen in der Virendatenbank, die aber schnell behoben werden können.
- Unentdeckbare physikalische Angriffsmöglichkeit auf den NT-Server: Vor der UPS Stromausfall simulieren (kommt sowieso 3 mal im Jahr vor). Dann fährt der Server herunter und meldet nur, daß ein Stromausfall da war. Mehr kann nicht registriert werden. Dann aufschrauben, SCSI-Kabel an der Karte abziehen und in externes Gerät stecken. Strom wieder an (Rechner registriert das nicht im Logfile!), Images aller Platten (ca. 3 Stunden) ziehen und alles wieder zuschrauben.

Nach der Untersuchung der Schwachstellen werden Risiken im Bereich der Infrastruktur vor allem durch die Möglichkeit von Blitzeinschlag, Stromausfall und - allgemein - höherer Gewalt gesehen.
Die Verfügbarkeit der Räume C 116 und C 107 sowie die Verfügbarkeit und Integrität der Stromversorgung sind durch die Möglichkeit eines Blitzeinschlages oder Flugzeugabsturzes (Höhere Gewalt) bedroht. Weitere Bedrohungen für die Verfügbarkeit der Räume bestehen durch die nicht auszuschließende Möglichkeit eines Anschlages (z.B. Brandanschlag) oder Ausbruch von Feuer. Pro Jahr werden 2 relevante Blitzeinschläge im Gelände des Fachbereiches bzw. unmittelbarer Umgebung registriert.
Ein Stromausfall oder Überspannung werden am NT-Server der Virusdatenbank nur durch eine USV abgefangen, ein mehrstufiges Blitzschutzkonzept unter Einschluß des Gebäudes gibt es nicht.

Im Bereich der Hardware werden Risiken für die Verfügbarkeit und Integrität des NT-Servers, der Test-PCs und der Netzkomponenten durch mögliches technisches Versagen und mögliche menschliche Fehlhandlungen gesehen.

Im Bereich der Datenträger ist das Risiko des Diebstahls und der Beschädigung von Streamer-Bändern, MO-Medien, und Installationsmedien als relevant einzustufen.

Im Bereich der Software bestehen Risiken durch Fehler im Betriebssystem des NT-Servers und Fehler in Testroutinen und Auswertung aufgrund fehlerhafter Software. Dies kann die Verfügbarkeit der Virendatenbank sowie den Viren-Scanner-Test beeinflussen. Auch besteht ein

Risiko, daß die Virus-Datenbank durch unberechtigten Zugang zum Server entweder direkt oder über das Netzwerk kopiert werden kann.

Die Bedrohung der Verfügbarkeit und Integrität der Virus-Datenbank durch Hardwaredefekte, fehlerhafte Software oder menschliche Fehlhandlungen (absichtlich oder unabsichtlich) ist ebenfalls als Risiko anzusehen. Die Vertraulichkeit der Virus-Datenbank ist durch die Möglichkeit des unberechtigten Kopierens im Falle der Kompromittierung des NT-Servers bedroht. Diese Bedrohung hat das größte Schadenspotential, demzufolge sollten die Maßnahmen hier priorisiert realisiert werden.

Ein hohes Risiko hinsichtlich der Verfügbarkeit ergibt sich durch die Zentrierung der Administration auf eine Person. Fällt diese aus, kann im Extremfall der NT-Server nicht fachkundig administriert werden, da diverse Einstellungen vorgenommen und Skripte geschrieben wurden, die nicht oder nur wenig dokumentiert sind.

Das Druckerkabel birgt das Risiko, daß jemand unberechtigt die Kommunikation zwischen AVTC-LAN und Drucker beobachtet und mithört.

4.5 Arbeitsbereich SWT

Es soll Grundschutz nach dem Grundschutzhandbuch 1998 des BSI realisiert werden. Dazu werden die typischen Gefährdungen erfaßt und Maßnahmen zusammengestellt, um ein Grundschutzniveau zu erreichen.

4.5.1 Grundschutzanalyse des Arbeitsbereichs SWT

Als Ergebnis der Grundschutzanalyse wird die Anwendung der Grundschutz-„Bausteine“ für folgende IT-Komponenten des Arbeitsbereichs vorgeschlagen:

Übergeordnete Komponenten

Hier werden Gefährdungen betrachtet, die sich pauschal auf den gesamten Betrieb erstrecken und nicht einzelnen IT-Anwendungen zuordnen lassen. Dazu gehören:

Organisation:
Gefährdungen, auf die Organisation und Regelung der Arbeitsabläufe zurückzuführen sind .

Personal:
Gefährdungen, die aus der Abhängigkeit des Arbeitsbereichs von Beschäftigten bestehen.

Notfallvorsorge-Konzept:
Der mögliche Ausfall des IT-Systems als Gefährdung für den Arbeitsbereich.

Datensicherungskonzept:
Der mögliche Verlust gespeicherter Daten als Gefährdung für die Abläufe im Arbeitsbereich betrachtet.

Infrastruktur

Gebäude:
Für den Arbeitsbereich Softwaretechnik (SWT) ist das Gebäude Haus D (1. Stock) zu betrachten.
Verkabelung Im Arbeitsbereich Softwaretechnik wird vollständig auf die Verkabelung durch die Haustechnik (230 V) und durch das Rechenzentrum zurückgegriffen. Im Interesse des reibungslosen Betriebs im Arbeitsbereich SWT ist die Verkabelung trotzdem Bestandteil der Untersuchung. Der Arbeitsbereich müßte sich hinsichtlich der Maßnahmen dann ggf. mit der Haustechnik-Abteilung und dem Rechenzentrum verständigen.

Büroräume:
Als Büroräume werden hier die Laborräume (Rechnerräume) des Arbeitsbereichs sowie die Mitarbeiterbüros im Haus D betrachtet.

Häusliche Arbeitsplätze:
Werden dienstliche Aufgaben in der häuslichen Umgebung und nicht in Räumen der Universität wahrgenommen, sind Sicherheitsmaßnahmen zu ergreifen, die eine mit einem Büroraum vergleichbare Sicherheitssituation erreichen lassen. Bei einem häuslichen Arbeitsplatz kann nicht die infrastrukturelle Sicherheit, wie sie in einer behördlichen Büroumgebung anzutreffen ist, vorausgesetzt werden. Besucher oder Familienangehörige haben oftmals Zutritt zu diesem Arbeitsplatz. Die MitarbeiterInnen des Arbeitsbereichs SWT nutzen ihren häuslichen Arbeitsplatz, um z.B. Dissertationen zu schreiben oder Lehrveranstaltungen vorzubereiten.

Nicht vernetzte Systeme/ Clientsysteme

Unix-Systeme:
Betrachtet werden SUN-Workstations, die unter dem Betriebssystem Solaris laufen.

PC unter Windows NT:
Betrachtet werden PCs, die unter dem Betriebssystem Windows NT 4.0 betrieben werden und als Klient in einem Windows NT-Netzwerk arbeiten.

Allgemeines nicht vernetztes IT-System:
Am Arbeitsbereich Softwaretechnik werden Macintosh-Systeme unter dem Betriebssystem MacOS 8 betrachtet. Da das IT-Grundschutzhandbuch für Systeme unter dem Betriebssystem MacOS8 keinen Maßnahmenkatalog vorschlägt, wurde dieser allgemeine Baustein ausgewählt, um ein adäquates Sicherheitsniveau zu erreichen.

Vernetzte Systeme

Servergestütztes Netz:
Betrachtet wird das lokale Arbeitsbereichsnetz, in dem sich mehrere Server befinden. Die Klienten sind PCs, darüberhinaus gibt es auch Unix-Workstations. Es besteht eine Kopplung mit dem Fachbereichsnetz. Dieser Baustein betrachtet Gefährdungen, die für lokale Netze typisch sind. Zusätzlich sind die Bausteine für die konkreten Netzsysteme, Server und Klienten zu realisieren.

Windows NT-Netz:
Betrachtet wird ein Windows NT Netzwerk, das als Client-Server-System unter dem Betriebssystem Windows NT 4.0 betrieben wird. Dies betrifft den NT-Server des Arbeitsbereichs SWT.

Vernetzte UNIX-Systeme:
Vernetzte Unix-Systeme sind Rechner mit dem Betriebssystem Unix, die in einem Netz Dienste anbieten (Server), die von anderen IT-Systemen in Anspruch genommen werden können, oder solche nutzen (Clients).

Datenübertragungseinrichtungen

Datentägeraustausch:
Betrachtet wird der Austausch von Datenträgern zur Datenübertragung zwischen den Rechnern in der Universität und in häuslichen Mitarbeiterarbeitsplätzen. Berücksichtigte Datenträger sind Disketten, Wechselplatten (magnetisch, magnetooptisch), CDs, Magnetbänder und Kassetten. Daneben wird auch die Speicherung der Daten auf dem Sender- und Empfänger-System, soweit es in direktem Zusammenhang mit dem Datenträgeraustausch steht, sowie der Umgang mit den Datenträgern vor bzw. nach dem Versand berücksichtigt.

Email:
Der Arbeitsbereich SWT hält für seine Mitarbeiter einen Emailzugang über das Fachbereichsrechenzentrum vor.

Telekommunikation

TK-Anlage:
Der Arbeitsbereich SWT nutzt die Telekommunikationsanlage des Fachbereichs.

Faxgerät:
Der Arbeitsbereich SWT hält ein Faxgerät vor.
Für den IT-Grundschutz werden bei der Informationsübermittlung per Fax folgende typische Gefährdungen angenommen:

Anrufbeantworter:
Im Arbeitsbereich Softwaretechnik wird ein Anrufbeantworter eingesetzt. Deshalb wird dieser Baustein angewendet. Ein Gefährdungspotential ergibt sich insbesondere aus dem heute üblichen Merkmal der Fernabfrage von Anrufbeantwortern.

Sonstige IT-Komponenten

Standardsoftware:
Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten wird und im allgemeinen über den Fachhandel, z.B. über Kataloge, erworben werden kann. Sie zeichnet sich dadurch aus, daß sie vom Anwender selbst installiert werden soll und daß nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist. Der Arbeitsbereich SWT nutzt Standardsoftware für Lehre, Forschung und Verwaltungstätigkeiten, z.B. MS Office 97, Netscape, JDK und Java Workshop.

Datenbanken:
Der Arbeitsbereich SWT nutzt in geringem Umfang das Datenbanksystem Access aus dem MS Office-Paket. Deshalb sollte der entsprechende IT-Grundschutz-Baustein realisiert werden.

4.6 Folgerungen aus den Grundschutz- und Risikoanalysen

Die Grundschutz- und Risikoanalysen zeigen Gefährdungen auf, gegen die Maßnahmen getroffen werden können bzw. müssen, um das Risiko für den IT-Betrieb gering zu halten oder zu verringern. Gerade die detaillierten Risikoanalysen zeigen darüberhinaus, daß die Entscheidung, ob ein Risiko tragbar ist oder nicht, u.a. vom IT-Budget der einzelnen Fachbereichseinrichtung abhängt.

Bei der Auswahl von IT-Sicherheitsmaßnahmen kommt es deshalb darauf an, das IT-Budget der Fachbereichseinrichtung zu entlasten, indem Maßnahmen nicht isoliert realisiert werden, sondern nach Möglichkeit gemeinsame Schutzinteressen mehrerer oder aller Fachbereichseinrichtungen gemeinsam umgesetzt werden.

Kapitel 5

IT-Sicherheitsempfehlungen

Während im Rahmen dieser Arbeit zunächst einzelne Empfehlungen für die Fachbereichseinrichtungen ausgearbeitet werden[1], soll es in diesem Kapitel darum gehen, die Einzelempfehlungen zu einem Gesamtkonzept für den Fachbereich zu vereinen. Dafür wird das folgende mehrstufige Konzept vorgeschlagen.

1. Der Fachbereich als Ganzes nimmt übergeordnete Aufgaben wahr. Zum einen sind dies diejenigen Aufgaben, die der Fachbereich als juristische Person übernehmen muß (z.B. Auftritt nach Außen, Organisationssicherheit), zum anderen übernimmt der Fachbereich die Sicherstellung der Versorgung (Sicherstellung der Stromversorgung, Telekommunikation) sowie die Notfallvorsorge (Einbruchschutz, Brandschutz, Katastrophenschutz).

2. Die Fachbereichseinrichtungen realisieren darauf aufbauend in ihrer Einrichtung ein Grundschutzniveau.

3. Für die hochschutzbedürftigen IT-Systeme sind dann IT-Sicherheitsmaßnahmen durch eine detaillierte Risikoanalyse zu finden.

5.1 Aufgaben des Fachbereichs

Der Fachbereich stellt den Fachbereichseinrichtungen eine Infrastruktur zur Verfügung. Diese muß sichergestellt werden, um die Fachbereichseinrichtungen von der Notwendigkeit eigener Maßnahmen in diesem Bereich zu entlasten. Für die IT ist vor allem die Sicherstellung der Verfügbarkeit und Integrität der Gebäude, Kommunikation und Stromversorgung wichtig.

Der Fachbereich sollte zudem gegen diejenigen Risiken, die alle Fachbereichseinrichtungen gleichermaßen betreffen, entsprechende Maßnahmen ergreifen. Die Notwendigkeit hierzu ergibt sich u.a. dann, wenn bei Eintreten von Ereignissen die Existenz des Fachbereichs bedroht

[1] siehe Teil II

ist oder großer Schaden droht. Gerade bei Umweltereignissen, die im allgemeinen als „höhere Gewalt“ bezeichnet werden, droht ein Schadensausmaß, das für den Fachbereich noch tragbar sein kann, wenn es nur eine einzelne Fachbereichseinrichtung trifft, das aber in der Summe der Schäden vom Fachbereich nicht mehr tragbar ist, wenn mehrere Fachbereichseinrichtungen betroffen sind.

Der Fachbereich sollte also neben der Sicherstellung der Versorgung und Infrastruktur auch Katastrophenvorsorge betreiben, wobei die Maßnahmen z.T. miteinander verwoben sind. Beispielsweise ist Blitzschutz neben Versorgungsschutz auch als Brandschutz zu betrachten.

5.1.1 Sicherstellung der Verfügbarkeit der Stromversorgung

Neben Schutz gegen Überspannung ist auch der Schutz gegen Stromausfall durch äußere Umstände oder durch Fehlkonfiguration oder Kurzschluß wichtig. Hierzu ist umzusetzen:
M 1.1 - Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
M 1.39 - Verhinderung von Ausgleichsströmen auf Schirmungen

Zur Dokumentation sind folgende Maßnahmen zu realisieren:
M 2.25 - Dokumentation der Systemkonfiguration
M 1.11 - Lagepläne der Versorgungsleitungen
M 5.4 - Dokumentation und Kennzeichnung der Verkabelung

Da der plötzlich unvorhergesehene Wegfall der Stromversorgung zu Datenverlusten führen kann, sollte der Fachbereich überlegen, einen zentralen Notstrompuffer von wenigen Minuten zu realisieren, an den die wichtigsten Server der Fachbereichseinrichtungen, sofern diese keinen eigenen Batteriepuffer realisiert haben, angeschlossen werden können. Bei Stromausfall können diese dann über einen Signalisierungskanal zum geordneten Herunterfahren veranlaßt werden.

Ebenso könnte der Fachbereich an einem zentralen Einspeisungspunkt eine Glättung gegen normale Spannungsschwankungen und -spitzen realisieren, um evtl. die Lebensdauer der eingesetzten IT zu erhöhen.

