Zentren für Kommunikation und
Informationsverarbeitung in
Lehre und Forschung e. V.

ZKI

IT-Sicherheit an Hochschulen

Erarbeitet durch den ZKI-Arbeitskreis IT-Sicherheit
Version 1.0 – Oktober 2005

Inhalt:

1 Motivation 4
2 Derzeitige Situation an den Hochschulen 5
3 Begriffsdefinitionen 9
4 Einführung und Erhalt von IT-Sicherheit 9
5 Zusammenfassung 18
6 Muster A für eine IT-Sicherheitsordnung 19
7 Muster B für eine IT-Sicherheitsordnung 22
8 Anhang A: Literatur, Quellen und weiterführende Information 26
9 Anhang B: Glossar 28

Zum Geleit

Nach der Vorstellung der Autoren der vorliegenden Publikation „ IT-Sicherheit an Hochschulen“ des ZKI Arbeitskreises „IT-Sicherheit“ wurden als Zielgruppe Rektorinnen und Rektoren, Präsidentinnen und Präsidenten, Kanzlerinnen und Kanzler, Hauptamtliche Vizepräsidentinnen und -präsidenten sowie die gesamten Hochschulleitungen ausgemacht.

Dieser Vorstellung kann ich mich nach dem Studium der Publikation klar anschließen.

Wir müssen die politische und organisatorische Verantwortung für die Sicherheit der von uns angewendeten Informationstechnologien erkennen und entsprechend handeln. Dabei muss der aufscheinende Interessenskonflikt zwischen der von uns allen geforderten Handlungsfreiheit im Bereich Lehre und Forschung und den Belangen der notwendigen Sicherheit erörtert und eine beiden Seiten gerecht werdende, angemessene Lösung erreicht werden. Die Situation im IT-Bereich der Hochschulen spitzt sich, ohne übertreiben und Ängste hervorrufen zu wollen, deutlich zu. Die Zahl der Zwischenfälle häuft sich, was mit Sicherheit zu internen Auseinandersetzungen führt, darüber hinaus aber dem Ansehen der Hochschulen in der Öffentlichkeit schadet.

Die Inhalte der Publikation,

1. den Ausgangspunkt für die internen Diskussionen an den Einrichtungen,
2. einen praktischen Leitfaden und
3. eine Zusammenfassung der einzuleitenden Schritte für den Start des IT-Sicherheitsprozesses

darzustellen, ist eine bedeutsame Unterstützung bei der Bewältigung des einzuleitenden Prozesses.

Eine enge Kooperation zwischen den Hochschulleitungen und den IT-Verantwortlichen und ein schnelles Handeln bilden die Grundlage für einen erfolgreichen Prozessverlauf, das Fatalste wäre eine abwartende Position auf jeweils einer oder auf beiden Seiten der Verantwortlichen.

Die angestrebte IT-Sicherheit ist eine unverzichtbare Grundlage für den stabilen Einsatz der Informationstechnologien.

Eine intensive Beschäftigung mit diesem Papier ist meine Empfehlung.

im Original gezeichnet

Dr.-Ing. H. Schultz
Kanzler der Bauhaus-Universität Weimar
Bundessprecher

Zum Geleit

IT-Sicherheit an Hochschulen ist für die meisten deutschen Hochschulen ganz gewiss kein neues Thema. Einige Hochschulen haben sich der dahinter stehenden Herausforderung frühzeitig offensiv gestellt, in anderen Hochschulen wurden die erforderlichen Prozesse initiiert, die dann jedoch aus unterschiedlichen Gründen oft stecken blieben.

Als Ergebnis einer Anzahl von Diskussionen im ZKI wurde deutlich, dass viele Hochschulen hinsichtlich der dringend notwendigen Einführung von Strukturen, Verfahren und Maßnahmen zur nachhaltigen Gewährleistung von IT-Sicherheit einen signifikanten Unterstützungsbedarf haben.

Der Vorstand des ZKI griff dies auf, indem er zunächst eine Kommission benannte, mit dem Auftrag, bestehende Defizite aufzugreifen und Handlungsempfehlungen auszuarbeiten. Auf Grund des hohen Stellenwerts des behandelten Themas und um einen breiten Erfahrungsaustausch zu ermöglichen, wurde die Kommission dann in den Arbeitkreis „IT-Sicherheit“ überführt. In intensiver Zusammenarbeit der Mitglieder des Arbeitskreises wurde ein sowohl an die Hochschulleitungen als auch an die Rechenzentren adressiertes Papier zur IT-Sicherheit an den Hochschulen ausgearbeitet. Es soll den Hochschulen behilflich sein, die notwendigen Schritte zu identifizieren, einzuleiten und erfolgreich einen transparenten IT-Sicherheitsprozess nachhaltig in der Hochschule zu verankern. Es gibt Hilfestellung insbesondere auch bei der Operationalisierung der kürzlich publizierten und den Hochschulleitungen zugeleiteten „DFN-Checkliste IT-Sicherheit“.

Im Namen des Vorstands bedanke ich mich bei Herrn Dr. von der Heyde, der mit großem Engagement die Arbeit an diesem Papier koordiniert hat und bei allen Mitgliedern des Arbeitskreises für die von hoher Motivation getragene, kooperative und fachlich fundierte Zusammenarbeit.

im Original gezeichnet

Manfred Seedig
Vorsitzender des ZKI

1 Motivation

Forschung und Lehre sowie die unterstützenden Querschnittsfunktionen der Verwaltung an Hochschulen erfordern in zunehmendem Maß die Integration von Verfahren und Abläufen, die sich auf Informationstechnik (IT) und hierbei insbesondere auf vernetzte IT-Systeme stützen. Dies stellt die Hochschulen vor die Aufgabe, ihre gesamte IT und die darauf basierende globale Kommunikation funktional zu erhalten, zu sichern und bedarfsgerecht auszubauen. Die IT hat sich dabei zu einem der wichtigsten Arbeitsmittel für den modernen Hochschulbetrieb entwickelt. Folglich entsteht daraus ein hoher Anspruch an die Betriebsstabilität und Verfügbarkeit der IT-Systeme. Hierfür müssen organisatorische Maßnahmen getroffen und flankierend funktionale und technisch-infrastrukturelle Komponenten bereitgestellt werden. Ziel ist, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten in Zukunft sicherzustellen.
Die Erfahrung zeigt, dass vernetzte Computersysteme sowohl von innen, d.h. durch Angehörige der Hochschulen, als auch von außen durch Dritte angreifbar sind und missbraucht werden.

Ein solcher Missbrauch

- führt zu hohen Kosten für die Beseitigung der verursachten Schäden,
- beeinträchtigt oder verhindert die bestimmungsgemäße Nutzung der IT-Systeme und hält Administratoren und Benutzer von ihren eigentlichen Aufgaben ab,
- erhöht die Kosten für den Betrieb der Datennetze und der Anbindung an das Internet,
- verletzt die Vertraulichkeit von Daten und schädigt damit das Vertrauen der Benutzer in die IT,
- verstößt unter Umständen gegen geltendes Recht,
- kann zu Schadenersatzansprüchen führen,
- schädigt das Ansehen der Hochschule in der Öffentlichkeit und beeinträchtigt Kooperationen der Hochschule mit Partnern aus Wissenschaft und Industrie.

Eine Aussage von Experten ist: Hochschulen sind ein ideales Ziel von Angriffen, denn sie verfügen über eine hohe Bandbreite und in der Regel wenig gesicherte Systeme. Die „Sicherheit in der Informationstechnik“ („IT-Sicherheit“) bekommt damit für die Hochschulen eine grundsätzliche Bedeutung, welche die Entwicklung und Umsetzung einer einheitlichen, hochschulweiten Rahmenrichtlinie der IT-Sicherheit erforderlich macht. Dieses kann wegen der komplexen Materie, der sich weiter entwickelnden technischen Bedingungen und der begrenzten finanziellen Mittel nur in einem kontinuierlichen Sicherheitsprozess erfolgen.
Zusätzlich folgt aus einer Re-Zentralisierung der IT-Dienste eine enge Verflechtung und Abhängigkeit der Einrichtungen der Hochschule untereinander, so dass Insellösungen, die Partikularinteressen abbilden, mehr denn je unsinnig erscheinen. Der übergreifende Sicherheitsprozess muss an die besonderen Bedingungen der jeweiligen Hochschule angepasst sein. Es empfiehlt sich, den Sicherheitsprozess an Prinzipien zu orientieren, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutzhandbuch [GSHB][1], einem – auch international – anerkannten de-facto-Standardwerk zur IT-Sicherheit, niedergelegt sind.
Der DFN-Verein hat mit seiner Initiative vom Juni 2004 das Thema bereits in die Leitungsebenen der Hochschulen und öffentlich geförderten Forschungseinrichtungen getragen. Die vom DFN-Verein erarbeitete Checkliste [DFNCL] soll als fachliche Basis für einen konstruktiven Dialog innerhalb der Einrichtungen über die Sicherheit von Informationstechnik dienen.

[1] siehe Literatur in [ ] jeweils in Anhang A.

Ähnliche Aktivitäten werden durch das BSI vorangetrieben. In seinem Positionspapier [PosP] vom November 2004 unterstützt das BSI den Arbeitskreis der Leiter von Rechenzentren an wissenschaftlichen Hochschulen des Landes NRW (ARNW) bei der Verbesserung der IT-Sicherheit an Hochschulen. Das BSI und der ARNW haben dazu unter Mitwirkung der Netzagentur NRW als ersten Schritt fünf wichtige Eckpunkte identifiziert und Umsetzungsempfehlungen ausgearbeitet.
Das vorliegende Papier soll die Gefährdung der IT-Sicherheit deutscher Hochschulen ins Bewusstsein rücken und gleichzeitig konkrete Maßnahmen zu ihrer Verbesserung aufzeigen. Aus der Vergleichbarkeit deutscher Hochschulen (organisatorisch und strukturell) lassen sich allgemeine Grundsätze für eine sichere hochschulweite IT ableiten. Zielstellung und Funktion der eingesetzten IT-Systeme und der darauf basierenden Prozesse sind ähnlich und erleichtern damit die Formulierung konkreter IT-Sicherheitsmaßnahmen. Der AK „IT-Sicherheit“ des ZKI hat sich deshalb in diesem Papier der Aufgabe angenommen, diese Gemeinsamkeiten zu formulieren. Dabei wird versucht, die Leitungsebene der Hochschule ebenso wie die Leitungsebene des jeweiligen Rechenzentrums bei der umfassenden, organisatorischen Einführung von IT-Sicherheit zu unterstützen.

2 Derzeitige Situation an den Hochschulen

Der Einsatz von IT stellt sich an vielen deutschen Hochschulen z.Z. folgendermaßen dar:

2.1 Mangelndes Sicherheitsbewusstsein

Vielen Benutzern in Lehre, Ausbildung, Forschung und Verwaltung ist nicht bewusst, dass ihr Computer nicht nur ein Werkzeug ist, mit dem sie Informationen über das Internet in kürzester Zeit abrufen und verarbeiten können, sondern dass ihr Computer als Teil dieses Internets weltweit erreichbar ist. Schwachstellen durch unsichere Administration und Konfiguration, durch Programmfehler, durch unsichere Kommunikation und nicht zuletzt durch die Verwendung einfach zu erratender Passworte sind vorhanden.
Durch die oft vom Benutzer nicht wahrgenommene Erreichbarkeit des eigenen Rechners können Schwachstellen durch „Cracker“ oder Viren und Würmer innerhalb von Sekunden mit weitreichenden Folgen ausgenutzt werden: Der Rechner ist kompromittiert, die vertraulichen Daten sind ausspioniert oder manipuliert und urheberrechtlich geschützte Software ist gestohlen. Dies betrifft keineswegs nur den eigenen Rechner. Vielmehr ist damit eine gefährliche Ausgangsbasis für Attacken auf weitere Rechner innerhalb der Hochschule geschaffen.
Gängige alltägliche Schutztechniken, wie z.B. das Abschließen des Zimmers, wenn der Raum verlassen wird, das Verschließen von Aktenordnern in Schränken, das Sperren eines Telefons durch einen Zahlenfolge usw. sind auf das Arbeiten mit dem Computer übertragbar, aber selten in der erforderlichen Konsequenz umgesetzt. Teilweise liegt es daran, dass entsprechende Techniken nicht bekannt sind (vgl. „best practice“ Hinweise [BP]), teilweise an der fatalen Fehleinschätzung, dass schon „nichts Schlimmes“ passieren wird.

Schaffung von Sicherheitsbewusstsein:
Eine Verbesserung dieser Situation kann mit gezielter Information aller Benutzer, abgestimmten Grundschutzmaßnahmen oder durch die Erkenntnis des vorliegenden Risikos eingeleitet werden. Es müssen konsequente Anstrengungen unternommen werden, ein gemeinsames Verständnis von Benutzer und Administrator für das angestrebte Sicherheitsniveau zu schaffen. Jeder Einzelne muss sich als Teil eines IT-Verfahrens begreifen, in dem er eine bestimmte Rolle ausfüllt, in der er sich selbst veranlasst sieht, aktiv auf Sicherheit zu achten.