5.1.2 Überspannungs- und Blitzschutz

Blitzschutz ist notwendig, da - wie in der detaillierten Risikoanalyse erfaßt - Blitzeinschläge zum einen hohen Schaden verursachen können und zum anderen regelmäßig im Fachbereich und unmittelbarer Umgebung auftreten. Der Fachbereich sollte auf ein mehrstufiges Blitzschutzkonzept, wie z.B. in [c't 17/1999] beschrieben, hinarbeiten. Hierzu werden in [BSI1998] folgende Maßnahmen vorgeschlagen:
M 1.1 - Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
M 1.5 - Galvanische Trennung von Außenleitungen (optional)
M 1.3 - Angepaßte Aufteilung der Stromkreise
M 1.25 - Überspannungsschutz

M 1.4 - Blitzschutzeinrichtungen
M 1.39 - Verhinderung von Ausgleichsströmen auf Schirmungen
M 5.2 - Auswahl einer geeigneten Netz-Topographie (bei Verkabelung neuer Netze)
M 5.3 - Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht (bei Verkabelung neuer Netze)
M 5.5 - Schadensmindernde Kabelführung (bei Verkabelung neuer Netze)
M 5.1 - Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen

5.1.3 Brandschutz

Zur Vorsorge gegen Feuer sollten Brandschutzvorschriften beachtet (M 1.1- Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften, M 1.6 - Einhaltung von Brandschutzvorschriften und Auflagen der örtlichen Feuerwehr) und regelmäßig deren Einhaltung kontrolliert werden (M 2.15 - Brandschutzbegehungen). Dies wird vom Fachbereich umgesetzt. Der Verhinderung von Bränden dienen auch Blitzschutzanlagen für Gebäude (M 1.4 - Blitzschutzeinrichtungen, siehe auch im vorigen Abschnitt).

Zur Beschleunigung der Entdeckung eines Brandes dienen Brandmelder in den Fluren der Gebäude des Fachbereiches. In besonders kritischen Bereichen wie Rechner-Laboren sollten ebenfalls Brandmelder (M 1.18 - Gefahrenmeldeanlage) installiert werden, da die Melder im Flur ansonsten verspätet anschlagen würden. Die Gebäude sollten regelmäßig inspiziert werden (M 2.18 - Kontrollgänge).

Zur Schadensbegrenzung sollten kritische Bereiche wie Rechnerlabore mit Sicherheitstüren gesichert werden (M 1.10 - Verwendung von Sicherheitstüren). Darüberhinaus werden folgende Maßnahmen vorgeschlagen:
M 1.7 - Regelmäßige Prüfung der Funktion von Handfeuerlöschern
M 1.9 - Brandabschottung von Trassen
M 1.26 - Installation von Not-Aus-Schaltern (an der Ausgangstür von Rechnerlaboren)
M 6.20 - Geeignete Aufbewahrung der Backup-Datenträger

Probealarme und Brandschutzübungen (M 6.17 - Alarmierungsplan und Brandschutzübungen) sollten in Zusammenhang mit Katastrophenübungen durchgeführt werden, um die Wirksamkeit auch der Katastrophenmaßnahmen zu prüfen.

5.1.4 Einbruchschutz

Zur Verminderung der Einbruchgefahr trägt ein Pförtnerdienst und Wachdienst (M 1.17), wie bereits umgesetzt, bei. Zusätzlich sollte die Installation von Sicherheitstüren (M 1.10) auch am Eingang zu Rechnerlaboren sowie die Installation einer Gefahrenmeldeanlage (M 1.18) in den Rechnerlaboren und, in Absprache mit den Fachbereichseinrichtungen, auch in kritischen Bereichen der Fachbereichseinrichtungen realisiert werden.
Einbruchschutz ist detailliert in M 1.19 - Einbruchschutz - beschrieben.

5.1.5 Katastrophenvorsorge

Zunächst ist zu definieren, was als Notfall betrachtet wird (M 6.2), wer in einem solchen Fall zu alarmieren ist (M 6.8 - Alarmierungsplan) und wer für die Umsetzung der einzuleitenden Maßnahmen die Verantwortung trägt (M 6.7 - Regelung der Verantwortung im Notfall).

Als Vorsorge sollten Sofortmaßnahmen geplant werden und in einem Notfall- oder Katastrophenhandbuch zusammengefaßt werden (M 6.3 - Erstellung eines Notfall-Handbuches, M 6.9 - Notfall-Pläne für ausgewählte Schadensereignisse). Dokumentiert werden sollte dabei unbedingt die Systemkonfiguration (M 2.25), es sollten auch Verfahrensschritte zum Wiederanlauf (M 6.11 - Erstellung eines Wiederanlaufplans) und für Ersatzbeschaffungen definiert werden (M 6.14 - Ersatzbeschaffungsplan, M 6.15 - Lieferantenvereinbarungen). Das Notfallhandbuch ist in mindestens zwei Kopien auszufertigen, wobei eine Kopie extern aufbewahrt wird und in kurzer Frist herbeizuschaffen sein muß.

Als weitere Vorsorge sollte im Fachbereich ein Datensicherungskonzept erstellt werden, das den Fachbereich in die Lage versetzt, nach einem katastrophalen Ereignis tatsächlich eine Datenrekonstruktion durchführen zu können. Hierfür sind folgende Maßnahmen umzusetzen:
M 6.36 - Festlegung des Minimaldatensicherungskonzeptes
M 2.137 - Beschaffung eines geeigneten Datensicherungssystems
M 6.20 - Geeignete (externe) Aufbewahrung der Backup-Datenträger
M 6.37 - Dokumentation der Datensicherung
Der Fachbereich sollte im Rahmen seines Datensicherungskonzeptes den Fachbereichseinrichtungen anbieten, Datensicherungen automatisch mit durchzuführen. Zudem sollte der Fachbereich eine externe (entsprechend gesicherte) Aufbewahrungsmöglichkeit für das Backup des Fachbereichs finden (Rechenzentrum oder Bankschließfach) und auch hier den Fachbereichseinrichtungen anbieten, in regelmäßigen Abständen deren Backup-Medien mit einzulagern.

Der Fachbereich sollte im Haushalt ein Budget für Notfallmaßnahmen vorsehen.

Die Notfallprozeduren sind regelmäßig zu üben, dies schließt auch die Datensicherung ein (M 6.12 - Durchführung von Notfallübungen).

5.1.6 Zentrale Bereitstellung von Standardsoftware und -Arbeitsplätzen

Im Fachbereich ist jede Fachbereichseinrichtung selbst zuständig für die Beschaffung von Standardsoftware wie Büropaketen oder Standardbetriebssystemen. Durch die zentrale Beschaffung und Bereitstellung von Standardarbeitsplätzen und -Software kann der Fachbereich auch einen Gewinn hinsichtlich der IT-Sicherheit erzielen, indem eine zentrale Untersuchung und Vorauswahl stattfindet und Installations- und Administrationshilfe gegeben werden kann. Es sollten Sicherheitslücken, die aus falschen oder vergessenen Einstellungen in den Arbeitsplatzrechnern entstehen, so vermieden werden. Maßnahmen hierzu sind:

M 2.79 - Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
M 2.10 - Überprüfung des Software-Bestandes
M 2.80 - Erstellung eines Anforderungskatalogs für Standardsoftware
M 2.69 - Einrichtung von Standard-Arbeitsplätzen
M 2.81 - Vorauswahl eines geeigneten Standardsoftwareproduktes (im Beispiel von Windows NT als Betriebssystem würde als Maßnahme u.a. M 4.76 - Einsatz einer sicheren Systemversion von Windows NT - Beachtung finden)
M 2.82 - Entwicklung eines Testplans für Standardsoftware
M 2.83 - Testen von Standardsoftware
M 2.86 - Sicherstellen der Integrität von Standardsoftware
M 2.84 - Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
M 2.87 - Installation und Konfiguration von Standardsoftware
M 2.89 - Deinstallation von Standardsoftware
M 2.85 - Freigabe von Standardsoftware
M 2.88 - Lizenzverwaltung und Versionskontrolle von Standardsoftware

5.1.7 Bereitstellung der Telekommunikationsanlage

Für die Gewährleistung der Betriebssicherheit der TK-Anlage sollten folgende Maßnahmen umgesetzt werden:
M 2.105 - Beschaffung von TK-Anlagen
M 4.6 - Revision der TK-Anlagenkonfiguration (Soll-Ist-Abgleich)
M 4.5 - Protokollierung der TK-Administrationsarbeiten
M 6.26 - Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
M 6.28 - Vereinbarung über Lieferzeiten lebensnotwendiger TK-Baugruppen
M 2.29 - Bedienungsanleitung der TK-Anlage für die Benutzer

Der Sicherheit gegen Angriffe auf die TK-Anlage von außen dienen folgende Maßnahmen:
M 2.27 - Verzicht auf Fernwartung der TK-Anlage (optional)
M 4.62 - Einsatz eines D-Kanal-Filters (optional)

Der Sicherheit gegen Angriffe auf die TK-Anlage durch unberechtigte Personen dienen die folgenden Maßnahmen:
M 3.13 - Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
M 3.12 - Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
M 4.12 - Sperren nicht benötigter TK-Leistungsmerkmale
M 4.7 - Änderung voreingestellter Paßwörter in der TK-Anlage
M 4.11 - Absicherung der TK-Anlagen-Schnittstellen
M 1.30 - Absicherung der Datenträger mit TK-Gebührendaten
M 4.10 - Paßwortschutz für TK-Endgeräte

Um eine Notruffunktion sicherzustellen, kann eine TK-Anlage i.d.R. entsprechend konfiguriert werden:

M 6.29 - TK-Basisanschluß für Notrufe
M 6.30 - Katastrophenschaltung

5.1.8 Emailnutzung am Fachbereich

Das Rechenzentrum des Fachbereichs stellt einen zentralen Emailserver zur Verfügung. Zur sicheren Nutzung von Email sollten die folgenden Maßnahmen umgesetzt werden:
M 2.118 - Festlegung einer Sicherheitspolitik für E-mail-Nutzung
M 2.119 - Regelung für den Einsatz von E-mail
M 2.122 - Einheitliche E-mail-Adressen
M 2.123 - Auswahl eines Mailproviders

Da der Emailbetrieb über die organisatorischen Regelungen hinaus in der Verantwortung des Rechenzentrums liegt, wird die technische Sicherheit des Mailservers dort betrachtet.

5.1.9 Nutzung von Telefax

Die Nutzung von Telefax ist Sache der Fachbereichseinrichtung selbst, jedoch sollte der Fachbereich auch hier übergeordnete Interessen, z.B. im Rahmen der gemeinsamen Außendarstellung, wahren. Zur Sicherheit bei der Nutzung von Telefax sollten die folgenden Maßnahmen fachbereichsübergreifend umgesetzt werden.
M 3.15 - Informationen für alle Mitarbeiter über die Nutzung eines Fax-Gerätes
M 5.24 - Nutzung eines geeigneten Fax-Vorblattes

5.1.10 IT-Sicherheit sonstiger Kommunikationseinrichtungen

M 5.14 - Absicherung interner Remote-Zugänge
M 5.15 - Absicherung externer Remote-Zugänge
M 5.4 - Dokumentation und Kennzeichnung der Verkabelung

5.1.11 Kommunikation von IT-Sicherheit

Zwischen dem Fachbereich, der zentrale Elemente der IT-Sicherheit bereitstellt, und seinen Einrichtungen, die mit diesen zentralen Elementen „leben“ müssen, sollte ein regelmäßiger Austausch über Notwendigkeit und Vorgehen im Bereich der IT-Sicherheit stattfinden. Ziel ist eine Sensibilisierung und Schulung der Administratoren in den jeweiligen Fachbereichseinrichtungen. Hierzu kommen die folgenden Maßnahmen zur Anwendung:
M 2.26 - Ernennung eines Administrators und eines Vertreters in jeder Fachbereichseinrichtung
M 3.10 - Auswahl eines vertrauenswürdigen Administrators und Vertreters
M 3.11 - Schulung des Wartungs- und Administrationspersonals

Als Ziel einer solchen Diskussion könnten u.a. die beschriebenen Standardarbeitsplätze entstehen, definiert und fortgeschrieben werden (M 2.23 - Herausgabe einer PC-Richtlinie, M 2.24 -

Einführung eines PC-Checkheftes)

Notwendig ist auch die Informationsbeschaffung über Sicherheitslücken des Systems (M 2.35). Diese wird derzeit maßgeblich von der DFN CERT GmbH vorangetrieben. Der Fachbereich profitiert derzeit davon, daß diese Einrichtung am Fachbereich Räume belegt und damit Know-How in der Nähe ist und davon, daß der Fachbereich Mitglied im DFN ist und das DFN als Internetprovider für den Fachbereich fungiert. Beides kann sich ändern, wie z.B. der derzeitigen Diskussion über die Zukunft des DFN zu entnehmen ist. Der Fachbereich muß Vorkehrungen für diesen Fall treffen, um spätestens dann eigenes Know-How vorzuhalten oder aufbauen zu können.

Auch die Mitarbeiter und Studierenden sollten auf die Notwendigkeit und Umsetzung von IT-Sicherheitsmaßnahmen hingewiesen werden. Als Maßnahmen kommen hierzu in Frage:
M 3.1 - Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
M 2.12 - Betreuung und Beratung von IT-Benutzern
M 3.5 - Schulung zu IT-Sicherheitsmaßnahmen, wozu z.B. auch die Schulung im Umgang mit Produkten wie den Verschlüsselungsprogrammen PGP[2], GPG[3] oder PEM[4] gehören könnte
M 3.2 - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
M 3.6 - Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
M 3.18 - Verpflichtung der PC-Benutzer zum Abmelden nach Aufgabenerfüllung
Auf Verletzungen der Sicherheitspolitik müssen entsprechende Reaktionen folgen (M 2.39).

Bei Entscheidungen zur Umsetzung von IT-Sicherheitsmaßnahmen sind die entsprechenden Regelungen zur Beteiligung von Betriebs- und Personalräten zu beachten (siehe M 2.40 - Rechtzeitige Beteiligung des Personal-/Betriebsrates).

5.1.12 Entsorgung von schützenswerten Betriebsmitteln

Der Fachbereich sollte an zentraler Stelle ein Angebot zur Entsorgung schützenswerter Betriebsmittel (siehe Maßnahme M 2.13) anbieten. Hierzu gehört neben der sicheren Löschung und Vernichtung von Datenträgern auch eine sichere Entsorgungsmöglichkeit für Papier.

[2]Pretty Good Privacy
[3]Gnu Privacy Guard
[4]Privacy Enhanced Mail

5.2 Aufgaben der Fachbereichseinrichtungen

Die Fachbereichseinrichtungen haben die Aufgabe, auf Basis der vom Fachbereich durchgeführten Sicherheitsmaßnahmen selbst weitere Anstrengungen zu unternehmen, um ihr Sicherheitsbedürfnis zu befriedigen. Dabei gibt es Maßnahmen, die im Zuge eines allgemeinen Grundschutzes von allen Fachbereichseinrichtungen in ihrem jeweiligen Bereich ergriffen werden müssen. Diese werden zunächst beschrieben.

Neben den allgemeinen Regelungen werden auch Regelungen notwendig sein, die von der jeweiligen Ausstattung der Fachbereichseinrichtung abhängen. Diese werden dann für jede der untersuchten Fachbereichseinrichtungen separat beschrieben.