2.2 Unsichere Administration

Die meisten Hochschulmitarbeiter sind als Benutzer vom einwandfreien Funktionieren ihres Computers – im Sinne eines allgemeinen Werkzeugs – abhängig. Dies lässt sich mit der Benutzung eines Autos leicht vergleichen. Die technische Komplexität des Werkzeugs (bzw. Transportmittels) verhindert für den größten Teil der Benutzer den pflegenden Eingriff. Die Oberfläche kann, wie bei der Autowäsche poliert werden, aber den Ölwechsel (d.h. das Einspielen von neuer Software) muss der Fachmann übernehmen.
Erstaunlicherweise ist ein sehr unterschiedlicher Umgang mit dem Pflegeaufwand des Computers bzw. des Transportmittels zu beobachten. Selten stehen genügend kompetente Fachleute zur Verfügung, so dass die gängige Praxis ist, dass Computer schlecht „gepflegt“ (administriert) werden. Es werden keine „Patches“ eingespielt, es werden keine Daten gesichert, es wird nicht geprüft, ob unnötige Programme ständig laufen und wo wichtige Daten gespeichert werden. Auch das hat fatale Folgen: Schlecht gepflegte Rechner sind leichter angreifbar, laufen instabiler und sind nicht so leistungsfähig wie gut gepflegte Rechner. Fällt so ein Computer schließlich aus, kommt ein weiterer Aspekt der mangelnden Pflege zum Tragen: Der Benutzer kennt sich mit seinem System nicht aus, weiß nicht, wie er es wieder reparieren soll; er hat sich schließlich nie zuvor mit der Administration beschäftigt!
Auch hierfür gibt es eine Vielzahl von Gründen: Betriebsysteme und Programme lassen sich leicht und einfach installieren bzw. sind häufig schon bei der Auslieferung vorinstalliert. Der Benutzer weiß nicht, wie aufwändig eine Wiederherstellung sein kann. Viele Hersteller von Computern und Programmen liefern ihre Systeme auch in einer meist funktional überfrachteten Konfiguration aus, die Fehler und Angriffsrisiken erhöht. Häufig werden die vorhandene Sicherheitsfeatures im Auslieferungszustand nicht oder nur unzureichend aktiviert. Viele Benutzer wiederum verstehen nicht, dass sie persönlich die Pflege des Rechners übernehmen müssen, falls keine zentrale Administration vorhanden ist. Sie wollen schließlich nur mit dem Rechner arbeiten und häufig fehlt ihnen auch das entsprechende Fachwissen. Fatal ist in diesem Zusammenhang nicht das fehlende Fachwissen der Benutzer, sondern dass sie sich nicht um eine adäquate Administration ihrer Rechner durch Hochschulrechenzentren oder Institutsadministratoren kümmern. Möglicherweise sind aber auch die Zuständigkeiten für die Administration der Mitarbeiterrechner nicht festgelegt, unzureichend kommuniziert oder sie werden nicht konsequent genug durchgesetzt.

Festlegung von Zuständigkeiten und Administrationsstandards:
Die Situation kann entscheidend verbessert werden, wenn die Zuständigkeit für die Pflege (Administration) klar durch die Hochschulleitung geregelt wird. Die Festlegung von einheitlichen Administrationsstandards in Form einer Rahmenrichtlinie kann die notwendige Basis für IT-Sicherheit legen. Wie im Straßenverkehr ist ein Mindestmaß an Einhaltung dieser Regeln unabdingbar, um Unfälle zu vermeiden.

2.3 Unsichere Kommunikation

Auch bei der Verwendung des Internets gibt es an den deutschen Hochschulen viele Benutzer, die sich über die hiermit verbundenen Risiken nicht bewusst sind. Es ist tägliche Praxis, über das Internet seine elektronische Post (E-Mail) zu verarbeiten und bei Händlern beispielsweise Bestellungen zu veranlassen. Nur wenige Benutzer wissen allerdings, ob die Übertragung ihrer persönlichen Kennungen hierbei geschützt wird oder von Dritten mitgelesen werden kann. Vielerorts verlassen sich Benutzer auf die Netztechnik und unterstellen dieser einen ausreichenden Schutz auch bei unverschlüsselter Übertragung. Dies mag bei der Verwendung moderner (strukturierter) Verkabelungssysteme sogar zutreffen, gerade aber bei der Verwendung von aktuellen Funktechnologien wie „Wireless LAN“ oder „Bluetooth“ gelten diese Annahmen nicht mehr.

Viele Benutzer, die ein Grundverständnis für sichere Kommunikation haben und nach Möglichkeit Verschlüsselungstechniken einsetzen, haben dennoch selten ein Verständnis für die erforderlichen Zertifikatsüberprüfungen. Die z.Z. unter der Bezeichnung „Phishing“ oder “Visual Spoofing“ auftretenden Missbrauchsfälle, bei denen Benutzer auf täuschend echt wirkenden Seiten von Kriminellen bei ihren Eingaben ausspioniert werden, zeigen nur zu deutlich, dass es hier einen enormen Nachholbedarf sowohl technologisch als auch bei der Aufklärung und Schulung der Benutzer gibt.
Bei den an den Hochschulen in immer stärkerem Maße eingesetzten verteilten und daher auf Kommunikation angewiesenen Arbeitsabläufen, wie z.B. Studierenden- und Prüfungsverwaltung oder Bearbeiten von vertraulichen interdisziplinären Forschungsergebnissen auf dezentralen Projektservern, ist unmittelbar einsichtig, dass es keinen Spielraum mehr für unsichere bzw. ungesicherte Kommunikation an den Hochschulen gibt.

Berücksichtigung der IT-Sicherheit bei der Prozessgestaltung:
Die Kommunikation muss bewusst die (Un-)Sicherheit des Kommunikationswegs berücksichtigen. Ziel ist, die technologischen Lösungen so einzusetzen, dass die organisatorisch festgelegten Kommunikationswege angemessen gesichert werden. Bei der Gestaltung von neuen Arbeitprozessen muss die Kommunikation explizit berücksichtigt werden.

2.4 Mangelnde Übersicht und mangelnde Kontinuität

Viele Arbeitsprozesse sind auf den Einsatz von IT inzwischen angewiesen. Häufig wird erst bei ungeplanten Ausfällen den dann Betroffenen diese Abhängigkeit bewusst. Die Ursache für die nicht bekannten Risiken liegt darin begründet, dass der Einsatz der IT über die Jahre gewachsen ist, ohne dass die Rollen der Beteiligten und entsprechende Ressourcen definiert wurden.
Viele Einrichtungen der Hochschule bieten offene oder auf eine bestimmte Benutzergruppe beschränkte IT-Dienste an. Die genutzte Hardware entspricht nicht mehr den aktuellen Erfordernissen, Daten werden nicht gesichert, die Verantwortlichkeiten ändern sich häufig und werden nur halbherzig wahrgenommen, letztlich geht das ursprünglich vorhandene Know-How verloren. Nach dem Motto „Never change a running system!“ bleiben solche Server „sicherheitshalber“ von weiteren Eingriffen seitens der Betreiber verschont bis sich schließlich ein Hacker dem System annimmt.

Vollständige Erfassung der IT-Verfahren:
Die längerfristige Sicherstellung eines funktionierenden und sicheren IT-Gesamtsystems einer Hochschule kann nur dann gelingen, wenn die Informationen über alle vorhandenen IT-Installationen (IT-Verfahren) an einer zentralen Stelle zusammengeführt und die Systembetreiber mit Informationen über andere IT-Systeme, zu ergreifende Sicherheitsrisiken und -maßnahmen versorgt werden können.

2.5 Alltägliche Sicherheitsrisiken

Zusammenfassend kann man festhalten, dass an den deutschen Hochschulen die wenigsten IT-Benutzer die alltäglichen Sicherheitsrisiken bei Inter-/Intranet-basierten Arbeitsabläufen verstanden haben, geschweige denn in der Lage wären, ihre Systeme und Arbeitsweisen entsprechend zu sichern.
Das Herunterladen einer Datei aus dem Internet, das „Anklicken“ einer E-Mail oder das Starten eines Programms kann bereits dazu führen, dass der Computer mit Viren/Trojanern infiziert wird, wichtige Daten unwiederbringlich gelöscht werden und der „eigene“ Computer von Kriminellen als Tauschbörse für Raubkopien urheberrechtlich geschützter Software missbraucht wird.

Weltweit steigt sowohl die Zahl der bekannt gewordenen Sicherheitslücken als auch die Zahl der sicherheitsrelevanten Vorfälle von Jahr zu Jahr. Die Abbildung 1 zeigt die Anzahl aller Vorfälle mit Bezug zur IT-Sicherheit, die durch das DFN-CERT in den zurückliegenden zehn Jahren bearbeitet werden mussten. Die Zahl der betroffenen Systeme dürfte sehr viel größer sein, da in verteilte Angriffe (z.B. Distributed Denial of Service-Attacken (DDoS)- oder Botnet Attacken) gleichzeitig eine Vielzahl von Einrichtungen[2] involviert sind.

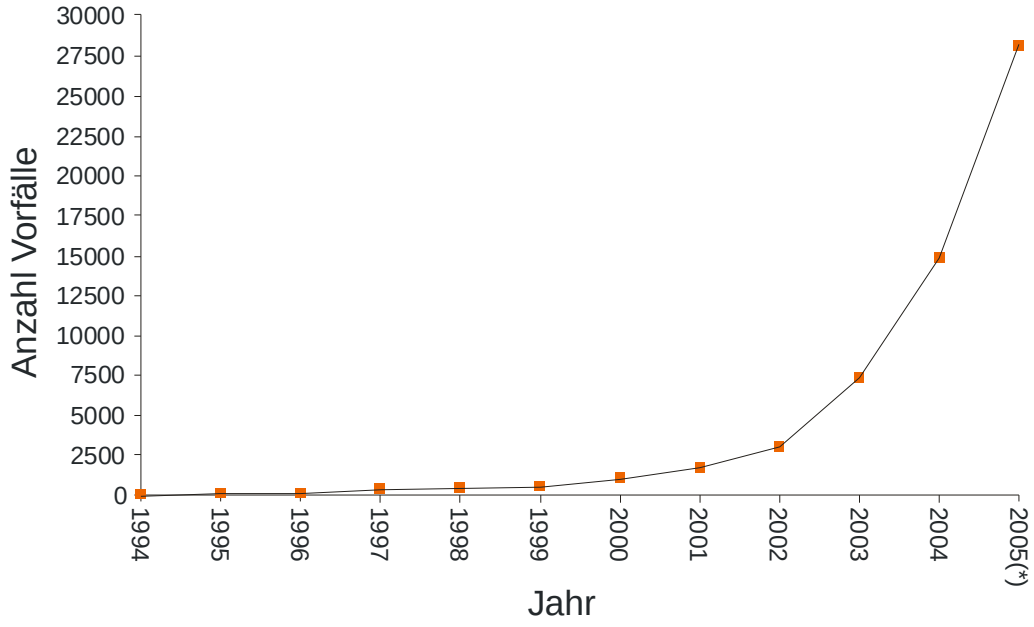

Abbildung 1: Vom DFN-CERT bearbeitete Vorfälle. (*)Die Zahl der Fälle im Jahr 2005 wurde aus den vorliegenden Monaten extrapoliert. Mitte Juli lag die Anzahl der tatsächlich gemeldeten Vorfälle bereits über 15.000.

2.6 Zusammenfassung der Situation

Ist die Lage an den deutschen Hochschulen wirklich so bedrohlich? Die Folgen aus dem mangelnden Sicherheitsbewusstsein, der unsicheren Administration, der unsicheren Kommunikation und den alltäglichen Sicherheitsrisiken sind nicht immer offensichtlich und bleiben oft unbemerkt.
Wie in der Wirtschaft ist es unter den Betroffenen unpopulär, die Vorfälle intern zu dokumentieren oder extern zu veröffentlichen. Die Dunkelziffer der Vorfälle ist daher schlecht schätzbar. Häufig werden durch das Engagement Einzelner die (zu spät) entdeckten Sicherheitslücken geschlossen, Systeme wieder in Betrieb genommen und lokale Maßnahmen ergriffen, um identische Vorfälle in Zukunft zu vermeiden. Die investierte Arbeitszeit wird mit ohnehin anstehenden Verbesserungen verbunden und als unvermeidbar aufgefasst.
Als konsequenter Ausweg aus dieser Situation wird in Abschnitt 4 der Weg aufgezeigt, wer mit wem die IT-Sicherheit an einer Hochschule etablieren kann. Das übergeordnete Ziel dabei ist, die Sicherheit der Geschäftsprozesse in Forschung, Lehre und Verwaltung, welche auf den Einsatz von Informationstechnologien angewiesen sind, herzustellen, indem Risiken erkannt und durch angemessene Maßnahmen kalkulierbar und akzeptabel gehalten werden. Dafür ist es notwendig, dass die Hochschulleitung die Verantwortlichkeit und Zuständigkeit sowie Kommunikationswege zur Herstellung und Erhalt der Sicherheit regelt. Die Balance zwischen Restriktionen und Freiheit soll die Funktionstüchtigkeit des Gesamtsystems bewahren.

[2] Die überwiegende Anzahl sind hierbei Hochschulen.

3 Begriffsdefinitionen

Sicherheit in der Informationstechnik (kurz **IT-Sicherheit**) heißt, innerhalb eines betrachteten Bereichs (engl. scope) (z.B. PC-Arbeitsplätze, E-Mail, elektronische Bibliotheken, Prüfungsverwaltung, Hochleistungsrechner, Gesamtheit der IT-Verfahren der Hochschule) die nachfolgend aufgelisteten Eigenschaften entsprechend der Vorgaben der Hochschulleitung und bestehender rechtlicher Auflagen durch Maßnahmen zu gewährleisten bzw. die potentiellen Bedrohungen so einzuschränken, dass die verbleibenden Risiken tragbar sind[3].