5.2.1 Allgemeine Maßnahmen in den Fachbereichseinrichtungen

Die in den Fachbereichseinrichtungen jeweils durchzuführenden Maßnahmen betreffen die Organisationssicherheit, ergänzende Vorkehrungen für Notfälle sowie infrastrukturelle Maßnahmen.

Maßnahmen zur Organisationssicherheit

- *Festlegung und Dokumentation von Aufgaben und Verantwortlichkeiten*
  Die Festlegung von Aufgaben und Verantwortlichkeiten dient zunächst der allgemeinen Arbeitsorganisation. Aus Sicht der Fachbereichseinrichtung ist hier jedoch vor allem die Dokumentation wichtig. Sie dient dem Nachweis, welche Verantwortlichkeiten bestehen bzw. bei Eintritt eines Schadensereignisses bestanden haben. Sie dient auch dem Nachweis der Ordnungsmäßigkeit des Betriebes in der Fachbereichseinrichtung.
  M 2.1 - Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
  M 2.5 - Aufgabenverteilung und Funktionstrennung
  M 3.3 - Vertretungsregelungen

- *Regelung und Dokumentation des Einsatzes der IT in der Einrichtung*
  Hier sollen vor allem die Anweisungen, Regelungen und Weisungen dokumentiert werden, die den allgemeinen Einsatz der IT in der betreffenden Fachbereichseinrichtung betreffen. Die Dokumentation dient im Schadensfalle dem Nachweis, daß alle erforderlichen Vorsorgemaßnahmen getroffen wurden. Die folgenden Maßnahmen sind hier anzuwenden:
  M 2.2 - Betriebsmittelverwaltung
  M 2.3 - Datenträgerverwaltung
  M 2.4 - Regelungen für Wartungs- und Reparaturarbeiten
  M 2.13 - Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
  M 2.22 - Hinterlegen des Administratorpaßwortes an einem sicheren Ort
  M 2.62 - Software-Abnahme- und Freigabe-Verfahren
  M 2.34 - Dokumentation der Veränderungen an einem bestehenden System

- *Regelung und Dokumentation der Benutzungsberechtigungen*
  Hierzu gehören neben der Berechtigung zur Benutzung auch die Zugangs-, Zutritts- und

Zugriffsberechtigungen. Die folgenden Maßnahmen beschreiben diese:
M 2.30 sowie M 2.132 - Regelung für die Einrichtung von Benutzern / Benutzergruppen / Datenbankbenutzern
M 2.31 - Dokumentation der zugelassenen Benutzer und Rechte
M 2.11 - Regelung des Paßwortgebrauchs
M 2.9 - Nutzungsverbot nicht freigegebener Software
M 2.7 - Vergabe von Zugangsberechtigungen
M 2.6 sowie M 2.17 - Vergabe von Zutrittsberechtigungen sowie die Zutrittskontrolle
M 2.8 und M 2.63 - Vergabe von Zugriffsrechten

- *Umgang mit Mitarbeitern*
  Um die eingesetzten IT-Systeme sicher bedienen zu können, sollten die beiden folgenden Maßnahmen umgesetzt werden
  M 3.4 - Schulung, insbesondere neuer Mitarbeiter, vor Nutzung der Software
  M 3.7 - Anlaufstelle bei persönlichen Problemen
  M 3.8 - Vermeidung von Störungen des Betriebsklimas
  M 3.9 - Schaffung eines ergonomischen Arbeitsplatzes

Maßnahmen zur Notfallvorsorge

- *Maßnahmen zur allgemeinen Notfallvorsorge*
  Für den Fall des Eintritts eines Notfalles sollten vorher Überlegungen getroffen worden sein, was zu tun ist und wie die Fachbereichseinrichtung weiterarbeiten kann und will. Die folgenden Maßnahmen unterstützen dies:
  M 6.1 - Erstellung einer Übersicht über Verfügbarkeitsanforderungen
  M 6.4 - Dokumentation der Kapazitätsanforderungen der IT-Anwendungen
  M 6.5 - Definition des eingeschränkten IT-Betriebs
  M 6.6 - Untersuchung interner und externer Ausweichmöglichkeiten
  M 6.10 - Notfall-Plan für DFÜ-Ausfall
  M 6.23 - Verhaltensregeln bei Auftreten eines ComputerVirus
  M 6.31 - Verhaltensmaßregeln nach Verlust der Systemintegrität
  M 6.33 - Entwicklung eines Datensicherungskonzepts

- *Datensicherung*
  Die Forschungsergebnisse und -daten sind vor Verlust zu schützen. Dazu gehört eine regelmäßige Datensicherung sowie die Aufbewahrung der Datensicherungsmedien an einem geschützten Ort. Der Fachbereich als übergeordnetes Organ hat die Aufgabe, einen sicheren Aufbewahrungsort für Backup-Datenträger zu finden. Die Fachbereichseinrichtungen sollten dann das Angebot annehmen und ihre Backup-Datenträger dort regelmäßig mit einlagern. Bei Bedenken bezüglich der Vertraulichkeit kann die Sicherungskopie verschüsselt werden.

  Neben der Umsetzung von Maßnahmen zur regelmäßigen Datensicherung ist diese auch zu dokumentieren sowie gelegentlich das Wiedereinspielen von Sicherheitskopien zu üben.

Folgende Maßnahmen beschreiben dieses detailliert:
M 6.25 und 6.32 - Regelmäßige Datensicherung sowie
M 6.50 - Archivierung von Datenbeständen
M 6.13 - Erstellung eines Datensicherungsplans
M 6.34 - Erhebung der Einflußfaktoren der Datensicherung
M 6.35 - Festlegung der Verfahrensweise für die Datensicherung
M 6.37 - Dokumentation der Datensicherung
M 6.41 - Übungen zur Datenrekonstruktion
M 6.22 - Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
M 6.21 - Sicherungskopie der eingesetzten Software

- *Absicherung von Restrisiken*
  Die Maßnahme M 6.16 - Abschließen von Versicherungen - ist nach allgemeinem Verständnis in einer Behörde, zu der die Universitä zählt, nicht möglich. Dennoch scheint es eine Möglichkeit hierfür zu geben: es hat der Hochschullehrerverband wohl ein entsprechendes Angebot ausgehandelt, nach dem Hochschullehrer die Möglichkeit haben, ihr Equipment, das sie im Rahmen von Drittmitteln einsetzen, zu versichern.

Allgemeine infrastrukturelle Maßnahmen zur Gebäudesicherung

- Ergänzung der Brandschutzmaßnahmen, die durch den Fachbereich getroffen wurden, durch eine Raumbelegung unter Berücksichtigung von Brandlasten (M 1.8), u.a. durch Konzentration von IT-Geräten auf wenige zu schützende Bereiche. In Abstimmung mit dem Fachbereich müssen diese Bereiche dann besonders überwacht werden, z.B. durch Brandmelder oder Einbruchmelder.

- Regelung des Zutritts zu Verteilern (M 1.2) sowie die materielle Sicherung von Leitungen und Verteilern (M 1.22).

- Ergänzung der Raumsicherung außerhalb der Betriebszeiten durch Schließen der Fenster und Abschließen der Türen bei Verlassen (M 1.15, M 1.23) sowie die Maßnahmen M 2.14 zur Schlüsselverwaltung.

5.2.2 Individuelle Aufgaben für die Bibliothek

Aufbauend auf den infrastrukturellen und organisatorischen Maßnahmen, die der Fachbereich zu treffen hat, und die jede Fachbereichseinrichtung durchführen muß, fallen der Bibliothek die folgenden weiteren Aufgaben zu, die aus der spezifischen IT-Struktur der Bibliothek resultieren:

Schutz der Informationstechnik am Arbeitsbereich

- *Schutz der Büro - Arbeitsplatzrechner*
  In der Bibliothek kommen derzeit Windows-NT-Workstations mit installiertem Office-Paket (Standard-Software) zum Einsatz. Diese sollten im Rahmen der Standard-PC, wie

im vorigen Abschnitt beschrieben, vom Fachbereich bereitgestellt und betreut werden. Dabei sind sowohl physikalische Maßnahmen, z.B. Diebstahlschutz oder der Verschluß von Diskettenlaufwerken, als auch Maßnahmen zur Sicherung gegen unbefugten Zugriff und ungewollte Veränderungen am System (z.B. durch Viren) vorzunehmen.

Die Maßnahmen betreffen z.B.

- den Paßwortschutz und den Einsatz von Bildschirmsperren bei Abwesenheit
- Physikalische Sicherung der Geräte durch:
  Verschluß der Diskettenlaufwerkschächte sowie die
  Absicherung des Boot-Vorgangs für ein Windows NT System
- Schutz gegen Viren durch regelmäßigen Einsatz eines Viren-Suchprogramms, besonders vor und nach einer Datenübertragung, wobei auch eine Prüfung auf Makro-Viren stattfinden soll.
  Deaktivieren der automatischen CD-ROM Erkennung und -Wiedergabe
- Schutz der Windows NT-Workstations, insbesondere Schutz
  der Registrierung und der Administratorkonten.
  Einrichtung einer eingeschränkten Benutzerumgebung

- *Erstellung eines Datenbanksicherheitskonzeptes für den Einsatz der Datenbanken MS Access und Oracle*
  Für den Schutz der Datenbanken unter MS Access und Oracle sollte ein Datenbanksicherheitskonzept erstellt werden. In [BSI1998] werden dazu die folgenden Maßnahmen zur Installation und Konfiguration einer Datenbank, Zugangs- und Zugriffskontrolle, Gewährleistung der Datensicherheit und -integrität sowie zur Datensicherung und Wiederherstellung einer Datenbank beschrieben.

- *Einbindung der Arbeitsplatzrechner ins Windows-NT-Netzwerk*
  Da die Windows-NT-Workstations in ein Windows-NT-Netzwerk eingebunden sind, sollten Maßnahmen zum Schutz der Daten und auch zum Schutz der Workstations vor Angriffen aus dem Netz getroffen werden. Desweiteren sind bei der Konfiguration des Netzes sowie der Netzdienste auf der Windows-NT-Workstation entsprechende Einstellungen zum Schutz der Workstations vorzunehmen, z.B. zu :

  - Einschränkung der Peer-to-Peer-Funktionalitäten bei Nutzung von WfW, Windows 95 oder Windows NT
  - zur sicheren Konfiguration der TCP/IP-Netzverwaltung unter Windows NT und
  - zur sicheren Konfiguration der TCP/IP-Netzdienste unter Windows NT

  An der Festlegung einer Sicherheitsstrategie (M 2.91) für das Windows NT - Netzwerk sollte die Bibliothek beteiligt sein.

- *Schutz der Daten*
  Zum Schutz vor Datenverlust sollte eine regelmäßige Datensicherung durchgeführt und dokumentiert werden. Die Backup-Datenträger können dann - sofern dies vom Fachbereich umgesetzt wird - an einem zentral vom Fachbereich organisierten Ort sicher eingelagert werden. Für die Backup-Datenträger sollte bis dahin ein sicherer Ort in räumlicher Entfernung zum Arbeitsbereich gefunden werden und ein Backup dort eingelagert werden.

  Vor Weitergabe sind Daten zu verifizieren, ggf. zu verschlüsseln. Manche Datenträger enthalten Altinformationen; diese sind von Restinformationen zu säubern, bevor sie weitergegeben werden. Vor und nach Verwendung sollten beweglich Datenträger gelöscht werden. Maßnahme M 4.64 - Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen - sollte hier beachtet werden.

  Zur Wahrung der Vertraulichkeit sollten Daten beim Transport, insbesondere über das Netzwerk, verschlüsselt werden. Hierzu sollte die Maßnahme M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen - beachtet werden.

- *Schutz der Kommunikation*
  Email
  Bei Kommunikation über Email sollten die folgenden Maßnahmen beachtet werden:
  M 5.32 - Sicherer Einsatz von Kommunikationssoftware
  M 5.57 - Sichere Konfiguration der Mailclients
  M 2.46 - Angepaßtes Schlüsselmanagement bei Verschlüsselung
  M 6.38 - Sicherungskopie der übermittelten Daten

  Telefax
  Für die Konfiguration und Bedienung des Telefax-Gerätes sind zu beachten:
  M 1.37 - Geeignete Aufstellung eines Fax-Gerätes im Büro der Bibliothek
  M 2.48 - Festlegung berechtigter Fax-Bediener
  M 2.47 - Ernennung eines Fax-Verantwortlichen sowie
  M 2.53 - Abschalten des Fax-Gerätes außerhalb der Bürozeiten

IT-Sicherheitsmaßnahmen zum Schutz des Katalog- und Ausleihsystems PICA
Für die Bestandskatalogverwaltung und das Ausleihsystem PICA ergeben sich aus der detaillierten Analyse die folgenden zusätzlichen Maßnahmen:

- Beschaffung eines USV-Gerätes (M 1.28) zum geordneten Herunterfahren der PICA-PCs, sofern eine Notstromversorgung nicht durch den Fachbereich gesichert wird.
- Erhöhung der Hardware-Zuverlässigkeit durch regelmäßige Wartung.
- Bereitstellung von Dokumentation und Handbüchern zur Bedienung und Wartung der PICA-Arbeitsplätze und auch der Benutzer-PCs.

- Zutrittskontrolle zu den Bibliotheksräumen, außerhalb der Bibliotheksöffnungszeiten mit Protokollierungsfunktion. Überwachung des Aufenthaltes von Personen in den Bibliotheksräumen außerhalb der Öffnungszeiten.
- Aufstellung der Bildschirme der PICA-PCs am Bibliothekstresen, so daß keine Einsicht von der Seite erfolgen kann. Möglichkeit zum Dunkelschalten des Bildschirms bzw. Einsatz von Bildschirmschonern mit Paßwortschutz bei Verlassen des Tresens durch die Mitarbeiter.
- Regelmäßiges Backup und Freigabeverfahren für Betriebssystem und Software.
- Reglung von Zugangsberechtigungen zum PICA-System. Identifikation der Benutzer der PICA-Software (Mitarbeiter) und Protokollierung der Zugriffe.
- Anwendung und Pflege von Virenschutzprogrammen sowie Einschränkung der Benutzung der PICA-PCs auf die notwendige Software. Benutzung von Software zur Erkennung von Veränderungen.
- Kontrolle der Bestandskatalogdaten durch regelmäßige Tests.
- Sperre der Diskettenlaufwerke und Versiegelung der PICA-PCs zum Schutz vor Manipulation.
- Verschlüsselung der Benutzerdaten und der PICA-Steuerungsdaten bei der Übertragung. Elektronische Signatur der Benutzerdaten, der Bestandskatalogdaten und der PICA-Steuerungsdaten bei der Übertragung zur Erkennung von Manipulationen an den Nachrichten. Aufbau eines sicheren Verbindungsweges (VPN), z.B. mittels SSH.
- Sensibilisierung und Schulung der Bibliothekarinnen und MitarbeiterInnen.
- Regelmäßige Datensicherung, insbesondere vor Wartungsarbeiten. Bereitstellung von Dokumentationen und Benutzungshandbüchern für die Mitarbeiter.
- Sicherstellung von Reparaturfristen durch einen Wartungsvertrag mit dem Regionalen Rechenzentrum.
- Aufbewahrung einer Systemdokumentation und Wartungsanleitung in der Bibliothek, so daß notfalls auf anderes Wartungspersonal zurückgegriffen werden kann.
- Regelung des PICA-Zugriffs für Aushilfskräfte. Benutzungshandbücher und Dokumentation des PICA-Systems auch für Aushilfskräfte bereithalten.