- **Vertraulichkeit** (engl. confidentiality)
  bezeichnet einen Zustand, in dem eine Informationsgewinnung aus sensiblen Daten nur berechtigten Personen und in der zulässigen Weise möglich ist.
- **Integrität** (engl. integrity)
  bezeichnet einen manipulationsfreien Zustand von Daten und/oder IT-Systemen.
- **Verfügbarkeit** (engl. availability)
  bezeichnet einen Zustand, in dem Daten, Dienste und Funktionen eines IT-Systems und seiner Komponenten von den berechtigten Personen zum geforderten Zeitpunkt, in der vorgesehenen Zeit und in zugesicherter Form und Qualität nutzbar sind.
- **Authentizität** (engl. authenticity)
  bezeichnet einen Zustand, in dem Daten jederzeit ihrem Ursprung zugeordnet werden können und die Identität von Personen und IT-Systemen nachvollzogen werden kann.
- **Verbindlichkeit** (engl. liability)
  charakterisiert einen Zustand, in dem die Durchführung einer Handlung mittels eines IT-Systems durch die agierende Instanz im Nachhinein nicht abgestritten werden kann.
- **Vermeidung von Missbrauch**
  bedeutet die Durchsetzung des Rechtes der Betreiber und/ oder Nutzer, die eigenen IT-Systeme nur für den vorgesehenen Zweck zu gebrauchen.
- **Konsistenz** (engl. consistency)
  bezeichnet einen Zustand, in dem sichere Subsysteme ein sicheres Gesamtsystem ergeben.

4 Einführung und Erhalt von IT-Sicherheit

Vorbemerkung

Die Einführung von Strukturen, Verfahren und Maßnahmen zur nachhaltigen Gewährleistung von IT-Sicherheit innerhalb einer Hochschule benötigt völlig neue Funktions- und Rollenverständnisse in der Institution. Angenehm daran ist, dass nicht zunächst überkommene Strukturen abgebaut werden müssen, sondern dass von Beginn an am Aufbau einer nützlichen Struktur gearbeitet werden kann.

Die Verankerung von IT-Sicherheit ist zunächst Chefsache

IT-Sicherheit hat zum Ziel, die Geschäftsprozesse in Forschung, Lehre und Verwaltung in breitem Umfang vor Bedrohungen zu schützen und missbräuchliche Nutzung zu verhindern und damit die Arbeitsfähigkeit und das Ansehen der Hochschule zu wahren. Das Leitungsgremium der Hochschule trägt hier die Gesamtverantwortung für die Sicherheit der IT der Hochschule. Für Unternehmen in der Wirtschaft wurde hierzu im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) die Verantwortlichkeit der Unternehmensführung explizit festgelegt. Für diese Verantwortlichkeit muss in manchen Einrichtungen ein entsprechendes Bewusstsein geschaffen werden. Zur Schaffung einer

[3] Ein vollständiges Glossar findet sich in Anhang B.

angemessenen IT-Sicherheit müssen gegebenenfalls zunächst in einem Kraftakt erhebliche Personal-Ressourcen eingesetzt werden und es sind unter Umständen „unbequem erscheinende“ Maßnahmen notwendig, die nachhaltig Missstände beseitigen bzw. vermeiden helfen. Dies macht eine unmittelbare und aktiv wahrgenommene Unterstützung durch die Hochschulleitung notwendig. Aufgabe der Hochschulleitung ist es, eine positive Meinungsbildung über IT-Sicherheit und ein hochschulweit einheitliches Verständnis für die Sicherheitsanforderungen, die Risikobewertung und die Risikobehandlung zu schaffen und zu fördern. Sie trifft in enger Rückkopplung mit allen Partnern im Prozess alle notwendigen organisatorischen Entscheidungen und stellt die benötigten finanziellen und personellen Ressourcen bedarfsgerecht bereit.

4.1 Anfangsbetrachtungen – Welches sind die ersten Schritte?

Kommunikation des angestrebten Ziels:
Fundamental ist die für jeden transparente Definition und Kommunikation des angestrebten Ziels der IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit). Hierbei kann man von Fall zu Fall sicherlich unterschiedlich gewichten bzw. muss man für Forschung, Lehre und Verwaltung unterschiedliche Gewichtungen zulassen. Insgesamt sollten sich jedoch Auftraggeber, Anwender und Betreiber von Informationstechnologie einig sein, was zu tun ist, damit sich jeder im Umgang mit und in der Anwendung der IT berechtigt sicher fühlt. Hierzu gilt es, insbesondere datenschutzrechtliche und personalvertretungsrechtlich relevante Belange zu kommunizieren und ein gemeinsam akzeptiertes Verständnis über die wesentlichen technischen Grundbegriffe zu erreichen.

Erstellen und Verabschieden einer IT-Sicherheitsordnung:
Die Sicherheitsordnung regelt vor allem Verantwortlichkeiten. Weiterhin werden Zuständigkeiten und Kommunikationswege beschrieben. Die IT-Sicherheitsordung stellt somit die von der oberen Leitungsebene formulierte Ziel-Vorgabe zur Erreichung eines erwünschten Schutzniveaus für den gesamten IT-Einsatz dar.

Erstellen und Verabschieden einer Rahmenrichtlinie der IT-Sicherheit:
In dieser Rahmenrichtlinie werden die verbindlichen, grundsätzlich anzuwendenden Verfahren und Maßnahmen zum Schutz der IT-Verfahren definiert. Diese Festlegungen müssen in stetiger Abwägung und Überarbeitung den gegebenen Anforderungen, Bedrohungen und Szenarien angepasst werden. Diese Fortschreibung wird als IT-Sicherheitsprozess bezeichnet und von den in der Ordnung definierten Gremien und Personen übernommen und sichergestellt.

4.2 Mit wem ist der Prozess zu gestalten?

Der Sicherheitsprozess stellt eine große Herausforderung für die Hochschulangehörigen dar, welche aber durch die Benennung bzw. sachgerechte Auswahl geeigneter Partner abgefedert werden kann. Die Rahmenrichtlinie, hier insbesondere die Vorgaben für die Beschreibung des IT-Einsatzes und die Formulierung der für die Hochschule relevanten Grundschutzmaßnahmen, sollte unbedingt als gemeinsame Gesamtaufgabe verstanden werden. Datenschutzbeauftragter, Personalvertretungen, Besitzer, Verarbeiter und Anwender von Daten sind aufgefordert mitzuarbeiten. Sie müssen zunächst gemeinsam geschult werden, sodass von Beginn an das Ziel, die Begrifflichkeiten und die übertragenen Aufgaben allen gleichermaßen bekannt sind. Auch ist es – gerade in der derzeitigen Lage der Haushalte – notwendig, von vorn herein das Kosten-Bewusstsein aller Beteiligten zu wecken.

Die im Rahmen des Prozesses immer wieder zu beantwortenden Fragen könnten sein:

Wie schaffen wir ein gemeinsames IT-Sicherheitsszenario, in dem die Ziele notwendiger Vertraulichkeit, Integrität und Verfügbarkeit erreicht werden?
Wie schaffen wir eine personalvertretungs- und datenschutzrechtlich konforme IT-Landschaft für die Hochschule?
Wie schaffen wir eine gemeinsame, funktionstüchtige und ressourcenschonend nutzbare IT-Infrastruktur für die Hochschule?

Etablierung von IT-Sicherheit auf Leitungsebene

Basierend auf der sicherlich veranlassenden und steuernden Rolle der Hochschulleitung gibt es eine Vielzahl von wichtigen Rollen/Funktionen im Prozess, die gemeinsam die weiter oben gestellten Fragen für sich und für die Hochschule beantworten und letztlich damit den Prozess gemeinsam vorantreiben müssen. In den Materialen zu diesem Dokument finden sich zwei Muster von Sicherheitsordnungen, die ähnliche Modelle zur personellen Verankerung eines IT-Sicherheitsprozesses an einer Hochschule beschreiben. Die fachliche Verantwortung für alle IT-Sicherheitsfragen innerhalb der Hochschule muss eindeutig festgelegt werden. Je nach lokalen Gegebenheiten empfiehlt es sich, eine der beiden folgenden Varianten strukturell in der Hochschule zu verankern:

Zentraler IT-Sicherheitsbeauftragter – Vorschlag in Korrespondenz zu Muster A

Es wird ein zentraler IT-Sicherheitsbeauftragter für die Hochschule eingesetzt[4]. Der IT-Sicherheitsbeauftragte hat die fachliche Verantwortung für alle IT-Sicherheitsfragen innerhalb der Hochschule. Zu seinen Pflichten gehören:

- die Leitung des IT-Sicherheitsprozesses in der Hochschule,
- die verantwortliche Mitwirkung an der Erstellung und Weiterentwicklung des IT-Sicherheitsmanagements,
- die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsmaßnahmen,
- die Planung und Koordination von Schulungs- und Informationsmaßnahmen,
- die Gewährleistung der IT-Sicherheit im laufenden Betrieb,
- die Einsatzplanung der für IT-Sicherheit zur Verfügung stehenden Ressourcen.

Der zentrale IT-Sicherheitsbeauftragte kann einzelne Aufgaben delegieren. Die Gesamtverantwortung für die IT-Sicherheit verbleibt aber bei ihm. Er soll direkt bei der Leitung angesiedelt sein und Zugriff auf dezentrale Ressourcen haben, also Weisungsbefugnis innerhalb des IT-Sicherheitsbereichs haben. Ein informeller Arbeitskreis, in dem die dezentralen IT-Sicherheitsbeauftragten ggf. zusammen mit dem Rechenzentrum regelmäßig über anstehende Aufgaben beraten, wäre in diesem Zusammenhang hilfreich.
Der zentrale IT-Sicherheitsbeauftragte ist die treibende Kraft, die neue IT-Sicherheitsrichtlinien vorstellt, mit den Entscheidungsträgern in den einzelnen Fakultäten, wissenschaftlichen, zentralen und sonstigen Einrichtungen ihre Notwendigkeit diskutiert und gemeinsam mit den dezentralen IT-Sicherheitsbeauftragten die angemessenen IT-Sicherheitsmaßnahmen entwirft und ihre Umsetzung vorantreibt.

[4] Mit dem zentralen IT-Sicherheitsbeauftragten steht und fällt der Erfolg aller Bestrebungen, IT-Sicherheit innerhalb der IT der Hochschule zu implementieren. Daher sind mögliche Interessenskonflikte bei der Besetzung zu berücksichtigen. Eine Ämteranhäufung (z.B. Sicherheitsbeauftragter und RZ-Leiter) muss aus Gründen der Neutralität unbedingt vermieden werden.

IT-Sicherheits-Management-Team – Vorschlag in Korrespondenz zu Muster B

Es wird ein IT-Sicherheits-Management-Team (SMT) von der Hochschulleitung eingesetzt. Dieses nimmt als Gruppe die oben beschriebenen Aufgaben des IT-Sicherheitsbeauftragten wahr. Das SMT ist ein politisches und damit entscheidendes Organ. Basierend auf heterogener Zusammensetzung aus Entscheidungsträgern und Fachleuten, berät und beschließt es alle Fragen in Sachen IT-Sicherheit. Die fachliche Verantwortung für alle IT-Sicherheitsfragen innerhalb der Hochschule liegt beim Vorsitzenden des SMT. Ziel ist es, ein funktionierendes Gleichgewicht zwischen Entscheidungsträgern und Fachleuten herzustellen. Die fachliche Qualifikation bestimmt dann die Aufgabenverteilung. Einerseits stecken Fachleute die Grenzen einer produktiven und sicheren IT ab. Andererseits ist die Beschränkung einer vollkommen offenen und ungepflegten IT ohne die volle Unterstützung der Entscheidungsträger nicht durchzusetzen.
Das SMT schreibt die Rahmenrichtlinie der IT-Sicherheit fort und legt jährlich einen IT-Sicherheitsbericht vor. Dazu ist es notwendig, dass beim SMT die sicherheitsrelevanten Informationen zusammenlaufen, damit daraus ein vollständiges Bild der IT-Sicherheit der Hochschule entstehen kann. Das SMT kann zur Unterstützung seiner Arbeit im operativen Bereich eine Arbeitsgruppe einsetzen.

Etablierung von IT-Sicherheit auf Instituts- bzw. Bereichs-Ebene

Um die IT-Sicherheit in der gesamten Hochschule organisatorisch zu verankern und um die Belange der Fakultäten und Einrichtungen angemessen zu berücksichtigen, ist es notwendig, in den Fakultäten und Einrichtungen dezentrale IT-Sicherheitsbeauftragte in verantwortlicher Rolle/Funktion zu benennen und diese von Beginn an in den gesamten IT-Sicherheitsprozess zu integrieren. Je näher von Beginn an seitens der Basis mitgewirkt wird, desto größer ist die Aussicht darauf, dass eine Rahmenrichtlinie der IT-Sicherheit mit allen Verfahren und Maßnahmen realisiert und gelebt wird.

Die Einrichtungen der Hochschule müssen verpflichtet werden, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zur IT-Sicherheit die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten sowie das SMT zu beteiligen[5]. In der Gesamtsicht auf eine große Einrichtung kann es sinnvoll sein, ein Anforderungsprofil eines IT-Sicherheitsbeauftragten hochschulweit zu definieren, sodass Rechte und Pflichten einheitlich vorgegeben sind. Grundlage hierfür können folgende Überlegungen bzw. Aufgabenstellungen sein:

- die Erfassung und Aktualisierung aller IT-Verfahren in einem Bereich,
- die Erarbeitung eines detaillierten Plans zur Realisierung von IT-Sicherheitsmaßnahmen in einem Bereich,
- die Verantwortlichkeit für die Umsetzung dieses Realisierungsplans,
- die regelmäßige Prüfung der Wirksamkeit und Einhaltung der eingesetzten IT-Sicherheitsmaßnahmen,
- die Meldung von sicherheitsrelevanten Ereignissen an den zentralen IT-Sicherheitsbeauftragten bzw. das Sicherheits-Management-Team (SMT),
- die Unterstützung des zentralen Sicherheitsbeauftragten bzw. des SMT bei der Sammlung von sicherheitsrelevanter Information (z.B. für die Berichtserstellung).

[5] Siehe Muster A §6 (5) bzw. Muster B §5 (7)

4.3 Der erste Meilenstein: die IT-Sicherheitsordnung

Muster A und Muster B stellen in sich schlüssige Entwürfe für eine IT-Sicherheitsordnung dar. Diese können als Ausgangspunkt für die interne Diskussion in der eigenen Hochschule herangezogen werden. Sie sind in sich konsistent und bereits an Hochschulen umgesetzt worden[6].

Gemeinsamkeiten der vorgeschlagenen IT-Sicherheitsordnungen

1. Beide Entwürfe stimmen im Kern überein. Es werden jeweils diejenigen Gremien und ihre Zusammensetzung festgelegt, die im IT-Sicherheitsprozess Aufgaben und Verantwortungen übernehmen sollen. Eine IT-Sicherheitsordnung legt lediglich die Struktur fest, in welcher der IT-Sicherheitsprozess an der Hochschule durchgeführt wird. Was es mit einem IT-Sicherheitsprozess auf sich hat, erklären die Muster nicht. Vielmehr setzen sie das Verständnis hierfür implizit voraus.
2. Der Geltungsbereich der IT-Sicherheitsordnung entspricht organisatorisch genau dem Einflussbereich der Hochschule. Werden über den IP-Bereich der Hochschule externe Einrichtungen versorgt, müssen diese zur sinngemäßen Anerkennung der IT-Sicherheitsordnung verpflichtet werden.
3. Für den besonderen Fall der Gefahren- bzw. Krisenintervention führen beide Entwürfe in gesonderten Paragraphen die präventiven und reaktiven Maßnahmen an, die im Gefahren- oder Schadensfall greifen sollen.
4. Die Aufgaben und Zuständigkeiten der dezentralen IT-Sicherheitsbeauftragten, der Einrichtungen der Hochschule und des Rechenzentrums stimmen in beiden Vorschlägen weitgehend überein.

Unterschiede der vorgeschlagenen IT-Sicherheitsordnungen

In den Unterschieden zwischen den Entwürfen (Muster A und Muster B) spiegeln sich zum einen strukturelle Entscheidungen über die Organisation der am IT-Sicherheitsprozesses Beteiligten wider (Punkt 1 und 2), zum anderen verdeutlichen sie den möglichen Spielraum beim Formulieren einer IT-Sicherheitsordnung (Punkt 3).

1. Die Strukturen, in denen der IT-Sicherheitsprozess implementiert wird, unterscheiden sich in den beiden Vorschlägen (siehe Abbildung 2 und Abbildung 3). Das IT-Sicherheits-Management-Team übernimmt im Entwurf B die zentrale Funktion. Seine Zusammensetzung und die Zuarbeit durch eine Arbeitsgruppe im operativen Bereich unterstreicht die Trennung zwischen Entscheidungsträgern und Fachleuten. Im Entwurf A konzentriert sich alles auf den zentralen IT-Sicherheitsbeauftragten, bei dem alle Informationen zusammenlaufen und der den IT-Sicherheitsprozess eigenverantwortlich vorantreiben soll.
2. Der Entwurf B verlangt nicht notwendig, dass die in das IT-Sicherheits-Management-Team entsandten Vertreter auch Mitglieder der sie delegierenden Einrichtungen sind. Dies eröffnet dem Leitungsgremium der Hochschule die Möglichkeit, mit ihrem Vertreter einen quasi zentralen IT-Sicherheitsbeauftragten zu installieren.
3. Darüber hinaus gibt es im Entwurf A Weglassungen, die im Entwurf B explizit Erwähnung finden; in der Präambel: der ausdrückliche Hinweis auf das Grundschutzhandbuch des BSI; in §1: die Nennung einer Benutzungsordnung als Bestandteil der Ordnung der Informationstechnik (siehe hierzu auch §6 Abs. 5); in §3: die Hervorhebung, dass IT-Sicherheit eine Sache der Hochschulleitung ist; in §5: die herausgehobene Rolle des Rechenzentrums für technische Aspekte der IT-Sicherheit und bei der Krisenintervention (siehe §7 Abs. 2) und in §6: die Bildung eines

[6] Als Vorlage für die zwei Muster diente die Ordnung aus Hannover. Muster A wurde an der FH Frankfurt umgesetzt; Muster B wurde in Weimar gemeinsam für zwei Hochschulen umgesetzt.

Arbeitskreises zum Erfahrungsaustausch über den Fortgang des IT-Sicherheitsprozesses und zur weiteren Abstimmung.

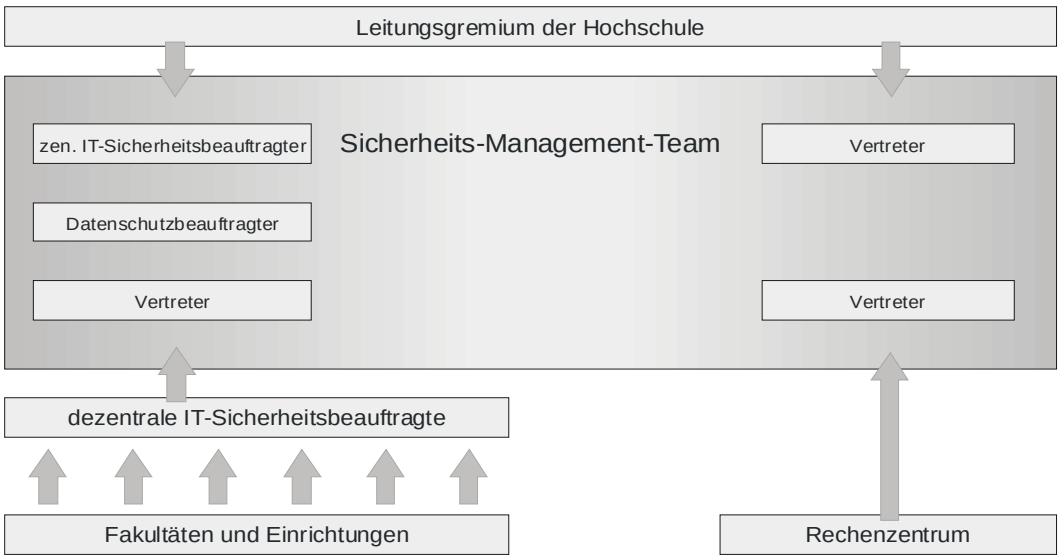

Abbildung 2: Organisationsstruktur im Ordnungsentwurf aus Muster A.

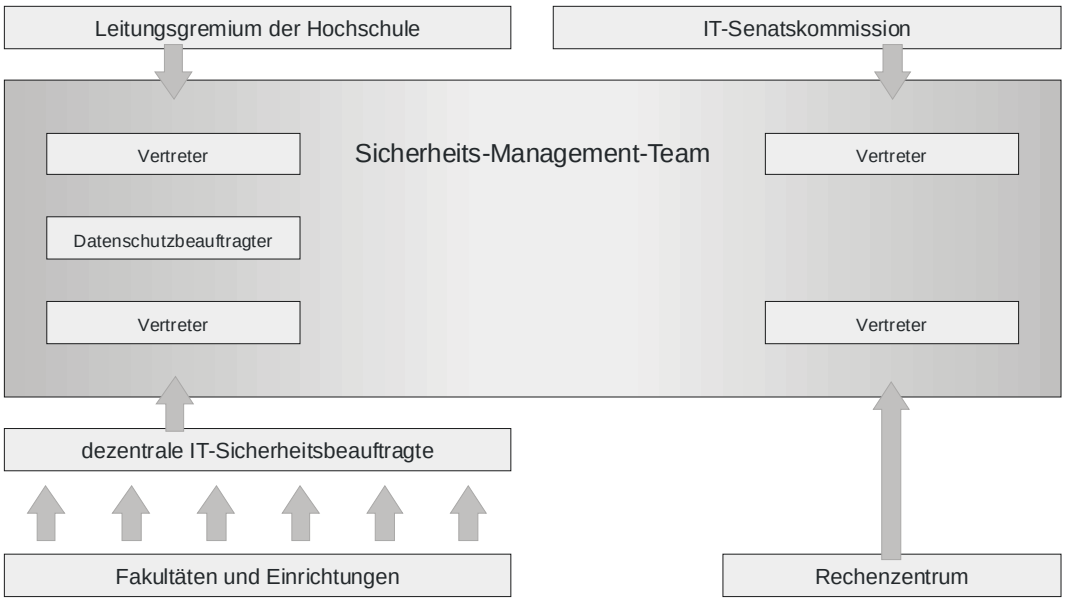

Abbildung 3: Organisationsstruktur im Ordnungsentwurf aus Muster B.

4.4 Der zweite Meilenstein: die Rahmenrichtlinie für IT-Sicherheit

Die Rahmenrichtlinie [RRL], die als Material diesem Dokument beigefügt ist, gliedert sich wie folgt:

- Beschreibung der Ausgangsituation
- Beschreibung der Grundschutzmaßnahmen
- Anleitung für eine Schutzbedarfsanalyse als Basis zur Beschreibung des IT-Einsatzes
- Anleitung für eine Risikoanalyse zur Erfassung ganz besonders sensibler IT-Bereiche
- Beschreibung der Umsetzung der IT-Sicherheit als Fortschreibungsprozess
- Beschreibung der IT-Infrastruktur als Basiskomponente des IT-Einsatzes

Grundschutzmaßnahmen (Anwender/IT-Personal)

Die Grundschutzmaßnahmen gewährleisten in ihrer Gesamtheit die notwendige Basis für einen verlässlichen IT-Einsatz. Werden diese Maßnahmen nicht eingehalten, ist ein seriöser Umgang mit IT nicht gegeben. Es hat sich als günstig erwiesen, in der Betrachtung die vom IT-Einsatz betroffene Klientel in Anwender (Nutzer) und IT-Personal (Administratoren, Applikationsbetreuer mit weit gehenden Rechten etc.) zu unterscheiden. Insbesondere die Entscheidung, wer in diesem Kontext zu welchen Fragestellungen wie intensiv geschult werden muss bzw. welche Auflagen einhalten muss, wird hierdurch erleichtert. Das IT-Grundschutzhandbuch des BSI enthält Standardsicherheitsmaßnahmen, Umsetzungshinweise und weitere Hilfsmittel für zahlreiche Konstellationen, die typischerweise in IT-Verfahren vorkommen. Die in diesem umfangreichen Katalog enthaltenen Maßnahmen sind geeignet, einen Grundschutz für die Systeme und Prozesse abzusichern. Das Informationsangebot soll einerseits zur zügigen Lösung häufiger Sicherheitsprobleme dienen und andererseits die Erstellung einer Rahmenrichtlinie der IT-Sicherheit vereinfachen.

Schutzbedarfsanalyse und Strukturierung der IT-Verfahren

Eine gute Beschreibung des gesamten IT-Einsatzes an der Hochschule ist das Ziel. Basierend auf der sorgsam modularisierten Erfassung der IT-Verfahren sind die Bewertung des Schutzbedarfs und die damit einhergehende Betrachtung der Risiken seriös machbar. Letztlich resultieren hieraus die anzuwendenden Schutzmaßnahmen, die immer so gut wie nötig und nicht so gut wie möglich ausfallen müssen, wenn IT-Sicherheit Kosten sparend umgesetzt werden muss. Bei der Modularisierung des IT-Einsatzes gibt es einen Spielraum, der sehr stark vom Grad der Zentralisierung bzw. Dezentralisierung abhängt.

Risikoanalyse

Für IT-Verfahren mit höherem Schutzbedarf müssen über die Grundschutz-Sicherheitsmaßnahmen hinaus zusätzliche verfahrensbezogene Maßnahmen erarbeitet werden, die aus entsprechenden Risikoanalysen abgeleitetet werden. In einer Risikoanalyse werden Risiken identifiziert und bewertet. Dabei wird für die möglichen Bedrohungen die Eintrittswahrscheinlichkeit gegen den entstehenden Schaden abgewogen. Die Kombination aus einer hohen Eintrittswahrscheinlichkeit und einem hohen erwarteten Schaden ist das „zu behandelnde Risiko“. Die übrigen Quadranten enthalten die akzeptablen Risiken. Die Überführung des zu behandelnden Risikos in ein akzeptables Risiko (z.B. durch Maßnahmen = Veränderung der Eintrittwahrscheinlichkeit oder Versicherungen = Verringerung der Schadenshöhe) kann in einem Risikomanagementplan festgehalten werden.