IT-Sicherheitsmaßnahmen zum Schutz der Recherche-PCs
Für die Bibliotheksrecherche-PCs ergeben sich aus der detaillierten Analyse aufgrund der Möglichkeit zur direkten Interaktion mit dem PICA-System per Telnet oder Netcsape die folgenden zusätzlichen Maßnahmen:

- Verhinderung von unkontrolliertem Import fremder Software, z.B. über Netscape. Selbst bei einer Recherche im Internet darf keine Software (oder Plug-In) installiert werden dürfen. Ggf. Einsatz einer sichereren Browser-Software. Freigabe der Software-Änderungen durch eine autorisierte Stelle.

- Zugangsberechtigungen zur PICA-Software regeln und umsetzen. Zugangsberechtigungen zu Netscape und Telnet-Software regeln. Die PCs unter Windows NT sind so zu sichern, daß Benutzer nur die vorgesehenen Funktionen nutzen können. Da die Benutzer-PCs zum allgemeinen Gebrauch bestimmt sind, wird eine Zugangsberechtigung auf Benutzerebene nicht greifen, da sie der bisherigen Praxis der Bibliotheksbenutzung widerspricht.

- Sperrung der Benutzer-PCs für andere Aktivitäten als die Recherche (Netscape) und Bestellvorgänge (Teraterm). Sperre der Diskettenlaufwerke und Versiegelung der Benutzer-PCs.

5.2.3 Individuelle Aufgaben für den Arbeitsbereich AGN

Der Arbeitsbereich AGN muß zusätzlich zu den allgemeinen nun noch Sicherheitsmaßnahmen zum Schutz der IT-Komponenten ergreifen. Dies sind Maßnahmenbündel zur Absicherung des Netzwerkes im AB AGN und der Arbeitsplatzrechner, der Kommunikationseinrichtungen sowie Maßnahmen für die Virus-Datenbank, die aus der detaillierten Risikoanalyse abgeleitet werden. Die detaillierte Darstellung von Maßnahmen befindet sich im Teil II; an dieser Stelle sollen die Maßnahmen grob umrissen werden.

Schutz der Informationstechnik am Arbeitsbereich

- *Schutz des NT-(Samba-)Server-Netzwerkes*
  Hier sind Maßnahmen zur Administration und Planung notwendig, u.a. eine restriktive Nutzertrennung, regelmäßige Sicherheitskontrollen und die regelmäßige Auswertung von Protokolldaten zur Erkennung von Sicherheitsrelevanten Vorfällen.

  Zur Vorsorge sollten die Daten auf dem Server verschlüsselt und die Hardware vor Beschädigung und Manipulation geschützt werden, u.a. durch die Sicherstellung der Stromzufuhr und den Schutz vor Überspannung. Dies kann und sollte - sofern es realisiert wird - zentral durch den Fachbereich geschehen. Der Raum selbst sollte vor unbefugtem Zutritt geschützt werden, der Zutritt im Nachhinein nachvollziehbar sein. Es könnte hierfür ein separater, zutrittsgesicherter Serverraum oder ein Schutzschrank eingerichtet werden. Manipulation muß mindestens aber erkennbar sein.

- *Firewall*
  Für den Betrieb des Firewallrechners sind nach dem Grundschutzhandbuch die folgenden Maßnahmen zu Planung und Betrieb umzusetzen.

Planung:
M 2.70 - Entwicklung eines Firewall-Konzeptes
M 2.71 - Festlegung einer Sicherheitspolitik für eine Firewall
M 2.72 - Anforderungen an eine Firewall
M 2.73 - Auswahl eines geeigneten Firewall-Typs
M 2.74 - Geeignete Auswahl eines Packet-Filters (bei Beschaffungsbedarf)
M 2.75 - Geeignete Auswahl eines Application-Gateway (bei Beschaffungsbedarf)
M 2.76 - Auswahl und Implementation geeigneter Filterregeln
M 2.77 - Sichere Anordnung weiterer Komponenten

Betrieb:
M 2.78 - Sicherer Betrieb einer Firewall
M 4.22 - Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
M 5.39 - Sicherer Einsatz der Protokolle und Dienste
M 5.19 - Einsatz der Sicherheitsmechanismen von sendmail
M 5.20 - Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
M 5.21 - Sicherer Einsatz von telnet, ftp, tftp und rexec
M 5.59 - Schutz vor DNS-Spoofing
M 4.47 - Protokollierung der Firewall-Aktivitäten
M 2.64 - Kontrolle der Protokolldateien

- *PCs im NT-(Samba-)Server-Netzwerk*
  Die Windows 98 - Rechner sowie die beiden Commodore AMIGA-Rechner sind gegen unbefugten Zugriff sowie Schäden durch fehlerhafte Software und Viren zu sichern. Das betrifft die Administration und Benutzung der Rechner sowie vorsorgliche Maßnahmen wie den Einsatz von Virenscannern, die Erstellung von Notfalldisketten. Die Maßnahmen sind in den Teilen II und III detailliert beschrieben.

- *Schutz der tragbaren PCs*
  Auch für die am Arbeitsbereich eingesetzten Laptops sind Schutzmaßnahmen vorzusehen. Dies betrifft die Aufbewahrung, aber auch Maßnahmen beim Wechsel des Benutzers. Sinnvoll erscheint hier der Einsatz eines Verschlüsselungsprogramms, so daß bei Diebstahl die Daten geschützt sind.

- *SUN - Workstation im Raum C 117*
  Für den Schutz der SUN - Sparc - Workstation im Raum C 117 unter dem Betriebssystem Solaris können lt [BSI1998] z.B. die folgenden Maßnahmen (Schutz einer Unix- Workstation) angewendet werden:
  M 5.17 - Einsatz der Sicherheitsmechanismen von NFS
  M 5.18 - Einsatz der Sicherheitsmechanismen von NIS
  M 4.9 - Sicherer Einsatz von X-Windows

- *VTC-Mailbox:*

Die VTC-Mailbox ist per Modem zu erreichen. Hier sieht das IT-Grundschutzhandbuch Maßnahmen zur geeigneten Aufstellung und Konfiguration des Modems vor. Die Mailbox sollte nicht mit dem Arbeitsbereichsnetz verbunden werden.

- *Schutz der Daten*
  Zum Schutz vor Datenverlust sollte eine regelmäßige Datensicherung durchgeführt und dokumentiert werden. Die Backup-Datenträger können dann - sofern dies vom Fachbereich umgesetzt wird - an einem zentral vom Fachbereich organisierten Ort sicher eingelagert werden. Für die Backup-Datenträger sollte bis dahin ein sicherer Ort in räumlicher Entfernung zum Arbeitsbereich gefunden werden und ein Backup dort eingelagert werden.

  Vor Weitergabe sind Daten zu verifizieren, ggf. zu verschlüsseln. Manche Datenträger enthalten Altinformationen; diese sind von Restinformationen zu säubern, bevor sie weitergegeben werden. Vor und nach Verwendung sollten beweglich Datenträger gelöscht werden.

Schutz der Kommunikation
Zum Schutz des Faxgerätes können Maßnahmen ergriffen werden, die vor unberechtigter Bedienung und Einsichtnahme, aber auch vor Angriffen auf die Verfügbarkeit durch Senden von Endlosfaxen schützen. Wichtige Faxsendungen sollten telefonisch angekündigt werden, damit sie vom Empfänger bei Bedarf persönlich entgegengenommen werden können. Wenn Zielwahltasten programmiert werden können, so sollte gelegentlich die Programmierung überprüft werden, damit nicht alte oder unrichtige Empängerrufnummern darin stehen.

Schutz der Virus-Datenbank
Für das IT-System Virus-Datenbank ist eine detaillierte Risikoanalyse durchgeführt worden; hieraus ergeben sich u.a. die folgenden Maßnahmen, die in der Einzelanalyse in Teil II ausgeführt sind und aus bestehenden Risiken hergeleitet werden.

Die Virusdatenbank ist auf die Verfügbarkeit der AVTC[5]-Raums angewiesen. Dieser sollte mit folgenden Maßnahmen geschützt werden:

- Brandschutz:
  Behinderung der Ausbreitung von Bränden durch Einbau einer feuerfesten Tür und und feuerfester Trennwände zu den Nachbarbüros sowie schwerbrennbare Innenausstattung
  Brandmeldung durch automatische Sensoren

- Schutz gegen Anschläge, z.B. durch Raumplanung: Lage des AVTC-Labors, so daß keine Einsicht (und Vorspionage) von der Straße aus möglich ist

- Einbruchschutz:
  Vorbeugung durch durchbruchhemmende Verglasung (Folie) und Einbau einer Stahltür

[5]Anti-Virus-Test-Center: Projekt am Arbeitsbereich, das die Virus-Datenbank betreut und verwendet

zum AVTC-Raum.
Entdeckung durch Bewegungsmelder und Alarmsensoren am Fenster (Öffnung, Glasbruch) sowie der Tür.
Aufzeichnung eines eventuellen Einbruchs auf Überwachungsvideo

Um die Verfügbarkeit und Integrität des NT-Servers, der Test-PCs und der Netzkomponenten gegen Bedrohungen durch physische Einwirkung zu sichern, werden die folgenden Maßnahmen empfohlen:

- Regelmäßige Kontrolle der Hardware-Umgebungsbedingungen (Klima, Standfestigkeit, Brandlasten, etc.)
- Schutz der Klimaversorgung im Raum des AVTC durch eine automatische Klimaanlage oder alternativ Temperatursensoren mit Alarmfunktion, die bei Überschreitung einer kritischen Temperatur gezielt Rechner abschalten
- Beschaffung manipulationssicherer Geräte und Sicherstellung der Manipulationserkennung (Versiegelung des NT-Servers)
- Regelmäßige Inspektion der Geräte unter Sicherheitsaspekten
- Zutrittskontrolle zu den Räumen des AVTC sowie dem VTC/NTC-Labor durch besondere Schlüssel, besser: Ausweisleser mit Protokollierung.
(Einrichtung eines gesicherten Bereiches.)
- Überwachung des Aufenthalts betriebsfremder Personen durch permanente Begleitung und Registrierung.
- Schutz der Datenverbindung zum Drucker durch Integration des Raums zwischen AVTC und VTC/NTC-Labor in den Arbeitsbereich AGN, um die Kontrolle über die Datenleitungen zu behalten. Besser ist die Verlegung des Druckers, so daß keine Datenverbindung durch fremde Büros geht.

Gegen Fehler im Betriebssystem des NT-Servers und Fehler in Testroutinen und Auswertung aufgrund fehlerhafter Software werden in [ITSHB1992] folgende Maßnahmen empfohlen:

- Verhinderung von unkontrolliertem Import von Software
- Kein Einsatz privater Datenträger
- Software-Freigabe durch autorisierte Stelle; Autorisierte Stelle definieren, z.B. AB-Leitung, Laborleitung, Administrator
- Sicherungsmaßnahmen vor Wartungsarbeiten, u.a. Backup

- Verwendung von Sicherheitszusätzen im Betriebssystem, z.B. Plattenverschlüsselung
  Prüfung des Betriebsmittelverbrauchs auf Abnormitäten
  Prüfung der Datenintegrität durch Prüfsummenvergleich

Gegen Fehler im Betriebssystem des NT-Servers aufgrund unberechtigten Zuganges zum NT-Server werden in [ITSHB1992] Maßnahmen in folgenden Bereichen empfohlen:

- Zugangsberechtigungen zum NT-Server und übers Netz regeln und dokumentieren.
  Paßwortregelung, Zentrale Benutzerverwaltung
- Verhinderung der Einkoppelung der Test-PC-Rechner ins AB-Netz
- Definition von Maßnahmen bei Ausscheiden von Mitarbeitern und AVTC-Teammitgliedern (Zugangsberechtigungen, Schlüssel, etc. einziehen)
- Inbetriebnahme von Rechnern nur mittels Schlüssel, ggf. Protokoll der Inbetriebnahme
- Verhinderung der Einkoppelung der Test-PC-Rechner ins AB-Netz
- Verhinderung von unkontrolliertem Import von Software
- Verwendung von Sicherheitszusätzen im Betriebssystem, z.B. Plattenverschlüsselung
  Prüfung des Betriebsmittelverbrauchs auf Abnormitäten
  Prüfung der Datenintegrität durch Prüfsummenvergleich
- Keine dezentralen Ein-/Ausgabegeräte für bewegliche Datenträger zulassen; kein bewegliches DAT-Laufwerk am Server zulassen.

Zur Schadensminderung bei Angriffen und Einwirkungen auf Daten und Datenträger werden die folgenden Maßnahmen empfohlen:

- Erstellen und Dokumentation eines Datensicherungskonzepts
  Dokumentation von Anweisungen zur Datenwiederherstellung
- Katastrophengeschützte Lagerung der Backup-Datenträger außer Haus
  Auslagern von Duplikaten außer Haus, z.B. in einen Banksafe oder mindestens in einem anderen Haus im Fachbereich.
- Sicherungsmaßnahmen vor Wartungsarbeiten, u.a. Backup
- Schutz der Datenträger-Inhalte durch Verschlüsselung.

Gegen die Bedrohung der Vertraulichkeit der Virus-Datenbank durch unberechtigtes Kopieren werden die folgenden Maßnahmen empfohlen. Diese Bedrohung hat ein großes Schadenspotential, demzufolge sollten die Maßnahmen priorisiert realisiert werden. Der Schutz gegen Einbruch und Maßnahmen zur Zutrittskontrolle wurden bereits beschrieben. Sie müssen hier auch realisiert werden.

- Zutrittsberechtigungen von Peronen zu Räumen regeln und umsetzen; Definition eines gesondert gesicherten Bereiches.
- Zugangsberechtigungen zum NT-Server und übers Netz regeln und dokumentieren. Paßwortregelung, Zentrale Benutzerverwaltung
- Definition von Maßnahmen bei Ausscheiden von Mitarbeitern und AVTC-Teammitgliedern (Zugangsberechtigungen, Schlüssel, etc. einziehen)
- Inbetriebnahme der Rechner nur mittels Schlüssel, ggf. Protokoll der Inbetriebnahme
- Zugriffsberechtigungen zu Programmen und Daten, vor allem der Virus-Datenbank, regeln. Die Regelungen sind zu dokumentieren.
- Schutz der Datenverbindung zum Drucker.
- Ergonomische Gestaltung der Arbeitsumgebung derart, daß die Sicherheitsmaßnahmen auch ergonomisch in den Arbeitsablauf integriert sind, damit sie nicht aus Bequemlichkeit ausgeschaltet werden.
- Schulungsmaßnahmen, u.a. Einweisung der Benutzer, Einarbeitung und fachliche Weiterbildung eines zweiten Administrators, Unterrichtung der Mitarbeiter über die Rechtslage und Ausprägung des Sicherheitsbewußtseins der Mitarbeiter im AVTC
- Zuweisung und Abgrenzung von Rechten und Rollen
- Betriebsvorschriften, z.B. Bedienungsanweisung und Dokumentation, Datensicherungskonzept und Katastrophenvorsorge
- Ergonomische Gestaltung der Arbeitsumgebung
  Benutzungsfreundliche Bedienoberflächen einsetzen
  Berücksichtigung arbeitsmedizinischer Aspekte bei Hardware-Auswahl und -Aufstellung (Bildschirmflimmern etc.)
- Kommunikationstechnische Maßnahmen auf Netz-Ebene
  Kommunikationstechnische Maßnahmen auf Nachrichten- und Verbindungsebene

Gegen die Bedrohung der Verfügbarkeit und Integrität der Virus-Datenbank durch fehlerhafte Software oder Fehlbedienung werden die folgenden Maßnahmen empfohlen:

- Zugriffsberechtigungen zu Programmen und Daten, vor allem der Virus-Datenbank, regeln. Die Regelungen sind zu dokumentieren.