Umsetzung im Sicherheitsprozess

Da Verfahren, Informationsverarbeitung (insbesondere die elektronische) und Bedrohungen bzw. Missbrauchmöglichkeiten sich in stetem Wandel befinden, kann die Sicherheit nicht statisch hergestellt werden und bestehen bleiben. Die Gesamtaufgabe muss vielmehr als ein kontinuierlicher Prozess aufgefasst werden, in dem sich die Phasen der Planung, Umsetzung, Überprüfung und Verbesserungen in einen anhaltenden Zyklus ablösen. Diesen Kreislauf bezeichnet man als IT-Sicherheitsprozess (siehe Abschnitt 4.6).

Beschreibung der technischen Infrastruktur

Für die Anteile der IT, die sich technisch oder inhaltlich nicht klar gegen andere IT-Verfahren abgrenzen lassen, weil sie anderen Verfahren als Basis dienen oder den Charakter eines Verkehrswegs für Informationen und Daten jeglicher Art aufweisen (z.B. Firewall, Datennetz), sollen detaillierte Dokumentationen erstellt werden, auf die man sich in der Schutzbedarfsanalyse beispielsweise durch Schnittstellen sowie Erweiterungen oder Ergänzungen beziehen kann.

4.5 Schaffung günstiger Randbedingungen

Kommunikation im Sicherheitsprozess:

Der Austausch bzw. die Weitergabe von sicherheitsrelevanten Informationen, sowohl innerhalb einer Einrichtung als auch zwischen Einrichtungen, ist ein wichtiger Aspekt bei der Realisierung und Gewährleistung der IT-Sicherheit. Durch einen gut organisierten Informationsdienst kann entsprechend schnell vorbeugend (präventiv) bei Sicherheitslücken bzw. reaktiv bei Sicherheitsvorfällen gehandelt werden. Für das Funktionieren dieses Informationsdienstes ist es wichtig, Wege, Zuständigkeiten und Zeitpunkte/-räume bzw. Fristen festzulegen und öffentlich zu dokumentieren. Die strukturierte Beschaffung der notwendigen Information ist Voraussetzung für einen funktionierenden Sicherheitsprozess. Nur dadurch kann die für alle notwendige Transparenz und damit die notwendige Akzeptanz erreicht werden.

Es gibt grundlegende sicherheitsrelevante Informationen, die neben der Tatsache, dass sie in den Grundschutzmaßnahmen Berücksichtigung finden, periodisch verbreitet werden bzw. generell öffentlich einsehbar sein sollen. Diese z.T. längerfristig gültigen und damit grundlegenden Informationen im Sinne von Handlungsleitlinien sind zum Beispiel:

- Informationen zum Umgang mit Passwörtern
- Informationen zum Virenschutz
- Informationen zum sicheren Kommunizieren (z.B. Einsatz vom PGP)
- Sicherheitsregeln für die Nutzung von PCs

Diese Informationen können auf folgenden Wegen verbreitet werden:

- als Flyer für neue Studierende und Mitarbeiter
- auf entsprechenden WWW-Seiten
- durch periodische Schulungen/Workshops für Angehörige der Einrichtung

Eine andere Art von sicherheitsrelevanten Informationen sind solche, die sich schneller ändern, also Material über neue Sicherheitspatches, neue Viren, aktuelle Vorfälle und ähnliches. Für diese sind folgende Informationswege geeignet:

- Mailinglisten
- spezielle WWW-Seiten
- direkte Kommunikation mit dem zuständigen CERT
- periodische Schulungen/Workshops für DV-Organisatoren und Sicherheitsbeauftragte der Bereiche einer Einrichtung

Hierbei sollte versucht werden, diese Informationswege so themenspezifisch wie möglich zu gestalten (z.B. Mailing-Listen für Betriebssysteme unterteilt nach Windows, Unix, Mac OS). So ist eine effektive und überschaubare Informationsweise und Nutzbarkeit gewährleistet. In ergänzendem Material zu diesem Dokument [CAIF] werden Kriterien und Strukturen vorgeschlagen, die bei der Organisation von Meldungsdiensten beachtet werden sollten.

Schulungen

Alle Beteiligten am Sicherheitsprozess haben die Selbstverpflichtung, stetig ihre Kompetenz in Sachen IT-Sicherheit zu erweitern. Hierzu muss in allen Bereichen der Hochschule eine entsprechende Aufgeschlossenheit erreicht werden.

4.6 Fazit: IT-Sicherheit ist ein Prozess

In aller Kürze lässt sich der in den Materialien zu diesem Dokument beschriebene IT-Sicherheitsprozess an einer Hochschule wie folgt skizzieren.

- Die Beschreibung der zu erreichenden Ziele setzt zunächst die Beschäftigung mit der Ausgangssituation voraus. Hier gilt es, sorgsam die Interessen von Forschung, Lehre und Verwaltung abzuwägen.
- Die Institutionalisierung der IT-Sicherheit bedarf der Formulierung einer Ordnung zur IT-Sicherheit.
- Der IT-Sicherheitsprozess wird durch die in der Ordnung benannten Verantwortlichen und weitere Partner betrieben. Es werden für die Hochschule verbindliche Schutzklassen definiert. Die für Anwender und IT-Personal relevanten Grundschutzmaßnahmen werden formuliert und verabschiedet. Jedes IT-Verfahren wird beschrieben und somit hinsichtlich der definierten Schutzklassen untersucht. Reicht der Grundschutz nicht aus, wird zusätzlich eine eingehende Risikoanalyse notwendig.

Im Ergebnis erhält man eine vollständige Beschreibung des gesamten IT-Einsatzes und erlangt damit Kenntnis über alle besonders zu überwachenden Szenarien. Im optimalen Fall werden je nach Detailierungsgrad der IT-Verfahrensbeschreibung gleichzeitig Inventarisierung und mittelfristige Ressourcen-Planung wesentlich erleichtert.

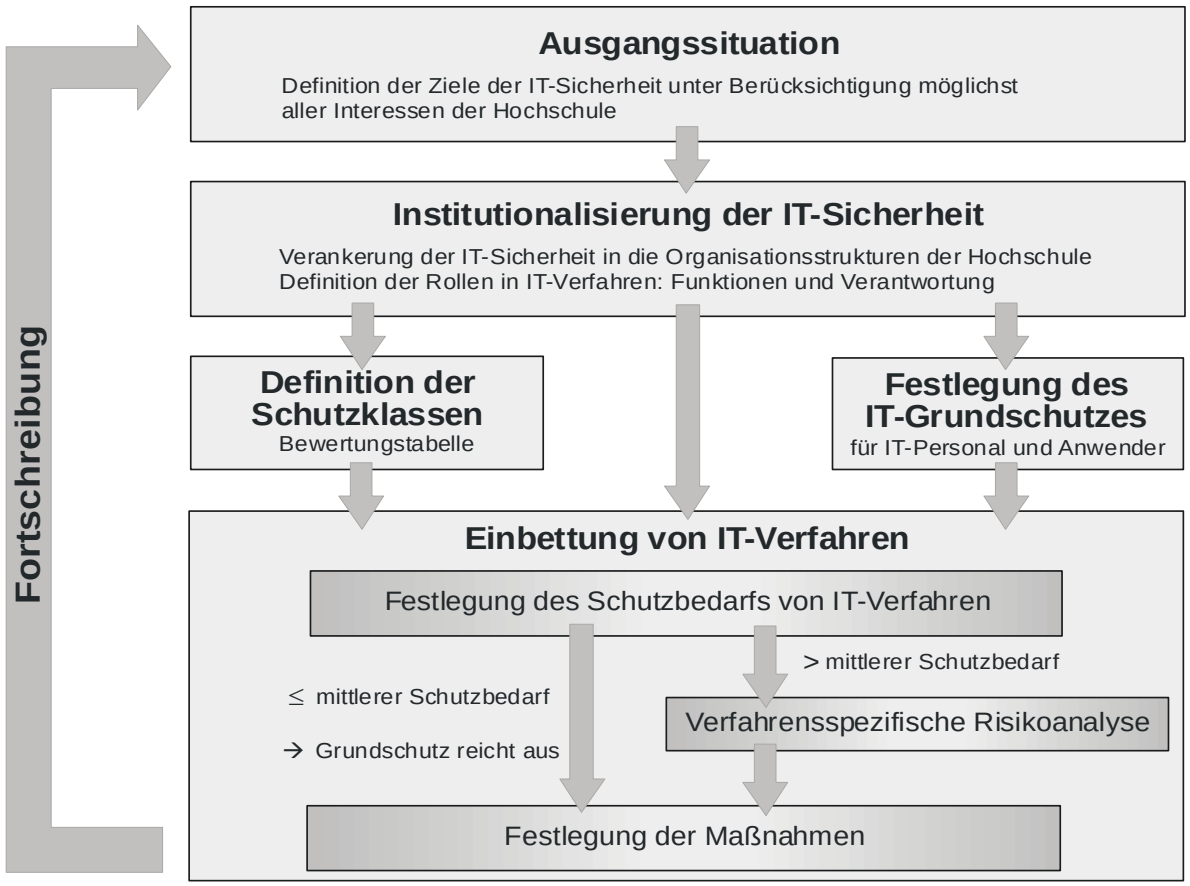

Abbildung 4: Graphische Darstellung des IT-Sicherheitsprozesses

5 Zusammenfassung

Eine funktionierende Informations- und Kommunikationsinfrastruktur ist für jede Hochschule von zentraler Bedeutung. Waren es in der Vergangenheit einige wenige, die sich mit Datenverarbeitung auf den wenigen Rechnern beschäftigt haben, so sind heute weite Teile von Forschung, Lehre und Verwaltung von sicherer und funktionierender Informationstechnologie abhängig und verarbeiten zum Teil sensible Forschungs- und personenbezogenen Daten. Durch die fortschreitende Vernetzung ist heute jeder Arbeitsplatz- oder Poolrechner Bestandteil einer globalen Anlage, die prinzipiell von außen wie von innen angreifbar ist. Neben der rein technischen Verfügbarkeit muss den Sicherheitsaspekten wie Vertraulichkeit, Integrität und Authentizität eine erhöhte Aufmerksamkeit gewidmet werden. Lücken in der IT-Sicherheit verursachen Kosten und schaden dem Ansehen der Hochschule. IT-Sicherheit muss als Gemeinschaftsaufgabe begriffen werden und kann nur im Konsens mit allen Beteiligten erreicht werden. Ohne die notwendige Sensibilisierung für bestehende Sicherheitsrisiken werden viele Nutzer die notwendigen Maßnahmen als einschränkend und unbequem ansehen und die Diskussion wird sich in der Kontroverse zwischen IT-Sicherheit und Freiheit von Forschung und Lehre verlieren.
Die Einführung von Sicherheitsstrukturen erscheint für eine komplexe gewachsene undurchsichtige Struktur wie die einer IT-Landschaft an Hochschulen eine unüberwindbare Hürde. In den vorangegangenen Abschnitten dieses Papiers wurden eine Reihe von überschaubaren Einzelschritten mit klar umrissenen Teilaufgaben aufgezeigt, die eine zügige Umsetzung erlauben.

Die wichtigsten Aufgaben bei der Einführung von IT-Sicherheit sind:

- Definition und Kommunikation des angestrebten Ziels
- Sicherheitsordnung beschließen
- Zuständigkeiten festlegen und in der Hochschulleitung verankern
- Rahmenrichtlinie für die Hochschule erarbeiten und verabschieden
- Bestandsaufnahme der vorhandenen IT-Verfahren

Damit ist dann bereits eine gute Grundlage gegeben für die kontinuierliche Risikoanalyse und die Fortschreibung der sich daraus ergebenden notwendigen Schritte, um die IT-Sicherheit zu garantieren. Für neue Projekte ist der Aspekt der IT-Sicherheit als inhärenter Bestandteil der Projektplanung zu verstehen.

Das vorliegende Papier soll die Wichtigkeit dieses Themas ins Bewusstsein der Leitungsebene von Hochschulen und Rechenzentren rufen und dabei gleichzeitig Lösungswege aufzeigen. Es soll vor Ort die Initiative derer fördern, die in ihrer spezifischen Rolle den Prozess ins Leben rufen und vorantreiben. Dabei steht im Mittelpunkt, dass sich alle Beteiligten gemeinsam den Problemen widmen, denn die vorliegenden Aufgaben können nur übergreifend mit und für die Nutzer der IT gelöst werden.

Danksagung

Der Hauptausschuss des ZKI hat das vorliegende Papier am 26. Aug. 2005 einstimmig zustimmend zur Kenntnis genommen. Allen Kolleginnen und Kollegen (des Arbeitskreises IT-Sicherheit und darüber hinaus) sei an dieser Stelle herzlich für ihr Engagement und die viele Zeit gedankt. Ohne den Fleiß und die Kraft dieser Personen hätte dieses Papier nicht geschrieben werden können.