- Schulungsmaßnahmen, u.a. Einweisung der Benutzer, Einarbeitung und fachliche Weiterbildung eines zweiten Administrators, Unterrichtung der Mitarbeiter über die Rechtslage und Ausprägung des Sicherheitsbewußtseins der Mitarbeiter im AVTC

- Verhinderung von unkontrolliertem Import von Software
  Verhinderung der Einkoppelung der Test-PC-Rechner ins AB-Netz
  Kein Einsatz privater Datenträger
  Software-Freigabe durch autorisierte Stelle; Autorisierte Stelle definieren, z.B. AB-Leitung, Laborleitung, Administrator

- Verwendung von Sicherheitszusätzen im Betriebssystem, z.B. Plattenverschlüsselung
  Prüfung des Betriebsmittelverbrauchs auf Abnormitäten
  Prüfung der Datenintegrität durch Prüfsummenvergleich

- Vorschriften zu Handhabung von Datenträgern (Schutz vor unberechtigter Nutzung, Kennzeichnung, Löschen vor Wiederverwendung

Eine wichtige Bedrohung stellt der mögliche Ausfall des Administrators dar. Um bei dessen Ausfall weiterarbeiten zu können, sollte ein zweiter Administrator eingearbeitet werden.

5.2.4 Individuelle Aufgaben für den Arbeitsbereich Softwaretechnik

Auch der Arbeitsbereich Softwaretechnik muß zusätzlich zu den allgemeinen nun noch Sicherheitsmaßnahmen zum Schutz der IT-Komponenten des eigenen Arbeitsbereichs ergreifen. Dies sind Maßnahmenbündel zur Absicherung des Netzwerkes im AB SWT und der Arbeitsplatzrechner sowie der Kommunikationseinrichtungen. Alle diese Maßnahmen werden auf Grundschutzniveau realisiert.
Die Maßnahmen werden hier zusammengefaßt und erläutert; sie sind detailliert in den Teilen II und III beschrieben.

Maßnahmen zum Schutz der Informationstechnik am Arbeitsbereich

- *Arbeitsbereichsspezifische Regelungen*
  Alle Regelungen, die der Arbeitsbereich zu treffen hat und die noch nicht in den bisherigen Schritten beachtet worden sind, sollten in einem Organisationshandbuch zusammengefaßt werden. Beispiele für solche Regelungen sind:
  Die Regelung der Administrationstätigkeiten im Arbeitsbereich, z.B. bei den eingesetzten Datenbanken oder dem Windows NT-Netzwerk, die Definition eines Verfahrens zum Test, zur Abnahme und Freigabe von Software oder Regelungen zur Aufbewahrung dienstlicher

Unterlagen und Datenträger.

Weitere Regelungen ergeben sich aus den Maßnahmen:
M 2.110 - Datenschutzaspekte bei der Protokollierung
M 2.136 - Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung
M 5.6 - Obligatorischer Einsatz eines Netzpaßwortes
M 5.10 - Restriktive Rechtevergabe
M 2.16 - Beaufsichtigung oder Begleitung von Fremdpersonen (optional)
M 2.18 - Kontrollgänge (optional)
M 2.64 - Kontrolle von Protokolldateien
M 4.78 - Sorgfältige Durchführung von Konfigurationsänderungen
M 2.37 - "Der aufgeräumte Arbeitsplatz"

- *Maßnahmen zur Datensicherung*
  M 2.41 - Verpflichtung der Mitarbeiter zur Datensicherung
  M 6.42 - Erstellung von Rettungsdisketten für Windows NT
  M 6.44 - Datensicherung unter Windows NT
  M 6.49 - Datensicherung einer Datenbank
  M 6.24 - Erstellen einer Notfalldiskette
  M 6.27 - Sichern des CMOS-RAM
  M 6.51 - Wiederherstellung einer Datenbank

- *Virenschutz*
  Ein Grundschutz gegen Viren soll durch die folgenden Maßnahmen erreicht werden:
  M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms
  M 4.33 - Einsatz eines Viren-Suchprogramms vor und nach einer Datenübertragung
  M 4.4 - Verschluß der Diskettenlaufwerkschächte

- *Systemübergreifende Schutzmaßmahmen*
  Bevor auf die einzelnen Systeme eingegangen wird, sollen kurz Maßnahmen angesprochen werden, die Systemübergreifend zum Schutz von Rechnern (Servern wie Workstations) realisiert werden sollten. Dies betrifft neben der Verkabelung und Netzverwaltung auch organisatorische Fragestellungen.
  M 5.7 - Netzverwaltung
  M 5.8 - Monatlicher Sicherheitscheck des Netzes
  M 1.28 - Lokale unterbrechungsfreie Stromversorgung (optional)
  M 1.20 - Auswahl geeigneter Kabeltypen unter physikalisch - mechanischer Sicht (bei Verkabelung neuer Netze)
  M 1.29 - Geeignete Aufstellung eines IT-Systems (optional) M 2.63 - Einrichten der Zugriffsrechte
  M 2.65 - Kontrolle der Wirksamkeit der Benutzertrennung am IT-System
  M 5.9 - Protokollierung am Server

Generell wird die Realisierung von Zugangsbeschränkungen für Accounts, Rechner und Daten empfohlen, was i.d.R. durch einen generellen Paßwortschutz umgesetzt wird. Das Administratorpaßwort sollte dabei an einem sicheren Ort hinterlegt werden. Die Systemverwaltung sollte sicherstellen, daß nicht mehr benötigte Accounts schnell gesperrt werden.
M 4.16 - Zugangsbeschränkungen für Accounts und / oder Terminals
M 4.17 - Sperren und Löschen nicht benötigter Accounts und Terminals

- *Windows NT - Netzwerk*
  Um einen Grundschutz für ein Windows-NT-Netzwerkes zu realisieren, wird die Anwendung der im folgenden beschriebenen Maßnahmen vorgeschlagen. Hierbei geht es im Wesentlichen darum, bereits bei der Planung des Netzes eine Sicherheitsstrategie zu verfolgen und diese dann umzusetzen.
  M 2.91 - Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
  M 2.93 - Planung des Windows NT Netzes
  M 2.92 - Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
  M 2.94 - Freigabe von Verzeichnissen unter Windows NT
  M 2.32 - Einrichtung einer eingeschränkten Benutzerumgebung
  M 4.50 - Strukturierte Systemverwaltung unter Windows NT
  M 4.53 - Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
  M 4.51 - Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
  M 5.41 - Sichere Konfiguration des Fernzugriffs unter Windows NT
  M 6.43 - Einsatz redundanter Windows NT Server

- *Unix - Workstations*
  Für Unix-Workstations wird im IT-Grundschutzhandbuch pauschal die Realisierung folgender Maßnahmen vorgeschlagen:
  M 2.33 - Aufteilung der Administrationstätigkeiten unter Unix
  M 4.9 - Einsatz der Sicherheitsmechanismen von X-Windows
  M 4.13 - Sorgfältige Vergabe von IDs
  M 4.14 - Obligatorischer Paßwortschutz unter Unix
  M 4.18 - Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
  M 4.19 - Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
  M 4.21 - Verhinderung des unautorisierten Erlangens von Administratorrechten
  M 4.25 - Einsatz der Protokollierung im Unix-System
  M 4.20 - Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
  M 4.24 - Sicherstellung einer konsistenten Systemverwaltung
  M 4.26 - Regelmäßiger Sicherheitscheck des Unix-Systems
  M 4.22 - Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
  M 4.40 - Verhinderung der unautorisierten Nutzung des Rechnermikrofons
  M 4.23 - Sicherer Aufruf ausführbarer Dateien

M 5.21 - Sicherer Einsatz von telnet, ftp, tftp und rexec
M 5.17 - Einsatz der Sicherheitsmechanismen von NFS
M 5.18 - Einsatz der Sicherheitsmechanismen von NIS
M 5.19 - Einsatz der Sicherheitsmechanismen von sendmail
M 5.20 - Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
M 5.35 - Einsatz von Sicherheitsmechanismen von UUCP

- *Windows NT - Klienten*
  Für die Windows NT - Arbeitsplatzrechner ist das folgende Maßnahmenbündel zu realisieren. Hierbei ist zu unterscheiden zwischen administrativen Maßnahmen (z.B. bei der Installation) und Maßnahmen, die die Benutzer des Systems realisieren müssen. Die administrativen Maßnahmen sind folgende:
  M 4.55 - Sichere Installation von Windows NT
  M 4.57 - Deaktivieren der automatischen CD-ROM Erkennung und -Wiedergabe
  M 4.76 - Sichere Systemversion von Windows NT
  M 4.75 - Schutz der Registrierung unter Windows NT
  M 4.77 - Schutz der Administratorkonten unter Windows NT
  M 4.49 - Absicherung des Boot-Vorgangs für ein Windows NT System
  M 4.54 - Protokollierung unter Windows NT
  M 4.52 - Geräteschutz unter Windows NT
  M 5.42 - Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT
  M 5.43 - Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT
  M 5.37 - Einschränken der Peer-to-Peer-Funktionalitäten bei Nutzung von WfW, Windows 95 oder Windows NT in einem servergestützten Netz
  M 5.58 - Installation von ODBC-Treibern

  Die Benutzer sollten in die Verfahren zum Virenschutz und die Sicherung von Dateien und Email durch Verschlüsselung eingewiesen werden.
  M 4.30 - Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
  M 4.44 - Prüfung eingehender Dateien auf Makro-Viren
  M 5.32 - Sicherer Einsatz von Kommunikationssoftware
  M 5.57 - Sichere Konfiguration der Mailclients
  M 5.36 - Verschlüsselung unter Unix und Windows NT
  M 4.56 - Sicheres Löschen unter Windows NT und Windows 95
  M 4.48 - Paßwortschutz unter Windows NT
  M 4.2 - Bildschirmsperre bei Abwesenheit

- *Macintosh - Rechner unter MacOS 8*
  Der Macintosh-Rechner ist mit ähnlichen Sicherheitsmechanismen auszustatten wie die anderen Rechner im Netzwerk von SWT. Insbesondere darf hierdurch kein unkontrollierbarer Netzzugriff bestehen. Das IT-Grundschutzhandbuch siehr hierfür derzeit noch keinen Baustein vor. In Bezug auf den Netzzugriff ist Maßnahme M 4.41 - Einsatz eines angemessenen PC-Sicherheitsproduktes zur Benutzertrennung - als Minimalforderung zu

erfüllen.
Darüberhinaus sollte, sobald ein entsprechender Baustein des IT-Grundschutzes vorhanden ist, dieser auf die Macintosh-Rechner am Arbeitsbereich SWT angewendet werden. Alternativ kann auch ein eigener Baustein hierfür entwickelt werden.

- *Häuslicher Arbeitsplatz*
  Wenn Mitarbeiter zuhause arbeiten (häuslicher Arbeitsplatz), dann muß dort bezüglich der verarbeiteten Daten und der eingesetzten Informationstechnik vergleichbares Sicherheitsniveau erreicht werden, als würde die Mitarbeiterin im Arbeitsbereich arbeiten. Dabei ist zu beachten, daß im häuslichen Arbeitsplatz i.d.R. keine Gebäude- oder Geländesicherheit durch einen Wachschutz realisiert ist, insofern erhöht sich z.B. das Schadenspotential bei einem Einbruch in die Räumlichkeiten der Mitarbeiterin. Es sind dann Daten wie Equipment gefährdet. Maßnahmen dagegen sind in M 1.44 - Geeignete Einrichtung eines häuslichen Arbeitsplatzes - sowie M 2.112 - Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution - beschrieben. Zusätzlich sollte M 1.7 - Handfeuerlöscher für den häuslichen Arbeitsplatz - realisiert werden.

Maßnahmen zum Schutz der Kommunikationseinrichtungen am Arbeitsbereich
Neben der Bereitstellung der Telekommunikationsanlage, die dem Fachbereich obliegt, und der Zurverfügungstellung des Emailverkehrs, die in einer detaillierten Analyse im Rechenzentrum untersucht wurde, sind Maßnahmen für die einzelnen Kommunikationseinrichtungen zu treffen.

- *Sichere Emailnutzung*
  M 5.57 - Sichere Konfiguration der Mailclients
  M 4.64 - Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
  M 4.35 - Verifizieren der zu übertragenden Daten vor Versand
  M 4.33 - Einsatz eines Viren-Suchprogramms vor und nach einer Datenübertragung
  M 4.34 - Einsatz von Verschlüsselung oder Checksummen
  M 5.32 - Sicherer Einsatz von Kommunikationssoftware
  M 5.55 - Kontrolle von Alias-Dateien und Verteilerlisten
  M 2.46 - Angepaßtes Schlüsselmanagement bei Verschlüsselung
  M 2.121 - Regelmäßiges Löschen von E-mails

- *Telefax*
  M 1.37 - Geeignete Aufstellung eines Fax-Gerätes
  M 2.42 - Festlegung der möglichen Kommunikationspartner
  M 2.47 - Ernennung eines Fax-Verantwortlichen
  M 2.48 - Festlegung berechtigter Fax-Bediener
  M 2.49 - Beschaffung geeigneter Fax-Geräte (bei Beschaffungsbedarf)
  M 2.50 - Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen
  M 2.51 - Fertigung von Kopien eingehender Fax-Sendungen
  M 2.52 - Versorgung und Kontrolle der Fax-Verbrauchsgüter
  M 2.53 - Abschalten des Fax-Gerätes außerhalb der Bürozeiten

M 4.36 - Sperren bestimmter Fax-Empfängerrufnummern
M 4.37 - Sperren bestimmter Fax-Absenderrufnummern
M 5.25 - Nutzung von Sende- und Empfangsprotokollen
M 5.26 - Telefonische Ankündigung einer Fax-Sendung
M 5.27 - Telefonische Rückversicherung über korrekten Fax-Empfang
M 5.28 - Telefonische Rückversicherung über korrekten Fax-Absender
M 5.29 - Gelegentliche Kontrolle programmierter Zieladressen und Protokolle

- *Anrufbeantworter*
  M 2.54 - Beschaffung/Auswahl geeigneter Anrufbeantworter
  M 2.55 - Einsatz eines Sicherungscodes (optional)
  M 2.56 - Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter
  M 2.57 - Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche
  M 2.58 - Begrenzung der Sprechdauer (optional)
  M 3.16 - Einweisung in die Bedienung des Anrufbeantworters
  M 4.38 - Abschalten nicht benötigter Leistungsmerkmale am Anrufbeantworter

Sichere Nutzung von Datenbanken
Für die Nutzung von Datenbanken wird im IT-Grundschutzhandbuch die Realisierung folgender Maßnahmen vorgeschlagen:
M 2.124 - Geeignete Auswahl einer Datenbank-Software
M 2.125 - Installation und Konfiguration einer Datenbank
M 2.126 - Erstellung eines Datenbanksicherheitskonzeptes
M 2.128 - Zugangskontrolle einer Datenbank
M 2.129 - Zugriffskontrolle einer Datenbank
M 2.130 - Gewährleistung der Datenintegrität
M 2.127 - Inferenzprävention
M 2.133 - Kontrolle der Protokolldateien eines Datenbanksystems
M 2.134 - Richtlinien für Datenbank-Anfragen
M 2.135 - Gesicherte Datenübernahme in eine Datenbank
M 4.68 - Sicherstellung einer konsistenten Datenbankverwaltung
M 4.69 - Regelmäßiger Sicherheitscheck der Datenbank
M 4.71 - Restriktive Handhabung von Datenbank-Links
M 4.72 - Datenbank-Verschlüsselung (optional)
M 4.73 - Festlegung von Obergrenzen für selektierbare Datensätze
M 4.67 - Sperren und Löschen nicht benötigter Datenbank-Accounts
M 4.70 - Durchführung einer Datenbanküberwachung
M 6.48 - Verhaltensregeln nach Verlust der Datenbankintegrität

5.2.5 Individuelle Aufgaben für die FB-Verwaltung

Zu beachten ist, daß hier nur die Systeme untersucht wurden und abgesichert werden können, die zum Wissenschaftsservice der Verwaltung zählen. Die Systeme MBV, Stellenverwaltung und

Prüfungsverwaltung müssen im Rahmen einer detaillierten Risikoanalyse gesichert werden. Es werden Grundschutzmaßnahmen aus den folgenden Bereichen zur Realisierung vorgeschlagen, detailliert sind diese in den Teilen II und III beschrieben. Viele der Maßnahmen sind auch - da sie pauschale Maßnahmen sind - bereits in der einen oder anderen Fachbereichseinrichtung erläutert. Sie werden dann hier nur kurz erwähnt.

Verwaltungsspezifische Maßnahmen zur Organisationssicherheit
M 2.37 - "Der aufgeräumte Arbeitsplatz"
M 2.38 - Aufteilung der Administrationstätigkeiten
M 2.39 - Reaktion auf Verletzungen der Sicherheitspolitik
M 2.41 - Verpflichtung der Mitarbeiter zur Datensicherung
M 2.110 - Datenschutzaspekte bei der Protokollierung
M 5.10 - Restriktive Rechtevergabe

Datensicherung, Notfallvorsorge
Als Grundschutz gegen Datenverlust und als Notfallvorsorge werden die folgenden Maßnahmen empfohlen:
M 6.24 - Erstellen einer Notfalldiskette
M 6.42 - Erstellung von Rettungsdisketten für Windows NT
M 6.44 - Datensicherung unter Windows NT
M 6.27 - Sichern des CMOS-RAM
M 6.49 - Datensicherung einer Datenbank
M 6.51 - Wiederherstellung einer Datenbank

Maßnahmen zum Schutz der Informationstechnik am Arbeitsbereich

- *Virenschutz*
  Ein Grundschutz gegen Viren soll durch die folgenden Maßnahmen erreicht werden:
  M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms
  M 4.33 - Einsatz eines Viren-Suchprogramms vor und nach einer Datenübertragung
  M 4.4 - Verschluß der Diskettenlaufwerkschächte

- *Windows NT - Server*
  Da die Fachbereichsverwaltung derzeit den Windows NT-Server des Fachbereichs-Rechenzentrums mitnutzt, sind die dort beschriebenen Sicherheitsmaßnahmen umzusetzen. Die Fachbereichsverwaltung sollte an der Planung des Windows NT-Netzes beteiligt werden.

- *Windows NT - Workstations*
  Der Schutz der Windows NT - Arbeitsplatzrechner erfolgt analog zu den Rechnern in der Bibliothek und im Arbeitsbereich SWT; da dort dieselben pauschalen Maßnahmeempfehlungen gegeben werden, wird auf die vorangegangenen Abschnitte verwiesen.

- *Macintosh - MacOS 8 - Rechner*
  Der Schutz der Macintosh - Rechner unter dem Betriebssystem Macintosh MacOS 8 erfolgt

zunächst analog zu den Rechnern im Arbeitsbereich SWT. Zusätzlich sind Maßnahmen zu ergreifen, die bei Einsatz des Programms „Softwindows“, einem Windows 95 - Simulationsprogramm, das Netzwerk und die anderen Rechner vor möglichen Sicherheitslücken in dieser Simulation schützen.

- *Solaris-Workstation*
  Für den Einsatz einer Workstation unter dem Betriebssystem Solaris gelten dieselben Grundschutzanforderungen wie im Fachbereich SWT, demzufolge sind dieselben Maßnahmen wir dort beschrieben zu realisieren.

Aufstellung und Bedienung von Schutzschränken in den Büroräumen
Hier soll Grundschutz mit folgenden Maßnahmen realisiert werden:
M 1.40 - Geeignete Aufstellung von Schutzschränken
M 2.95 - Beschaffung geeigneter Schutzschränke
M 2.96 - Verschluß von Schutzschränken
M 3.20 - Einweisung in die Bedienung von Schutzschränken

Druckerraum
M 1.32 - Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern
M 1.29 - Geeignete Aufstellung eines IT-Systems

Schutz der Kommunikation
Der Schutz der Kommunikation bezieht sich auf den Schutz des Email- und des Faxeinsatzes in der FB-Verwaltung und kann analog zur Bibliothek realisiert werden:

- *Email*
  Bei Kommunikation über Email sollten die folgenden Maßnahmen beachtet werden:
  M 5.32 - Sicherer Einsatz von Kommunikationssoftware
  M 5.57 - Sichere Konfiguration der Mailclients
  M 2.46 - Angepaßtes Schlüsselmanagement bei Verschlüsselung
  M 6.38 - Sicherungskopie der übermittelten Daten
  M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

- *Telefax*
  Für die Konfiguration und Bedienung des Telefax-Gerätes sind zu beachten:
  M 1.37 - Geeignete Aufstellung eines Fax-Gerätes im Büro der Bibliothek
  M 2.48 - Festlegung berechtigter Fax-Bediener
  M 2.47 - Ernennung eines Fax-Verantwortlichen sowie
  M 2.53 - Abschalten des Fax-Gerätes außerhalb der Bürozeiten

  Der Schutz der Telekommunikationsanlage ist ebenfalls bereits betrachtet worden.

Einsatz von Datenbanken
Für den Schutz von Datenbanken wie z.B. MS Access werden die folgenden Maßnahmen zur Realisierung empfohlen:
M 2.124 - Geeignete Auswahl einer Datenbank-Software
M 2.125 - Installation und Konfiguration einer Datenbank
M 2.126 - Erstellung eines Datenbanksicherheitskonzeptes
M 2.128 - Zugangskontrolle einer Datenbank
M 2.129 - Zugriffskontrolle einer Datenbank
M 2.130 - Gewährleistung der Datenintegrität
M 2.131 - Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
M 2.127 - Inferenzprävention
M 2.133 - Kontrolle der Protokolldateien eines Datenbanksystems
M 2.134 - Richtlinien für Datenbank-Anfragen
M 2.135 - Gesicherte Datenübernahme in eine Datenbank
M 4.68 - Sicherstellung einer konsistenten Datenbankverwaltung
M 4.69 - Regelmäßiger Sicherheitscheck der Datenbank
M 4.71 - Restriktive Handhabung von Datenbank-Links
M 4.72 - Datenbank-Verschlüsselung (optional)
M 4.73 - Festlegung von Obergrenzen für selektierbare Datensätze
M 4.67 - Sperren und Löschen nicht benötigter Datenbank-Accounts
M 4.70 - Durchführung einer Datenbanküberwachung
M 6.48 - Verhaltensmaßregeln nach Verlust der Datenbankintegrität

5.2.6 Individuelle Aufgaben für das FB-Rechenzentrum

Maßnahmen zur Organisationssicherheit
M 2.42 - Festlegung der möglichen Kommunikationspartner
M 2.109 - Rechtevergabe für den Fernzugriff
M 2.37 - „Der aufgeräumte Arbeitsplatz“
M 2.38 - Aufteilung der Administrationstätigkeiten
M 2.41 - Verpflichtung der Mitarbeiter zur Datensicherung
M 2.62 - Software-Abnahme- und Freigabe-Verfahren
M 4.78 - Sorgfältige Durchführung von Konfigurationsänderungen
M 2.110 - Datenschutzaspekte bei der Protokollierung
M 2.16 - Regelung zur Beaufsichtigung von Fremdpersonen
M 2.21 - Rauchverbot
M 2.90 - Regelung zur Überprüfung der Lieferung bei Warenannahme
M 2.111 - Bereithalten von Handbüchern

Datensicherung, Notfallvorsorge
Das Rechenzentrum sollte über die bereits beschriebenen Maßnahmen hinaus regelmäßige Datensicherung für die Unix-Server und die vom Rechenzentrum verwalteten Windows NT-Server betreiben. Die Datensicherungsmedien sind dann an einem sicheren Ort - möglichst außerhalb des Rechenzentrums - zu lagern. Es werden die folgenden Maßnahmen empfohlen:
M 6.42 - Erstellung von Rettungsdisketten für Windows NT
M 6.44 - Datensicherung unter Windows NT
M 6.49 - Datensicherung einer Datenbank
M 6.48 - Verhaltensmaßregeln nach Verlust der Datenbankintegrität
M 6.24 - Erstellen einer Notfalldiskette
M 6.27 - Sichern des CMOS-RAM (bei PCs)
M 6.51 - Wiederherstellung einer Datenbank

Räume
Da im Rechenzentrum Equipment mit hohem materiellen Wert und auch grundlegende Infrastruktur des Fachbereiches zusammenkommen, sollte die Maßnahme M 1.12 - Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile - beachtet werden. Darüberhinaus sollten für Rechnerräume und Administrator/ Serverräume weitere Maßnahmen beachtet werden:

- *Rechnerräume*
  M 1.24 - Vermeidung von wasserführenden Leitungen
  M 1.27 - Klimatisierung

- *Administrations- und Serverräume*
  Neben dem Schutz der IT sind für die vorhandenen Schutzschränke die folgenden Maßnahmen zu beachten.
  M 2.95 - Beschaffung geeigneter Schutzschränke
  M 1.40 - Geeignete Aufstellung von Schutzschränken

M 2.96 - Verschluß von Schutzschränken
M 3.20 - Einweisung in die Bedienung von Schutzschränken
M 1.14 - Selbsttätige Entwässerung in den Kellerräumen

Schutz der IT-Systeme

- *Rechnerbetrieb*
  Für den Rechnerbetrieb im Lehre- und Projektcluster sind im Rahmen des Grundschutzes eine Reihe von Maßnahmen zu beachten:
  M 1.29 - Geeignete Aufstellung eines IT-Systems
  M 1.32 - Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern
  M 1.31 - Fernanzeige von Störungen
  M 1.41 - Schutz gegen elektromagnetische Einstrahlung (optional)
  M 2.63 - Einrichten der Zugriffsrechte
  M 2.65 - Kontrolle der Wirksamkeit der Benutzertrennung am IT-System
  M 2.32 - Einrichtung einer eingeschränkten Benutzerumgebung
  M 4.1 - Paßwortschutz für IT-Systeme, PCs und Server
  M 4.2 - Bildschirmsperre bei Abwesenheit
  M 4.7 - Änderung voreingestellter Paßwörter, auch in TK-Anlagen
  M 4.3 - Regelmäßiger Einsatz eines Viren-Suchprogramms
  M 4.4 - Verschluß der Diskettenlaufwerkschächte
  M 4.15 - Gesichertes Login
  M 4.16 - Zugangsbeschränkungen für Accounts und / oder Terminals
  M 4.17 - Sperren und Löschen nicht benötigter Accounts und Terminals
  M 4.30 - Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
  M 4.40 - Verhinderung der unautorisierten Nutzung des Rechnermikrofons
  M 4.44 - Prüfung eingehender Dateien auf Makro-Viren
  M 5.6 - Obligatorischer Einsatz eines Netzpaßwortes
  M 5.7 - Netzverwaltung
  M 5.8 - Monatlicher Sicherheitscheck des Netzes
  M 5.10 - Restriktive Rechtevergabe
  M 5.34 - Einsatz von Einmalpaßwörtern
  M 5.45 - Sicherheit von WWW-Browsern (bei Clients)
  M 5.9 - Protokollierung am Server
  M 5.16 - Übersicht über Netzdienste

- *Schutz der Unix-Server*
  Zum Schutz der Unix-Server werden im IT-Grundschutzhandbuch die folgenden Maßnahmen zur Realisierung vorgeschlagen:
  M 2.33 - Aufteilung der Administrationstätigkeiten unter Unix
  M 4.9 - Einsatz der Sicherheitsmechanismen von X-Windows
  M 4.13 - Sorgfältige Vergabe von IDs

M 4.14 - Obligatorischer Paßwortschutz unter Unix
M 4.18 - Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
M 4.19 - Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
M 4.21 - Verhinderung des unautorisierten Erlangens von Administratorrechten
M 4.24 - Sicherstellung einer konsistenten Systemverwaltung
M 4.25 - Einsatz der Protokollierung im Unix-System
M 4.20 - Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
M 4.26 - Regelmäßiger Sicherheitscheck des Unix-Systems
M 4.22 - Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
M 4.23 - Sicherer Aufruf ausführbarer Dateien
M 5.17 - Einsatz der Sicherheitsmechanismen von NFS
M 5.18 - Einsatz der Sicherheitsmechanismen von NIS
M 5.19 - Einsatz der Sicherheitsmechanismen von sendmail
M 5.20 - Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
M 5.21 - Sicherer Einsatz von telnet, ftp, tftp und rexec
M 5.35 - Einsatz der Sicherheitsmechanismen von UUCP
M 5.39 - Sicherer Einsatz der Protokolle und Dienste
M 5.47 - Einrichten einer Closed User Group
M 5.36 - Verschlüsselung unter Unix

- *Schutz der Windows NT-Server im Rechenzentrum*
  Analog zum Schutz der Unix-Server sind auch die Windows NT-Server zu sichern. Die Windows NT-Server im Rechenzentrum haben besondere Bedeutung, da einige Fachbereichseinrichtungen wie die Bibliothek oder die Fachbereichsverwaltung mangels eigener Server auf die Windows NT-Server des Rechenzentrums zugreifen. Als Grundschutz sind die folgenden Maßnahmen umzusetzen:
  M 2.91 - Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
  M 2.93 - Planung des Windows NT Netzes
  M 2.92 - Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
  M 2.94 - Freigabe von Verzeichnissen unter Windows NT
  M 4.48 - Paßwortschutz unter Windows NT
  M 4.49 - Absicherung des Boot-Vorgangs für ein Windows NT System
  M 4.75 - Schutz der Registrierung unter Windows NT
  M 4.77 - Schutz der Administratorkonten unter Windows NT
  M 4.50 - Strukturierte Systemverwaltung unter Windows NT
  M 4.52 - Geräteschutz unter Windows NT
  M 4.53 - Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
  M 4.54 - Protokollierung unter Windows NT
  M 4.55 - Sichere Installation von Windows NT
  M 4.57 - Deaktivieren der automatischen CD-ROM-Erkennung

M 4.51 - Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
M 4.56 - Sicheres Löschen unter Windows NT und Windows 95
M 4.76 - Sichere Systemversion von Windows NT
M 5.58 - Installation von ODBC-Treibern

- *Schutz der Firewall*
  Der Firewallrechner des Fachbereichs-Rechenzentrums geht als Sicherheitsmerkmal in die detaillierte Risikoanalyse des Netzbetriebes ein. Dort wird das Firewallsystem jedoch, da es aufgrund der derzeitgen Konfiguration kein untragbares Risiko für das Rechenzentrum birgt, nicht weiter untersucht. Eine Firewallkonfiguration, die den Grundschutzanforderungen genügt, kann mit folgenden Maßnahmen erreicht werden:
  M 1.28 - Lokale unterbrechungsfreie Stromversorgung (optional)
  M 1.32 - Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern
  M 1.31 - Fernanzeige von Störungen (optional)
  M 1.41 - Schutz gegen elektromagnetische Einstrahlung (optional)
  M 2.70 - Entwicklung eines Firewall-Konzeptes
  M 2.71 - Festlegung einer Sicherheitspolitik für eine Firewall
  M 2.72 - Anforderungen an eine Firewall
  M 2.73 - Auswahl eines geeigneten Firewall-Typs
  M 2.74 - Geeignete Auswahl eines Packet-Filters (bei Beschaffungsbedarf)
  M 2.75 - Geeignete Auswahl eines Application-Gateway (bei Beschaffungsbedarf)
  M 2.76 - Auswahl und Implementation geeigneter Filterregeln
  M 2.77 - Sichere Anordnung weiterer Komponenten
  M 2.78 - Sicherer Betrieb einer Firewall
  M 4.44 - Prüfung eingehender Dateien auf Makro-Viren
  M 5.9 - Protokollierung am Server
  M 2.64 - Kontrolle von Protokolldateien
  M 5.16 - Übersicht über Netzdienste
  M 5.59 - Schutz vor DNS-Spoofing
  M 4.47 - Protokollierung der Firewall-Aktivitäten

- *Modem/ISDN-Modem*
  Da im Rechenzentrum Modem - und ISDN-Zugänge zu administrativen Zwecken vorgehalten werden, sind folgende Grundschutzmaßnahmen zur Absicherung umzusetzen. Ein Sicherheitsloch an dieser Stelle würde u.U. eine Umgehung der Firewall ermöglichen.