6 Muster A für eine IT-Sicherheitsordnung

Entwurf einer IT-Sicherheitsordnung

Präambel

Der Betrieb einer Hochschule hängt in hohem Maße von der Qualität seiner IT-Dienstleistungen ab. Das Vertrauen der Benutzer in die Informationstechnik bildet die Grundlage für ihren erfolgreichen Einsatz. Um dieses Vertrauen zu rechtfertigen, muss die Integrität, Vertraulichkeit und Verfügbarkeit der IT-Dienste und Daten sichergestellt sein. Um dieser Verpflichtung angesichts einer wachsenden Bedrohung der sich rasch weiterentwickelnden Technik bei gleichzeitig begrenzter personeller und finanzieller Ausstattung der Hochschulen nachzukommen, müssen sämtliche Einrichtungen der Hochschule den Schutz der Informationstechnik als gemeinsame Herausforderung begreifen. Diese Aufgabe soll auf der Basis einer einheitlichen Rahmenrichtlinie der IT-Sicherheit der Hochschule in einem kontinuierlichen IT-Sicherheitsprozess bewältigt werden.
Conditio sine qua non für den Erfolg ist ein Ausgleich zwischen akademischer Freiheit und IT-Sicherheit.

§1
Gegenstand der Ordnung

Die IT-Sicherheitsordnung bestimmt die für den IT-Sicherheitsprozess erforderliche Organisationsstruktur und definiert Aufgaben und Verantwortlichkeiten.

§2
Geltungsbereich

Die IT-Sicherheitsordnung erstreckt sich auf die gesamte Informationstechnik und sämtliche Benutzer, die diese einsetzen oder bereitstellen und ist damit verbindlich für alle Fakultäten und wissenschaftlichen, zentralen oder sonstigen Einrichtungen der Hochschule.

§3
Beteiligte am IT-Sicherheitsprozess

Die IT-Sicherheitsordnung bestimmt folgende Beteiligte am IT-Sicherheitsprozess:
(1) Leitungsgremium der Hochschule
(2) zentrale IT-Sicherheitsbeauftragte
(3) IT-Sicherheits-Management-Team (SMT)
(4) dezentrale IT-Sicherheitsbeauftragte
(5) Einrichtungen der Hochschule
(6) Rechenzentrum

§4
Einsetzung der IT-Sicherheitsbeauftragten

(1) Die Hochschulleitung setzt einen zentralen IT-Sicherheitsbeauftragten ein.
(2) Jede Fakultät, wissenschaftliche, zentrale und sonstige Einrichtung der Hochschule hat einen dezentralen IT-Sicherheitsbeauftragten und einen Stellvertreter zu benennen.
(3) Ein dezentraler IT-Sicherheitsbeauftragter kann für mehrere Einrichtungen zuständig sein.
(4) Die Berufungen müssen den gesamten Geltungsbereich abdecken, d.h. jedem IT-System und jedem Benutzer ist ein dezentraler IT-Sicherheitsbeauftragter zugeordnet.
(5) Bei der Berufung ist auf personelle Kontinuität zu achten, d.h. die Beteiligten sollten zum hauptamtlichen Personal der Hochschule gehören.

§5
Mitglieder des IT-Sicherheits-Management-Teams

Die IT-Sicherheitsordnung bestimmt folgende Mitglieder des IT-Sicherheits-Management-Teams:
(1) ein Vertreter des Leitungsgremiums der Hochschule
(2) zentrale IT-Sicherheitsbeauftragte
(3) ein Vertreter der dezentralen IT-Sicherheitsbeauftragten
(4) ein Vertreter des Rechenzentrums
(5) Datenschutzbeauftragte

§6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(1) Das IT-Sicherheits-Management-Team bildet für die Hochschule das zentrale Beschluss- und Kontrollorgan in Sachen IT-Sicherheit. Es verfasst und beschließt die einheitliche Rahmenrichtlinie der IT-Sicherheit der Hochschule und erstellt jährlich einen IT-Sicherheitsbericht.
(2) Der zentrale IT-Sicherheitsbeauftragte ist für die Umsetzung der Rahmenrichtlinie der IT-Sicherheit an der Hochschule verantwortlich und wird darin vom IT-Sicherheits-Management-Team unterstützt. Der zentrale IT-Sicherheitsbeauftragte ist in allen sicherheitsrelevanten Fragen Ansprechpartner nach innen und außen. Er dokumentiert sicherheitsrelevante Vorfälle und entwickelt einen Schulungs- und Weiterbildungsplan zur IT-Sicherheit.
(3) Die dezentralen IT-Sicherheitsbeauftragten sind für die Durchführung des IT-Sicherheitsprozesses in ihrer Einrichtung verantwortlich.
(4) Das Rechenzentrum unterstützt die IT-Sicherheitsbeauftragten und das IT-Sicherheits-Management-Team in technischen Fragen.
(5) Die Benennung der dezentralen IT-Sicherheitsbeauftragten entlässt die Leitung der Fakultäten, wissenschaftlichen, zentralen und sonstigen Einrichtungen nicht aus ihrer Verantwortung für die IT-Sicherheit in ihrem Bereich. Sie sind verpflichtet an allen Planungen, Verfahren und Entscheidungen mit Bezug zur IT-Sicherheit den zuständigen dezentralen IT-Sicherheitsbeauftragten und den zentralen IT-Sicherheitsbeauftragten zu beteiligen.
(6) Die am IT-Sicherheitsprozess Beteiligten arbeiten in allen Belangen der IT-Sicherheit zusammen. Bei Bedarf können externe Fachleute beratend hinzugezogen werden.

§7
Verwirklichung des IT-Sicherheitsprozesses

(1) Der zentrale IT-Sicherheitsbeauftragte konzipiert ein hochschulweites Informations- und Kommunikationssystem, über das alle Beteiligte am IT-Sicherheitsprozess in Kontakt stehen.
(2) Die dezentralen IT-Sicherheitsbeauftragten sind verpflichtet sich aktuelle sicherheitsrelevante Informationen zu beschaffen und werden darin vom zentralen IT-Sicherheitsbeauftragten unterstützt. Die dezentralen IT-Sicherheitsbeauftragten veranlassen in ihrem Bereich die erforderlichen IT-Sicherheitsmaßnahmen zur Gefahrenabwehr. Hierzu müssen sie von der Leitung ihrer Einrichtung mit den notwendigen Kompetenzen ausgestattet werden.
(3) Die am IT-Sicherheitsprozess Beteiligten informieren sich gegenseitig unverzüglich, umfassend und vollständig über sicherheitsrelevante Vorfälle. Über jeden Vorfall muss der zentrale IT-Sicherheitsbeauftragte informiert werden.
(4) Der zentrale IT-Sicherheitsbeauftragte darf sämtliche Informationen, die bei der Durchführung des IT-Sicherheitsprozesses in den einzelnen Einrichtungen anfallen, einholen.

(5) Zur kontinuierlichen Weiterentwicklung der Rahmenrichtlinie der IT-Sicherheit soll das IT-Sicherheits-Management-Team regelmäßig tagen. Die Beteiligten am IT-Sicherheitsprozess können hierzu dem IT-Sicherheits-Management-Team Vorschläge unterbreiten.

§8
Gefahrenintervention

(1) Bei einem Verstoß gegen die IT-Sicherheitsordnung oder die einheitliche Rahmenrichtlinie der IT-Sicherheit der Hochschule kann der zentrale IT-Sicherheitsbeauftragte die sofortige, vorübergehende Stillegung des betroffenen IT-Systems anordnen sowie die verantwortlichen Benutzer vorübergehend von der Nutzung der Informationstechnik ausschließen. Der zentrale IT-Sicherheitsbeauftragte muss unverzüglich den zuständigen dezentralen IT-Sicherheitsbeauftragten über den Vorgang informieren.
(2) Bei Gefahr in Verzug kann das Rechenzentrum Netzanschlüsse vorübergehend sperren, wenn anders ein voraussichtlich großer Schaden von der Hochschule nicht abgewendet werden kann. Das Rechenzentrum muss unverzüglich den zentrale IT-Sicherheitsbeauftragten und den zuständigen dezentralen IT-Sicherheitsbeauftragten über den Vorgang informieren.
(3) Die Wiederinbetriebnahme vorübergehend stillgelegter IT-Systeme setzt deren eingehende Überprüfung durch den zuständigen dezentralen IT-Sicherheitsbeauftragten voraus.
(4) Nach Rücksprache mit dem IT-Sicherheits-Management-Team hebt der zentrale IT-Sicherheitsbeauftragte den Ausschluss eines vorübergehend von der Nutzung der Informationstechnik ausgeschlossenen Benutzer wieder auf.
(5) Das IT-Sicherheits-Management-Team bestimmt die IT-Dienste, für die der zentrale IT-Sicherheitsbeauftragte Notfallpläne erstellt. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen und unterteilen sich in einen allgemein zugänglichen Benachrichtigungsplan und in ein detailliertes Notfallkonzept für den Dienstgebrauch.

§9
Finanzierung

Die Hochschule muss den am IT-Sicherheitsprozess Beteiligten ausreichend Mittel zur Verfügung stellen, damit diese ihre Aufgaben unverzüglich, umfassend und vollständig erfüllen können.

§10
Gleichstellungsklausel

Status- und Funktionsbezeichnungen nach dieser Ordnung gelten gleichermaßen in der weiblichen wie in der männlichen Form.

§11
Inkrafttreten

Die IT-Sicherheitsordnung tritt nach ihrer Verabschiedung im Senat am Tag nach ihrer Bekanntmachung in Kraft.

7 Muster B für eine IT-Sicherheitsordnung

Entwurf einer IT-Sicherheitsordnung

Präambel

Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit einer Hochschule auf den Gebieten Lehre und Forschung. Der Hochschulbetrieb erfordert in zunehmenden Maß die Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Informationstechnik (IT) stützen. Dafür ist aber die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten zwingend erforderlich.
Unter diesen Bedingungen kommt der „Sicherheit in der Informationstechnik“ („IT-Sicherheit“) eine grundsätzliche und strategische Bedeutung in der Hochschule zu, die die Entwicklung und Umsetzung einer einheitlichen hochschulweiten Rahmenrichtlinie der IT-Sicherheit für die Hochschule erforderlich macht. Hauptziel der Gestaltung von IT-Sicherheit muss es sein, den entsprechenden Rahmen für das Funktionieren von Lehre und Forschung zu bieten.
Dieses kann wegen der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten und wegen der begrenzten finanziellen und personellen Möglichkeiten nur in einem kontinuierlichen IT-Sicherheitsprozess erfolgen, der den besonderen Bedingungen der Hochschule gerecht wird.

Diese Ordnung regelt die Zuständigkeiten und die Verantwortung sowie die Zusammenarbeit im hochschulweiten IT-Sicherheitsprozess.
Ziel der IT-Sicherheitsordnung ist es nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern primär die in der Hochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen zu schützen sowie die Hochschule soweit möglich vor Imageverlust und finanziellen Schäden zu bewahren.
Die Entwicklung und Fortschreibung des IT-Sicherheitsprozess muss sich einerseits an den gesetzlich festgelegten Aufgaben der Hochschulen sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren, andererseits ist sie nur über einen kontinuierlichen IT-Sicherheitsprozess innerhalb geregelter Verantwortungsstrukturen zu erzielen. Es empfiehlt sich diesen IT-Sicherheitsprozess an Prinzipien zu orientieren, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutzhandbuch niedergelegt sind.

§1
Gegenstand der Ordnung

Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines hochschulweiten IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen, eine grobe Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten. Diese Ordnung wird ergänzt durch die separaten Ordnungen für die Benutzung der IT-Infrastrukturen der Hochschule.

§2
Geltungsbereich

Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Einrichtungen der Hochschule (Fachbereiche, wissenschaftliche Einrichtungen, zentrale Einrichtungen und sonstige Einrichtungen), auf die gesamte IT-Infrastruktur der Hochschule, einschließlich der daran betriebenen IT-Systeme sowie der Gesamtheit der Benutzer.

§3
Beteiligte am IT-Sicherheitsprozess

Die Hauptverantwortung für den IT-Sicherheitsprozess liegt bei der Hochschulleitung. Sie setzt daher folgende Gremien und Funktionsträger ein und bindet bestehende Einrichtungen in den IT-Sicherheitsprozess ein:

(1) IT-Sicherheitsmanagement-Team (SMT)
(2) Dezentrale IT-Sicherheitsbeauftragte
(3) Hochschulrechenzentrum
(4) Einrichtungen der Hochschule

§4
Einsetzung der Beteiligten

(1) Die Hochschulleitung setzt ein IT-Sicherheitsmanagement-Team (SMT) ein. Die Zusammensetzung des SMT sollte – unter Beschränkung der Anzahl der Mitglieder auf das notwendige Maß – sowohl die unterschiedlichen Aufgabenbereiche der Hochschule widerspiegeln als auch die unterschiedlichen, für die Hochschule relevanten Aspekte der IT-Sicherheit berücksichtigen.
Ständige Mitglieder des SMT sind:
- ein Vertreter der Hochschulleitung,
- der Datenschutzbeauftragte,
- ein Vertreter der dezentralen IT-Sicherheitsbeauftragten (siehe Abs. (3)),
- ein Vertreter des Hochschulrechenzentrums,
- ein Vertreter der IT-Senatskommission.