  Modemeinsatz:
  M 2.61 - Regelung des Modem-Einsatzes
  M 1.38 - Geeignete Aufstellung eines Modems
  M 2.59 - Auswahl eines geeigneten Modems in der Beschaffung
  M 2.60 - Sichere Administration eines Modems
  M 3.17 - Einweisung des Personals in die Modem-Benutzung

M 5.30 - Aktivierung einer vorhandenen Callback-Option
M 5.31 - Geeignete Modem-Konfiguration
M 5.32 - Sicherer Einsatz von Kommunikationssoftware
M 5.33 - Absicherung der per Modem durchgeführten Fernwartung
M 5.48 - Authentisierung mittels CLIP/COLP
M 5.49 - Callback basierend auf CLIP/COLP
M 5.50 - Authentisierung mittels PAP/CHAP
M 5.44 - Einseitiger Verbindungsaufbau

Grundschutz für ein ISDN-Modem:
M 1.43 - Geeignete Aufstellung von ISDN-Routern
M 2.106 - Auswahl geeigneter ISDN-Karten in der Beschaffung
M 2.107 - Dokumentation der ISDN-Karten-Konfiguration
M 2.108 - Verzicht auf Fernwartung der ISDN-Netzkoppelelemente (optional)
M 4.59 - Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
M 4.60 - Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
M 4.61 - Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
M 4.62 - Einsatz eines D-Kanal-Filters beim ISDN-Modem

- *Tragbare PCs*
  Zur Ausleihe an Lehrveranstalter werden tragbare PCs bereitgehalten. Zum Schutz der Laptops wird die Anwendung folgender Maßnahmen vorgeschlagen:
  M 1.33 - Geeignete Aufbewahrung tragbarer PCs bei mobilem Einsatz
  M 1.34 - Geeignete Aufbewahrung tragbarer PCs im stationären Einsatz
  M 1.35 - Sammelaufbewahrung mehrerer tragbarer PCs
  M 2.36 - Geregelte Übergabe und Rücknahme eines tragbaren PC
  M 4.27 - Paßwortschutz am tragbaren PC
  M 4.29 - Einsatz eines Verschlüsselungsproduktes für tragbare PCs (optional)
  M 4.31 - Sicherstellung der Energieversorgung im mobilen Einsatz
  M 4.28 - Software-Reinstallation bei Benutzerwechsel eines tragbaren PC (optional)

Kommunikation

- *Email*
  Email sollte durch eine Verschlüsselung geschützt werden. Desweiteren sollte ein Virenschutz betrieben werden.
  M 4.34 - Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen (optional)
  M 2.46 - Angepaßtes Schlüsselmanagement bei Verschlüsselung (optional)
  M 4.33 - Einsatz eines Viren-Suchprogramms vor und nach einer Datenübertragung

- *Fax*
  Für den Schutz des Faxgerätes des Rechenzentrums werden die in den anderen Einrich-

tungen beschriebenen Maßnahmen vorgeschlagen:
M 1.37 - Geeignete Aufstellung eines Fax-Gerätes
M 2.47 - Ernennung eines Fax-Verantwortlichen
M 2.48 - Festlegung berechtigter Fax-Bediener
M 2.49 - Beschaffung geeigneter Fax-Geräte (bei Beschaffungsbedarf)
M 2.50 - Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen
M 2.51 - Fertigung von Kopien eingehender Fax-Sendungen (optional)
M 2.52 - Versorgung und Kontrolle der Fax-Verbrauchsgüter
M 2.53 - Abschalten des Fax-Gerätes außerhalb der Bürozeiten
M 4.36 - Sperren bestimmter Fax-Empfängerrufnummern
M 4.37 - Sperren bestimmter Fax-Absenderrufnummern
M 5.25 - Nutzung von Sende- und Empfangsprotokollen
M 5.26 - Telefonische Ankündigung einer Fax-Sendung
M 5.27 - Telefonischer Rückversicherung über korrekten Fax-Empfang
M 5.28 - Telefonische Rückversicherung über korrekten Fax-Absender
M 5.29 - Gelegentliche Kontrolle programmierter Zieladressen und Protokolle

Datenbanken
Für die im Rechenzentrum installierten Datenbanken sind folgende Maßnahmen zu beachten:
M 2.124 - Geeignete Auswahl einer Datenbank-Software
M 2.125 - Installation und Konfiguration einer Datenbank
M 2.126 - Erstellung eines Datenbanksicherheitskonzeptes
M 2.128 - Zugangskontrolle einer Datenbank
M 2.129 - Zugriffskontrolle einer Datenbank
M 2.130 - Gewährleistung der Datenintegrität
M 2.131 - Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
M 2.132 - Regelung zur Einrichtung von Datenbankbenutzern/-benutzergruppen
M 2.127 - Inferenzprävention
M 2.133 - Kontrolle der Protokolldateien eines Datenbanksystems
M 2.134 - Richtlinien für Datenbank-Anfragen
M 2.138 - Strukturierte Datenhaltung
M 2.135 - Gesicherte Datenübernahme in eine Datenbank M 4.69 - Regelmäßiger Sicherheitscheck der Datenbank
M 4.71 - Restriktive Handhabung von Datenbank-Links
M 4.72 - Datenbank-Verschlüsselung (optional)
M 4.73 - Festlegung von Obergrenzen für selektierbare Datensätze
M 4.67 - Sperren und Löschen nicht benötigter Datenbank-Accounts
M 4.70 - Durchführung einer Datenbanküberwachung
M 4.68 - Sicherstellung einer konsistenten Datenbankverwaltung

Emailverkehr und Netzbetrieb
Der Emailverkehr und der Netzbetrieb sind im Rahmen einer detaillierten Risikoanalyse un-

tersucht worden[6]. Daraus ergibt sich die Notwendigkeit der folgenden zusätzlichen Maßnahmen:

Gegen die Bedrohung der Verfügbarkeit des Außen-Netzes durch Blitzeinschlag wird die folgende Maßnahme empfohlen:

- Trennen des Außennetzes in galvanisch isolierte Teilnetze.
  Bereits jetzt werden u.a. deswegen Glasfaserkabel im Außennetz verwendet.

Gegen die Bedrohung der Verfügbarkeit und Integrität der Stromversorgung durch Blitzeinschlag werden als Maßnahmen empfohlen:

- Schutz des Gebäudes durch Blitzableiter und Potentialausgleich
- Schutz der IT-Geräte gegen induzierte Überspannungen durch Trennen der Geräte vom Stromnetz oder Überspannungsschutzsteckdosen
- Mehrstufiges Blitzschutzkonzept
  Es gibt derzeit Schutzsteckdosenleisten, jedoch kein integriertes Blitzschutzkonzept.

Gegen die Bedrohung der Verfügbarkeit und Integrität der Router, des ATM-Switches, der Netzwerkkabel und -dosen sowie des Firewallrechners durch spontane Fehler oder Ausfall werden als Maßnahmen empfohlen:

- Blitzschutz der IT-Geräte gegen induzierte Überspannungen durch ein mehrstufiges Blitzschutzkonzept
- Schutz der Stromversorgung gegen Spannungsschwankungen und Spannungsabfall durch Verwendung von Notstromaggregaten. Router und Switches werden derzeit mit USVs gesichert.
- Schutz der Firewallbastion durch Raumklimatisierung.
- Sicherstellung der Funktionsfähigkeit der Schutzeinrichtungen (USVs, Überspannungsschutz, Klimaanlage, Alarmsensoren) durch regelmäßige Überprüfung bzw. Wartung.
- Erhöhung der Zuverlässigkeit durch regelmäßige Inspektion und vorbeugende Wartung (vorbeugender Austausch anfälliger Komponenten), auch unter Sicherheitsaspekten (Auswertung von Protokollen).
- Kontrolle der Umgebungsbedingungen (Klima, Störungen, etc.) der Hardwarekomponenten, wasserfeste Verlegung der Datenleitungen in den Gebäuden.
- Manipulationssichere Aufstellung der Netzgeräte (abschließbar, Verwendung von Schutzschränken) und des Firewallrechners.
- Maßnahmen zum Schutz vor Störungen von außen (Lichtwellenleiter-Verbindungen, Einrichten Faradayscher Käfige um die wichtigsten Netzkomponenten).

[6] siehe Teil II

Für die Konfiguration des Mailservers sollten die folgenden Grundschutzmaßnahmen mit beachtet werden.
M 5.56 - Sicherer Betrieb eines Mailservers
M 5.53 - Schutz vor Mailbomben
M 5.54 - Schutz vor Mailüberlastung und Spam

Kapitel 6

Zusammenfassung und Ausblick

Es wurde im Rahmen der Diplomarbeit die aus der Literatur hergeleitete Vorgehensweise zur Erstellung eines IT-Sicherheitskonzeptes am Beispiel des Fachbereiches Informatik der Universität Hamburg untersucht. Dabei ist folgendermaßen vorgegangen worden:

Zunächst wurden Einrichtungen des Fachbereichs zur Untersuchung ausgewählt, dabei wurde Wert darauf gelegt, ein möglichst breites Spektrum der unterschiedlichen Einrichtungen zu erfassen. Es wurden neben übergreifenden Einrichtungen wie der Fachbereichsverwaltung, dem Fachbereichs-Rechenzentrum und der Fachbereichs-Bibliothek auch die Arbeitsbereiche AGN sowie SWT untersucht. Zusätzlich wurden als Drittmittelprojekte die Projekte DFN Firewallabor und DFN PCA und auch eine Fachbereichsexterne Einrichtung, die DFN CERT GmbH, untersucht, die eine Sonderrolle einnimmt, da sie zum einen aus juristischer Sicht eine externe Einrichtung ist, andererseits ihre Räumlichkeiten im Fachbereich selbst hat und auch personelle Überschneidungen existieren.

6.1 Ergebnisse der Voruntersuchung

Die Einrichtungen wurden befragt, um einen Eindruck von den möglichen Schadenspotentialen sowie von Schwachstellen oder bereits realisierten Schutzmaßnahmen zu bekommen. Die Befragung richtete sich zum einen nach den Vorschlägen des IT-Grundschutzhandbuches1998 des BSI [BSI1998] für eine solche Befragung, zum anderen wurden Schwachstellen und bisherige Maßnahmen durch Anwendung eines Fragenkataloges aus den Grundsätzen für eine ordnungsmäßige Datenverarbeitung erkundet.

Alle identifizierten IT-Systeme in den Einrichtungen wurden nach ihrem Schadenspotential hinsichtlich der drei IT-Sicherheitsmerkmale *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* bewertet und in insgesamt vier Schadenskategorien eingeteilt. Der Vorgehensweise des IT-Grundschutzhandbuches zufolge sind für die in die unteren zwei Schadenskategorien eingeteilten IT-Systeme pauschale Maßnahmen zur Erreichung eines mittleren (Grund-)Schutzniveaus zu realisieren. Die in die oberen zwei Schadenskategorien eingeteilten IT-Systeme sind dann mit einer detaillierten Risikoanalyse zu untersuchen. Diese Vorgehensweise wurde am Bei-

spiel der Fachbereichseinrichtungen nachvollzogen. Für eine detaillierte Risikoanalyse wurde dann ein Verfahren ausgewählt, das detailliert alle bedrohten Teilsysteme des zu untersuchenden IT-Systems nach möglichen Schäden und nach den Eintrittshäufigkeiten der jeweiligen Schäden klassifiziert. Hierzu wurde die Vorgehensweise des IT-Sicherheitshandbuches des BSI [ITSHB1992] angewendet.

Als Ergebnis der Voranalyse wurde festgestellt, daß für alle IT-Systeme der Fachbereichseinrichtungen ein genereller Grundschutz realisiert werden müßte, während die höher schutzbedürftigen IT-Systeme zumeist IT-Teilsysteme in den Fachbereichseinrichtungen sind, für die dann zusätzliche IT-Sicherheitsmaßnahmen realisiert werden müßten.

6.2 Ergebnisse der Grundschutzanalysen

Im Rahmen der Grundschutzanalyse wurden die IT-Systeme nach dem Baukastenprinzip des Grundschutzhandbuches analysiert. Analysiert werden hierbei nicht die Gefährdungen, die den Objekten drohen, sondern es wird nur die Existenz bestimmter IT-relevanter Elemente (z.B. „Existiert ein Rechnernetz ?“, „Gibt es Windows 95-Clients ?“, „Gibt es ein Faxgerät ?“, usw.) analysiert.

Als Schwierigkeit ergab sich hier, daß die Struktur eines Lehre- und Forschungsbetriebes aus den bisherigen Grundschutzbausteinen nicht deutlich wird. Objekte wie Rechner-Pool-Räume oder Rechner-Labore sind derzeit nur ungenau erfaßt und können daher nur mit einem Zurechtbiegen anderer Bausteine (Rechner-Labor = Server-Raum ?) realisiert werden. Hier ist es jedoch möglich bzw. sinnvoll, eigene Bausteine für einen Universitätsbetrieb zu entwickeln.

Die Maßnahmen, die aus der Grundschutzanalyse für die untersuchten Fachbereichseinrichtungen folgen würden, werden nach der Analyse in pauschalen Maßnahmenbündeln ausgewählt – je nachdem, welcher Grundschutzbaustein zur Anwendung ausgewählt wurde. So gibt es Maßnahmen zur Grundsicherung von Faxgeräten, Räumlichkeiten oder z.B. zur Infrastrukturellen Sicherheit. Wesentliches Merkmal ist, daß nicht untersucht wird, wie real die angenommene Gefährdung wirklich ist, gegen die Maßnahmen ergriffen werden sollen. Das Grundschutzverfahren dient in erster Linie zur Aufwandsminimierung; die Kräfte sollen für die Untersuchung der wirklich hochschutzbedürftigen IT-Systeme gespart werden.