Weitere sachverständige Mitglieder werden in Abstimmung mit den Hochschulgremien von der Hochschulleitung benannt.
(2) Das SMT wählt aus dem Kreis der ständigen Mitglieder einen Vorsitzenden.
(3) Das SMT kann zur Unterstützung seiner Arbeit im operativen Bereich eine Arbeitsgruppe einsetzen. Bei Bedarf sollte es den Rat von Experten einholen (z.B. Juristen, Spezialisten für Teilbereiche der IT-Sicherheit).
(4) Jeder Fachbereich und jede Einrichtung der Hochschule hat einen dezentralen IT-Sicherheitsbeauftragten und einen Stellvertreter zu bestellen. Es kann aber auch ein dezentraler IT-Sicherheitsbeauftragter für mehrere Einrichtungen zuständig sein. Durch die Benennung müssen alle IT-Systeme im Geltungsbereich sowie die für den Betrieb vor Ort verantwortlichen Personen einem IT-Sicherheitsbeauftragten zugeordnet sein.
(5) Bei der Bestellung/Benennung der im IT-Sicherheitsprozess aktiven Personen soll die erforderliche personelle Kontinuität berücksichtigt werden. Deshalb sollen die IT-Sicherheitsbeauftragten über langfristige Verträge verfügen oder möglichst zum hauptamtlichen Personal der Hochschule gehören.
(6) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leitung der Einrichtungen nicht von ihrer Gesamtverantwortung für die IT-Sicherheit in ihrem Zuständigkeitsbereich.

§5
Aufgaben der Beteiligten

(1) Das SMT ist für die Richtlinienerstellung, Forschreibung, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich. Unter anderem ist dabei das Erarbeiten von Notfallplänen zu berücksichtigen.
(2) Das SMT gibt die hochschulinternen technischen Standards zur IT-Sicherheit vor. Außerdem veranlasst es die Schulung und Weiterbildung der dezentralen IT-Sicherheitsbeauftragten und die Unterstützung bei der Richtlinienumsetzung.
(3) Das SMT dokumentiert sicherheitsrelevante Vorfälle und erstellt jährlich einen IT-Sicherheitsbericht.

(4) Der Vorsitzende des SMT berät die Hochschulleitung in relevanten Fragen der IT-Sicherheit.
(5) Die dezentralen IT-Sicherheitsbeauftragten sind für die Umsetzung aller mit dem SMT abgestimmten Sicherheitsbelange bei den IT-Systeme und -Anwendungen sowie den Mitarbeitern in ihren Verantwortungsbereichen verantwortlich. Sie sind verpflichtet sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf einem aktuellen Stand zu halten.
(6) Das Hochschulrechenzentrum ist für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit verantwortlich. Es arbeitet eng mit dem SMT zusammen.
(7) Die Einrichtungen der Hochschule sind verpflichtet, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zu IT-Sicherheit die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten sowie das SMT zu beteiligen.
(8) Die am IT-Sicherheitsprozess Beteiligten arbeiten in allen Belangen der IT-Sicherheit zusammen, stellen die dazu erforderlichen Informationen bereit und regeln die Kommunikations- und Entscheidungswege sowohl untereinander wie auch in Beziehung zu Dritten. Hierbei ist insbesondere der Aspekt der in Krisensituationen gebotenen Eile zu berücksichtigen.

§6
Umsetzung des IT-Sicherheitsprozesses

(1) Das SMT initiiert, steuert und kontrolliert die Umsetzung des IT-Sicherheitsprozesses, der nach festzulegenden Prioritäten technische und organisatorische Maßnahme sowohl präventiver als auch reaktiver Art sowie Maßnahmen zur schnellen Krisenintervention umfassen muss.
(2) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Zuständigkeitsbereich verantwortlich. Dafür müssen sie vom SMT und der Leitung der jeweiligen Einrichtung mit entsprechenden Kompetenzen ausgestattet werden. Sie informieren regelmäßig sowohl die Leitung ihrer Einrichtung als auch das SMT über den Stand der Umsetzung und über aktuelle Problemfälle.
(3) Es sind Notfallpläne zu erarbeiten, die Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse beinhalten sollen, mit dem Ziel, Gefahren soweit möglich abzuwenden sowie eine möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen zu erreichen.
(4) Das SMT setzt einen Arbeitskreis ein, der primär als Basis dienen soll, um die Umsetzung des IT-Sicherheitsprozesses hochschulweit abzustimmen und Erfahrungen auszutauschen.
(5) Auf der Grundlage der Benutzungsordnung sind alle Angehörigen und Mitarbeiter der Hochschule zur Meldung sicherheitsrelevanter Ereignisse verpflichtet.

§7
Krisenintervention

(1) Bei Gefahr im Verzuge veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige vorübergehende Stilllegung betroffener IT-Systeme in ihrem Zuständigkeitsbereich, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist. Das SMT ist unverzüglich zu informieren.
(2) Soweit das Hochschulrechenzentrum Gefahr im Verzuge feststellt, kann es Netzanschlüsse (ggf. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur der Hochschule in Teilen oder insgesamt nicht anders abzuwenden ist. Der zuständige dezentrale IT-Sicherheitsbeauftragte sowie das SMT werden unverzüglich ggf. nachträglich informiert.

(3) Die Wiederinbetriebnahme erfolgt erst nach der Durchführung hinreichender IT-Sicherheitsmaßnahmen in Abstimmung mit dem SMT.

§8
Finanzierung

(1) Die personellen und finanziellen Ressourcen für alle erforderlichen IT-Sicherheitsmaßnahmen in einer Einrichtung der Hochschule sind von der betreffenden Einrichtung zu erbringen. Darunter fallen auch die Schulungskosten für den/die dezentralen IT-Sicherheitsbeauftragten sowie die Benutzer der Einrichtung.
(2) Die personellen und finanziellen Ressourcen aller zentralen IT-Sicherheitsmaßnahmen sind aus zentralen Ansätzen zu finanzieren.

§9
Gleichstellungsklausel

Status- und Funktionsbezeichnungen nach dieser Ordnung gelten gleichermaßen in der weiblichen wie in der männlichen Form.

§10
In-Kraft-Treten

Diese Ordnung tritt nach ihrer Verabschiedung im Senat am Tag nach ihrer Bekanntmachung in Kraft.

8 Anhang A: Literatur, Quellen und weiterführende Information

8.1 Ergänzendes Material zu diesem Dokument

Dieses Dokument wird gemeinsam mit den folgenden, z.T. eigenständigen Dokumenten verbreitet. Zum einen wurde versucht, die Textlänge in einem überschaubaren Rahmen zu halten, zum anderen wird im Text direkt auf diese Dokumente Bezug genommen, so dass es angemessen erschien, die Dokumente zu einem Gesamtwerk zu bündeln. Die jeweils aktuelle Zusammenstellung wird über den ZKI Server verbreitet: http://www.zki.de/ak_itsi/it-sicherheit_an_hochschulen.html

Auszug aus der Rahmenrichtlinie der Freien Universität zu Berlin

- [RRL] ITSi_Rahmenrichtlinie.pdf

Rechtlicher Rahmen der IT-Sicherheit

- [Recht] ITSi_RechtlicherRahmen.pdf

Strukturierung von Sicherheitsmeldungen durch das Common Announcement Interchange Format (CAIF) Verfahren des RUS-CERT

- [CAIF] ITSi_CAIF.pdf

Verfahren des RUS-CERT zur Erstellung einer Whitelist zum Schutz abgegrenzter IT-Verbünde

- [WL] ITSi_WhiteList.pdf

8.2 Allgemeine Literatur und Quellen

Im Text wurde auf weitere Dokumente direkt oder indirekt Bezug genommen, auf die der interessierte Leser verwiesen sein möge.

[BP] Beispiele für „best practices“

- Kapitel 7 „Wichtige Sicherheitsmaßnahmen“ des BSI-Leitfadens (http://www.bsi.bund.de/gshb/Leitfaden/index.htm)
- DTI-Best-Practice-Guide (http://reporting.dti.gov.uk/cgi-bin/rr.cgi/http://www.dti.gov.uk/bestpractice/assets/security/intro-to-info.pdf)
- FIRST best practice guide library (BPGL) http://www.first.org/resources/guides/
- Site Security Handbook, RFC 2196: http://rfc.net/rfc2196.html
- Users' Security Handbook, RFC 2504: http://rfc.net/rfc2504.html
- Securing Desktop Workstations: http://www.cert.org/security-improvement/modules/m04.html
- Securing Network Servers: http://www.cert.org/security-improvement/modules/m07.html
- Application Security Assessments, http://www.technicalinfo.net/papers/ApplicationSecurityAssessments.html

CERT-Statistics

- http://www.cert.org/stats/cert_stats.html

DFN-CERT – Computer Notfall Team für das Deutsche Forschungsnetz und seine Dienste

- http://www.cert.dfn.de/dfncert/info.html

DFN – Checkliste „IT-Sicherheit“ für die Leitungsebene von Hochschulen und öffentlich geförderten Forschungseinrichtungen vom Juni 2005

- [DFNCL] http://www.dfn.de/sicherheit/checkliste

IT-Grundschutzhandbuch

- [GSHB] Bundesamt für Sicherheit in der Informationstechnik: http://www.bsi.de/gshb/deutsch/menue.htm

Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

- Datenschutzbeauftragte des Bundes und der Länder, September 1998: http://www.lfd.nrw.de/pressestelle/presse_7_zusammensetzen.html

Positionspapier des ARNW und des BSI zur Förderung der IT-Sicherheit an Hochschulen

- [PosP] http://www.wiwi.uni-muenster.de/bdv/sicherheit/bsi_hochschulen.pdf

Regelungen zur IT-Sicherheit

- Arbeitskreis der Leiter Wissenschaftlicher Rechenzentren in NRW (ARNW), W. A. Franck, Aachen; W. Held, Münster; J. W. Münch, Siegen; St. Ost, Münster; B. Wojcieszynski, Bochum; H. Ziegler, Dortmund 21. Februar 2002: http://www.uni-muenster.de/Rektorat/abuni/ab020507.htm
- Sicherheit im Belwue: siehe http://www.belwue.de/security/
    - insbesondere http://www.belwue.de/security/sicherheitskonzept.pdf

Sicherheitsüberlegungen für Endsysteme – Empfohlene Vorgehensweisen zur Unternehmenssicherheit

- Dodds, Kerby und Howard: http://www.microsoft.com/technet/Security/bestprac/bpent/sec3/datavail.mspx

Sicherheitsvorfälle im Internet, Beobachtungen des DFN-CERT

- Vortrag im Rahmen der Informationsveranstaltung: Bekämpfung der Kriminalität im Internet, 15. –16. Februar 2000, BKA Wiesbaden: http://www.bka.de/vorbeugung/agenda98/

9 Anhang B: Glossar

Angriff (engl. attack)	Versuchte oder gelungene vorsätzliche Gefährdung oder Verletzung der Grundwerte der IT-Sicherheit durch Ausnutzung einer Schwachstelle eines IT-Systems. Der Erfolg eines Angriffs ist abhängig von seiner Stärke und Art, sowie der Wirksamkeit bestehender Schutzmaßnahmen beim angegriffenen IT-System.
ARNW (Arbeitskreis der Leiter von Rechenzentren an wissenschaftlichen Hochschulen des Landes NRW)	Kooperationsverbund von 14 Rechenzentren nordrheinwestfälischer Hochschulen
Authentizität (engl. authenticity)	kennzeichnet einen Zustand, in dem Daten jederzeit ihrem Ursprung zugeordnet werden können und die Identität von Personen und IT-Systemen nachvollzogen werden kann.
Backup (Datensicherung)	Erstellung und sichere Aufbewahrung von Sicherungskopien vorhandener Datenbestände, um diese vor Datenverlust zu schützen und die ständige Verfügbarkeit sicherzustellen.
Bedrohungen (engl. threats)	Mögliche Aktivitäten oder Ereignisse, die die IT-Sicherheit eines Systems gefährden, so dass ein Schaden entstehen kann.
Benutzer	→ Nutzer
Benutzungsordnung	Die Benutzungsordnung bestimmt die für die Benutzung der Informationstechnik verbindlichen Verhaltensregeln und definiert Rechte und Pflichten der Benutzer und Betreiber.
Betreiber	Natürliche oder juristische Personen, die die IT-Infrastruktur für Nutzungen bedarfsgerecht bereitstellen und alle administrativen Aufgaben im laufenden Betrieb wahrnehmen.
Bot	abgeleitet von robot (engl. = Roboter), Bezeichnung für ein Computerprogramm welches weitgehend selbstständig bestimmte oft zu wiederholende Aufgaben ausführt. Bots stellen ein Sicherheitsproblem dar, wenn sie in Form von Trojanern fremde Rechner infizieren, um diese mittels Fernsteuerung vom Nutzer möglichst unbemerkt bestimmte Befehle auszuführen zu lassen.
Botnet	fernsteuerbarer Zusammenschluss einer großen Anzahl von mit Bots infizierten Rechnern, die häufig für die Spam-Verbereitung und DDoS-Attacken missbraucht werden.
BSI (Bundesamt für Sicherheit in der Informationstechnik)	1991 gegründete Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern und Sitz in Bonn , die als unabhängige und neutrale Stelle für Fragen der IT-Sicherheit in der Informationsgesellschaft zuständig ist.
CAIF (Common Announcement Interchange Format)	Vom RUS-CERT entwickelte und zum anerkannten Standard avancierte Struktur von Sicherheitsmeldungen, die sich überwiegend auf bekannte Angriffe oder offene Sicherheitslücken beziehen.
CERT (Computer Emergency Response Team)	Computer-Notfall-Team welches einen Kreis von Anwendern oder Organisationen bei derVerhinderung und der Behandlung von Vorfällen im Bereich Rechner- und Netzwerksicherheit unterstützt. Schwerpunkte sind die Analyse von Sicherheitslücken und die Vorfallsbearbeitung, sowie die Herausgabe von Warnungen und die Beantwortung von Anfragen. CERTs sind weltweit verteilt aufgestellt.
Cracker	Personen, die versuchen oder denen es gelingt sich unautorisierten Zugang zu IT-Systemen zu verschaffen, bestehende Schutzmaßnahmen von urheberrechtlich geschützten Werken zu umgehen oder fremde Daten zu beschädigen. Sie verfolgen destruktive Ziele, wie die unberechtigte Erlangung persönlicher Vorteile oder die Schädigung des betroffenen IT-Systems oder einer Institution. Anstelle des Begriffs Cracker wird häufig fälschlicherweise der Begriff Hacker verwendet.
Datenschutz	Gesamtheit der Standards der gesetzlichen und betrieblichen Regelungen zum Schutz des Einzelnen vor einer Beeinträchtigung in seinem Persönlichkeitsrecht durch den Umgang mit seinen personenbezogenen Daten.