6.3 Ergebnisse der detaillierten Risikoanalysen

Die detaillierte Risikoanalyse wurde auf Basis der Vorgehensweise des IT-Sicherheitshandbuches des BSI [ITSHB1992] durchgeführt. Dies führte zu einer sehr granularen Betrachtung der untersuchten Objekte sowie potentieller Bedrohungen der Verfügbarkeit, Integrität oder Vertraulichkeit dieser Objekte. Jeder potentiellen Bedrohung eines Objektes wurde ein Wert zugeordnet, der die Eintrittshäufigkeit der jeweiligen Bedrohung beschreibt. Die Schwierigkeit besteht hier in der möglichst genauen Abschätzung dieser Eintrittshäufigkeit. Diese Häufigkeit ist allerdings

in den meisten Fällen nicht nachweisbar. Das IT-Sicherheitshandbuch gibt hier nur den Hinweis, möglichst genau zu schätzen und zieht sich dann auf den Standpunkt zurück, daß die Schätzwerte in späteren Schritten – z.B. bei einer jährlichen Revision des IT-Sicherheitskonzeptes – angepaßt werden sollten. Die Häufigkeiten werden in sechs Kategorien (wie z.B. „sehr selten"... „sehr oft") logarithmisch eingeteilt, was die Schätzung etwas erleichtert.

In der detaillierten Risikoanalyse nach dem IT-Sicherheitshandbuch werden – im Gegensatz zur Grundschutzanalyse – die bereits realisierten Sicherheitsmaßnahmen in die Betrachtung mit einbezogen. Durch bereits realisierte Maßnahmen kann die Eintrittshäufigkeit von Ereignissen oder deren Schadenshöhe bereits gesenkt worden sein. Großen Einfluß auf die Feststellung, welche Risiken tragbar oder untragbar sind, hat zudem die individuelle Risikobereitschaft der jeweiligen Fachbereichseinrichtung, die nicht zuletzt von dem IT-Budget abhängt. Das Rechenzentrum kann beim Betrieb des Fachbereichsnetzes ein höheres Risko vertragen als beispielsweise die Bibliothek oder der Arbeitsbereich AGN. Im Fachbereichs-Rechenzentrum, das bereits viele IT-Sicherheitsmaßnahmen realisiert, konnten deswegen wesentlich weniger noch untragbare Risiken identifiziert werden als z.B. im Bereich des Bibliothekssystems oder der Virus-Datenbank des Arbeitsbereichs AGN.

6.4 Einbindung externer Gesellschaften

Schwierigkeiten anderer Art ergaben sich bei der Untersuchung der DFN CERT GmbH. Aufgrund der räumlichen und teilweise personellen Überschneidung mit den Fachbereichseinrichtungen (insbesondere dem Fachbereichs-Rechenzentrum) ergibt sich eine enge Verbindung mit dem Fachbereich. Die Sicherheitsmaßnahmen, vor allem übergeordnete Maßnahmen, müßten deshalb auch die DFN CERT GmbH umfassen. Da dessen IT-Sicherheitspolitik jedoch Gegenteiliges vorsieht – das DFN CERT ist juristisch seit Januar 1999 eine vom Fachbereich unabhängige GmbH – ergibt sich die Schwierigkeit, daß der Fachbereich das CERT nicht mit in die Untersuchung und damit in die vom Fachbereich unternommenen Sicherheitsmaßnahmen einbeziehen kann und darüberhinaus im eigenen Interesse sich gegenüber dem DFN CERT absichern muß.

Beispiel: Nutzt eine Einrichtung wie die DFN CERT GmbH den Fachbereichszugang zum WIN[1], so muß sie auch die Beschränkungen, z.B. die Firewall-Politik, des Fachbereichs akzeptieren bzw. mit dem Fachbereich aushandeln.

Durch die personelle Überschneidung in der Leitung der DFN CERT GmbH und des Fachbereichs-Rechenzentrums, das den WIN-Anschluß und die Firewall des Fachbereichs verwaltet, ist das derzeit kein großes Problem. Zudem hat das CERT höhere Sicherheitsinteressen als der Fachbereich, wird also eine schwächere Firewall des Fachbereichs durch eine eigene stärkere

[1] Wissenschafts-Netz, Internetzugang der Universität über den DFN-Verein

Firewall ergänzen.

Ein Problem tritt aber spätestens dann auf, wenn eine (andere), innerhalb des Fachbereichsgeländes residierende, eigenständige Gesellschaft ein geringeres Sicherheitsniveau fordert, als der Fachbereich gerne gewähren möchte. Hier kollidieren möglicherweise IT-Sicherheitsinteressen, der Fachbereich sollte sich mit dieser Problematik frühzeitig auseinandersetzen, da beispielsweise bereits bei der Verhandlung über den Einzug anderer Gesellschaften ins Gelände des Fachbereichs dieses beachtet werden muß.

6.5 Mehrstufiges Maßnahmenkonzept

Die Erstellung eines IT-Sicherheitskonzeptes für den Fachbereich nach derzeitiger Vorgehensweise ist sehr aufwendig, da im Fachbereich sehr vielfältige IT-Elemente zusammenkommen. Zudem wird durch die Eigenverantwortung der Fachbereichseinrichtungen im Bereich der Forschung und auch des dazu notwendigen Equipments das Niveau der IT-Sicherheit vom IT-Budget bestimmt. Weniger Geld für Sicherheitsmaßnahmen bedeutet mehr Geld für Forschung.

Der Fachbereich sollte zentral ein Mindestmaß an Sicherheit realisieren. Das ist im Kapitel 5 aus der Untersuchung ausgewählter Fachbereichseinrichtungen hergeleitet worden. Vorgeschlagen wird dort ein dreistufiges Konzept, hier kurz nochmals dargestellt:

1. Der Fachbereich realisiert grundlegende organisatorische Maßnahmen, die das Gesamterscheinungsbild des Fachbereichs nach außen beeinflussen, z.B. Sicherstellung und Vorschriften zur Kommunikation und Emailnutzung, aber auch Brand- und Einbruchschutz sowie Katastrophenvorsorge.

2. Die Arbeitsbereiche können darauf aufbauend eigene, weitergehende, Sicherheitsmaßnahmen realisieren, z.B. nach dem Baukastenprinzip. Hierfür könnten zentral vom Fachbereich fehlende Grundschutzbausteine entwickelt sowie Unterstützung bei der Anwendung gegeben werden.

3. Die hochschutzbedürftigen Projekte können dann zusätzlich mit einer detaillierten Risikoanalyse untersucht und dann individuell auf festgestellte Risiken reagieren.

6.6 Weiterführung des IT-Sicherheitsprozesses am Fachbereich Informatik

Das beschriebene und durchgeführte Verfahren ist als Teil eines IT-Sicherheitsmanagement-Prozesses gedacht. Die aufgezeigten Maßnahmen stellen einen Vorschlag zur Absicherung des Fachbereichs Informatik als einer wissenschaftlichen Einrichtung dar. Über deren Realisierung muß eine Entscheidung gefällt werden, die auch die Kosten der vorgeschlagenen Maßnahmen

berücksichtigt.

Wenn die Maßnahmen realisiert worden sind, muß in regelmäßigen Abständen eine Revision der IT-Sicherheit am Fachbereich von neuem beginnen, um neue Schwachstellen aufzuzeigen, Gefährdungen und Risiken zu identifizieren und Gegenmaßnahmen zu finden. Dabei muß nicht nur ein Gefühl für das Verfahren, sondern auch Routine im Umgang mit der Bewertung von Schadenspotentialen und, im Falle der detaillierten Risikoanalyse, der Bestimmung von Schadenshäufigkeiten gewonnen werden. Gerade weil hier Schätzwerte in die Analyse einfließen, müssen diese immer wieder auf ihre Plausibilität untersucht werden.

6.7 Fazit

Die beschriebene Vorgehensweise bietet einen Ansatz zur Absicherung einer wissenschaftlichen Einrichtung wie z.B. den Fachbereich Informatik. Sie muß jedoch weiter ausgearbeitet werden. Im Bereich des Grundschutzes fehlen u.a. Bausteine für Rechner-„Pool"-Räume und Rechner-„Labore" (so, wie sie in der Informatik verstanden werden).

Ein Nachteil der pauschalen Grundschutzanalyse nach [BSI1998] wird deutlich, wenn Einrichtungen mit vielen IT-Komponenten untersucht werden. Dies führt - im Teil II zu sehen - zu sehr umfangreichen Listen mit zu realisierenden Maßnahmen. Werden nun mehrere solcher Einrichtungen betrachtet, was in dieser Arbeit geschehen ist, so führt das zu Maßnahmenlisten, die sehr unübersichtlich und schwer zu vermitteln sind. Im Kapitel 5 wurde versucht, diese zu strukturieren.

Für die detaillierte Risikoanalyse sollte ein Verfahren gefunden werden, das es gestattet, die Häufigkeit von Schäden genauer zu klassifizieren. Für die Schadenswerte sollte eine Möglichkeit gefunden werden, eine zeitliche Komponente einzubringen, da die Schadensdauer oft Einfluß auf die Schadenshöhe hat. Ein Schaden, der z.B. durch die „Unterbrechung des Betriebs" hervorgerufen wird, ist oftmals nicht zu spezifizieren. Es kann sich um einen kurzen Ausfall mit geringen Kosten oder um eine einwöchige Betriebsunterbrechung mit hohen Kosten handeln, die zudem evtl. organisatorische Maßnahmen nach sich zieht. Hier sind die Kosten zeitabhängig; das war im durchgeführten Verfahren nicht einzubringen.

Insgesamt wurde jedoch im Laufe der Arbeit die Notwendigkeit deutlich, ein IT-Sicherheitskonzept auch für wissenschaftliche Einrichtungen zu erstellen und umzusetzen. Die oft als Argument angeführte Offenheit der Kommunikation innerhalb der Wissenschaft hat, das wurde am Beispiel der Drittmittelprojekte oder ganz konkret auch am Beispiel der Virus-Datenbank deutlich, ein Ende dort, wo „brisante" Daten generiert, gesammelt und ausgewertet werden und wo Forschungsergebnisse erzeugt werden, deren vorzeitige oder vollständige Veröffentlichung einen finanziellen Schaden oder Rufschaden für die Einrichtung oder einfach nur Nachteile für die betroffenen Wissenschaftler nach sich ziehen können.

Daneben wird zur Aufrechterhaltung des Wissenschaftsbetriebes Verwaltungsaufwand betrieben, wofür entsprechende Verwaltungsdaten (Personaldaten, Fiskaldaten, Planungsdaten) notwendig sind, wofür entsprechende Sicherheitsanforderungen aus dem Datenschutzrecht oder aus Verwaltungsvorschriften herleitbar sind. Auch dies rechtfertigt die Untersuchung und Umsetzung von Maßnahmen im Bereich der IT-Sicherheit.

Literaturverzeichnis

[BDSG] *Bundesdatenschutzgesetz vom 20. Dezember 1990*, in: Der Hamburgische Datenschutzbeauftragte (Hrsg.): Hamburger Datenschutzhefte - Das neue Datenschutzrecht; Hamburg, 1991

[BSI1998] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutzhandbuch 1998 - Manahmenempfehlungen für den mittleren Schutzbedarf*; Köln; Bundesanzeiger Verlagsges.mbH, 1998

[Chapman1997] D. Brent Chapman, Elisabeth D. Zwicky: *Einrichten von Internet-Firewalls* Dt. Ausgabe; O'Reilly; Internat. Thomson-Verl., Bonn, 1996

[c't 17/1999] *c't magazin für Computertechnik, Nr. 17/ 1999*, S. 130-151; Verlag Heinz Heise GmbH & Co KG, Hannover, 1999

[Duden] *DUDEN - Rechtschreibung der deutschen Sprache und der Fremdwörter* 19. Aufl.; Bibliographisches Institut, Mannheim, 1986

[Fraser1997] Barbara Y. Fraser: *Site Security Handbook, RFC 2196*, Network Working Group; CMU; Pittsburgh, 1997

[Freiss1998] Martin Freiss: *Protecting Networks with SATAN*; O'Reilly & Associates Inc., Sebastopol, 1998

[Garfinkel1996] Simson Garfinkel, Gene Spafford: *Practical UNIX and Internet Security*, 2nd Ed.; O'Reilly & Associates Inc., Sebastopol, 1996

[GMITS1] DIN-Fachbericht 66: *Informationstechnik - Leitfaden für das IT-Sicherheitsmanagement (GMITS), Teil 1*, 1997

[GMITS2] ISO/IEC TR 13335-2: *Information Technology - Guidelines for the management of IT Security, Part 2*, 1997

[GMITS3] ISO/IEC TR 13335-3: *Information Technology - Guidelines for the management of IT Security, Part 3*, 1998

[Goncalves1997] Marcus Goncalves: *Firewalls Complete*; McGraw Hill, 1997

[Hahn1990] Heiner Hahn: *Buchhaltung und Bilanz, Teil A: Grundlagen der Buchhaltung*, 3.Aufl.; Oldenbourg-Verlag; München, 1990

[ITSHB1992] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Sicherheitshandbuch, Handbuch für die sichere Anwendung der Informationstechnik*, Version 1.0, Bundesdruckerei, Bonn, 1992

[Kultus1998] Bayerisches Staatsministrerium für Unterricht, Kultus, Wissenschaft und Kunst (Hrsg.): *Sicherheit in Verwaltungs- und Kliniknetzen - Anforderungen, Möglichkeiten, Empfehlungen*; München, 1998

[Langenscheidt1990] Langenscheidt: *Taschenwörterbuch Englisch*; Langenscheidt KG, Berlin und München, 1990

[Liem1994] Peter Liem: *Ein Vergleich von IT-Sicherheitspolitiken großer Unternehmen*, Diplomarbeit, Universität Hamburg, Fachbereich Informatik; Hamburg, 1994

[LIT1998] Landesamt für Informationstechnik Hamburg (Hrsg.): *Integrierte und sichere Kommunikation - Ergebnisse der Vorstudie 1997*; Hamburg, 1998

[McMillan1998] Rob McMillan: *Site Security Policy Developement*, FTP-Ressource: ftp.auscert.org.au/security/papers/Site.Security.Policy.Developement.txt - heruntergeladen am 14.12.1998

[Pfleeger1998] Charles P. Pfleeger: *Security in Computing*, 2nd Ed.; Prentice Hall PTR, 1998

[Reymann1999] Peer Reymann: *IT-Sicherheitskonzepte von Großunternehmen - Zum Stand von Sicherheitspolitiken (Security Policies)*, Diplomarbeit; Universität Hamburg, Fachbereich Informatik; Hamburg, 1999

[Russell1992] Deborah Russell, G.T. Gangemi Sr.: *Computer Securuty Basics*; O'Reilly & Associates Inc., 1992

[Schuppenhauer1998] Rainer Schuppenhauer: *Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV); Handbuch der DV-Revision*, 5.Aufl.; Düsseldorf; IDW-Verlag, 1998

[Stelzer1992] Dirk Stelzer: *Sicherheitsstrategien in der Informationsverarbeitung: ein wissensbasiertes, objektorientiertes System für die Risikoanalyse*; Dt. Univ.-Verl., Köln, 1992

[Strauß1991] Christine Strauß: *Informatik-Sicherheitsmanagement*; B.G.Teubner, Stuttgart 1991

[Studienführer1997] *Studienfuehrer Informatik 1997/98*; Universität Hamburg, Fachbereich Informatik (Hrsg.); Hamburg, 1997

[TCSEC1985] *Department of Defense Trusted Computer System Evaluation Criteria* Fort George G. Meade, MD; National Computer Security Center, 1985