(behördlicher) Datenschutzbeauftragter	Eine gemäß gesetzlicher Grundlage von der Hochschulleitung bestellte Person, die für den gesetzeskonformen Umgang mit personenbezogenen Daten, für die Beratung in allen Belangen des Datenschutzes und jederzeitige auch unangemeldete Kontrollen der Einhaltung des Bundesdatenschutzgesetzes (BDSG) sowie weiterer Rechtsvorschriften für den Datenschutz in der Hochschule verantwortlich ist.
DV (Datenverarbeitung)	Gesamtheit der Prozesse zur Erhebung, Erfassung, Aufbereitung, Nutzung, Speicherung, Übermittlung, programmgesteuerten Verarbeitung, internen Darstellung, Ausgabe und Wiedergewinnung von Daten die typischerweise von IT-Systemen durchgeführt werden.
Denial-of-Service (DoS) Distributed-Denial-of-Service (DDoS)	Angriff mit dem Ziel die Verfügbarkeit eines IT-Systems und/oder bestimmter Dienste erheblich einzuschränken. (Denial of Service = außer Betrieb setzen) Ziel ist es das angegriffene IT-System durch ein Überhäufen mit IP-Paketen oder Anfragen (flooding genannt) so stark auszulasten, bis es abstürzt oder es so zu überlasten, dass es seine eigentlichen Funktionalitäten nicht mehr in geforderter Art und Weise erbringen kann. Um eine Effizienzsteigerung zu erzielen, werden beim so genannten „Distributed Denial of Service“ (DDoS)-Angriff eine Vielzahl von IT-Systemen koordiniert zum Einsatz gebracht.
Deutsches Forschungsnetz (DFN)	von der Wissenschaft selbst verwaltetes Hochleistungsnetz für Wissenschaft und Forschung in Deutschland, welches Hochschulen und Forschungseinrichtungen miteinander verbindet.
DFN-Verein	→ Verein zur Förderung eines Deutschen Forschungsnetzes.
Firewall	Schutzsystem am Übergang zwischen zwei (Teil-)Netzen, das den Datenfluss zwischen diesen (Teil-)Netzen (häufig zwischen einem LAN und dem Internet) kontrolliert gemäß festgelegten Regeln gestattet, einschränkt oder verwehrt. Ziel ist es, Gefahren von Angriffen aus dem als unsicher anzusehenden Internet gegen das eigene zu schützende LAN zu minimieren oder die Weitergabe von sicherheitsrelevanten Informationen aus dem eigenen LAN zu verhindern.
IT- Grundschutzhandbuch (IT-GSHB, GSHB)	Vom BSI herausgegebenes umfangreiches Dokument, dass als De-facto-Standard für die Implementierung und Überprüfung der IT-Sicherheit in einem Unternehmen oder einer Behörde in Deutschland angesehen wird und auch international anerkannt ist. Es beschreibt detailliert Standard-Sicherheitsmaßnahmen für IT-Systeme, gibt Hinweise zur Lösung von Sicherheitsproblemen und der Anhebung der Sicherheitsniveaus, sowie Hilfestellung bei der Erstellung von IT-Sicherheitskonzepten. Es wird halbjährlich fortgeschrieben. Vgl.: http://www.it-grundschutzhandbuch.de/.
Grundwerte der IT-Sicherheit	Kennzeichnung der Hauptziele der IT-Sicherheit an der Hochschule. Durch das BSI werden als Grundwerte der IT-Sicherheit Vertraulichkeit, Verfügbarkeit und Integrität benannt. Diese können im eigenen Bereich um weitere grundlegende Ziele ergänzt werden.
Hacker	Personen mit hohem Fachwissen im IT-Bereich und umfassenden Programmierkenntnissen. Auch sie versuchen in IT-Systeme einzudringen. Im Gegensatz zu Crackern ist das Ziel nicht die bewusste Schädigung, sondern zum Beispiel Neugier, der Reiz Schutzsysteme zu überwinden, das Aufdecken von Sicherheitslücken oder die Erlangung von ihrer Meinung nach zu Unrecht geheim gehaltenen Informationen. Hacker fühlen sich der so genannten Hackerethik, die die Motive und Grenzen ihrer Aktionen fixiert, verpflichtet. (Vgl.: Chaos Computer Club: http://www.ccc.de/hackerethics?language=de) Der Begriff Hacker wird fälschlicherweise oft anstelle von Cracker verwendet.
IT-Infrastruktur	Baulich-technische Gegebenheiten von Gebäuden, Räumen und Schutzschränken, die für den IT-Einsatz verwendet werden.[7]
Integrität (engl. integrity)	kennzeichnet einen manipulationsfreien Zustand von Daten und/oder IT-Systemen.
IT (Informationstechnik)	Gesamtheit der technischen Mittel zur Erhebung, Erfassung, Aufbereitung, Nutzung, Speicherung, Übermittlung, programmgesteuerten Verarbeitung,

[7] BSI Schulung IT-Grundschutz

	internen Darstellung, Ausgabe und Wiedergewinnung von Daten.
IT-Prozess	Folge von zueinander in Beziehung stehenden Aktivitäten die IT gestützt, parallel oder aufeinander folgend abgearbeitet werden um ein Ziel zu erreichen.
IT-Sicherheits-Management-Team	→ SMT
IT-System	Funktionelle Einheit aus Hard- und Software, die Daten erhebt, erfasst, aufbereitet, nutzt, speichert, übermittelt, programmgesteuert verarbeitet, intern darstellt, ausgibt und wiedergewinnt.
IT-Verfahren	Es besteht aus Arbeitsabläufen und -prozessen, die sich auf IT stützen und eine arbeitsorganisatorisch abgeschlossene Einheit bilden.
kompromittieren	Verletzen der Vertraulichkeit bei einem IT-System in Folge eines Angriffs bzw. unbeabsichtigte oder unautorisierte Offenlegung eines geheimen Schlüssels oder verschlüsselter Daten.
Konsistenz (engl. consistency)	kennzeichnet einen Zustand, in dem sichere Subsysteme ein sicheres Gesamtsystem ergeben.
KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)	Das seit 1998 rechtskräftige Gesetz verpflichtet Aktiengesellschaften zur Durchführung eines angemessenen Risikomanagements, was die Pflicht der Geschäftsführung beinhaltet alle relevanten Schwachstellen, die bedrohlich für ein Unternehmen werden könnten, transparent zu machen. Nach herrschender Meinung gilt das Gesetz auch für große GmbHs.
MDStV	Mediendienste-Staatsvertrag http://www.internetrecht-rostock.de/Gesetze/MDStV-Neu.htm
(IT-Sicherheits-)Meldungen (engl. (security) announcements)	Strukturierte Informationen zu entdeckten Schwachstellen mit Problembeschreibungen und Lösungsmöglichkeiten.
Netzagentur NRW	Die Netzagentur NRW ist eine Projektgruppe im Auftrag der Hochschulen des Landes NRW die mit der Bearbeitung landesweiter Aufgaben im Bereich der Netze betraut ist.
Nutzer (engl. user)	Natürliche Person, die als Angehöriger oder Gast der Hochschule berechtigt IT verwendet.
Nutzungsordnung	→ Benutzungsordnung
Passwort (engl. password)	Geheime Zeichenfolge die unerlaubten Zugriff auf Daten, Dienste und IT-Systeme verhindern soll. Die Güte des Passwortes ist abhängig vom Grad der Geheimhaltung, der Länge und dem gewählten Zeichenvorrat.
Patch	Datei, die dazu dient identifizierte Fehler in einem installierten Programm zu beheben. Häufig werden mit Patches Sicherheitslücken in bereits veröffentlichter Software geschlossen.
PGP (Pretty Good Privacy, dt. recht gute Geheimhaltung/ Privatsphäre)	Programm zur Verschlüsselung von E-Mails und Daten (Sicherung der Vertraulichkeit), dass mit dem Public-Key-Verfahren arbeitet. Zusätzlich können Dokumente mit einer digitalen Signatur versehen werden (Wahrung der Authentizität und Integrität).
Phishing	Wortschöpfung aus den Wörtern „password“ und „fishing“ die sinngemäß „nach Passwörtern fischen“ bedeutet. Mit gefälschten E-Mails und Webseiten werden Nutzer getäuscht und zur Preisgabe von vertraulichen und sensiblen Daten veranlasst, die dann missbraucht werden können.
Public-Key-Verfahren	Krytografisches Verfahren bei dem für die Verschlüsselung ein anderer Schlüssel als zur Entschlüsselung verwendet wird. Zum Einsatz kommt ein Schlüsselpaar, was jeweils aus einem geheimen (private key) und einem öffentlichen Schlüssel (public key), der allgemein bekannt bzw. zugänglich ist, besteht. Der geheime Schlüssel darf sich praktisch nicht aus dem öffentlichen Schlüssel ableiten lassen.
Rahmenrichtlinie der IT-Sicherheit (engl. standards)	zentrales Dokument im IT-Sicherheitsprozess der Hochschule, in dem die Aussagen und Forderungen der IT-Sicherheitsordnung durch die verantwortlichen Gremien und Personen konkretisiert werden. Sie enthält die Vorgaben, die die Umsetzung der IT-Sicherheitsziele der Hochschule sicherstellen sollen. Mit ihrem übergeordneten Charakter betrifft sie alle IT-Verfahren der Hochschule.
Risiko	Maß für die Gefährdung und das Ausmaß der möglichen Schädigung eines IT-Systems durch das Zusammentreffen einer Bedrohung und einer vorhandenen Schwachstelle.
Risikoanalyse (engl. risk	Untersuchung der Eintrittswahrscheinlichkeit eines schädigenden Ereignisses

assessment Analysis)	und der daraus resultierenden potentiellen Schadensausmaßes.
Schutzbedarf	Maß für die Bedeutung bzw. den Wert, den die zu schützenden Daten oder IT-Systeme für die Hochschule besitzen. Aus wirtschaftlicher Perspektive sollte der Aufwand für Schutzmaßnahmen mit dem Wert der Daten und IT-Systeme korrespondieren. Als Schutzbedarfskategorien werden üblicherweise niedrig bis mittel, hoch und sehr hoch verwendet. Die Tabelle aus dem Beispiel für eine Rahmenrichtlinie definiert diese Kategorien in Relation zur Bedrohung der Grundwerte und des möglichen Schadens.
Schwachstelle/ Verwund-barkeit/ Sicherheitslücke (engl. vulnerability)	Sicherheitsrelevante Eigenschaft eines IT-Systems oder eines seiner Bestandteile, die das Wirksamwerden einer Bedrohung ermöglicht.
IT-Sicherheit/ Sicherheit in der Informationstechnik	Zustand oder Ziel eines IT-Systems oder der Gesamtheit der IT-Infrastruktur der Hochschule , bei dem die implementierten IT-Sicherheitsmaßnahmen gewährleisten, dass die Grundwerte der IT-Sicherheit entsprechend der Vorgaben der Hochschulleitung und bestehender rechtlicher Auflagen gewahrt werden und die potentiellen Bedrohungen nur so wirksam werden können, dass die verbleibenden Risiken tragbar sind.
IT-Sicherheitsbeauftragter – zentral/ dezentral (ITSiBe)	Mitarbeiter der Hochschule, mit eigener Fachkompetenz zur IT-Sicherheit, der im Auftrag der Hochschulleitung für alle IT-Sicherheitsfragen zuständig ist, aktiv im IT-Sicherheitsprozess und dem SMT mitwirkt, Richtlinien im Bereich der IT-Sicherheit koordinierend erstellt und deren Umsetzung plant und überprüft. Neben dem zentralen IT-Sicherheitsbeauftragten werden für die Fachbereiche und Einrichtungen der Hochschule dezentrale IT-Sicherheitsbeauftragte eingesetzt. Die IT-Sicherheitsbeauftragten sind für die Umsetzung aller mit dem SMT abgestimmten Sicherheitsbelange bei den IT-Systeme und -Anwendungen sowie den Mitarbeitern in ihren Verantwortungsbereichen verantwortlich.
IT-Sicherheitsmaßnahme(engl. guideline)	Technische, organisatorische, personelle und rechtliche Handlung, die durchgeführt wird um die Grundwerte der IT-Sicherheit zu sichern und die Erreichung des angestrebten IT-Sicherheitsniveaus zu gewährleisten.
IT-Sicherheitsniveau	Zielwert für das angestrebte Maß an IT-Sicherheit an einer Hochschule
IT-Sicherheitsordnung/ IT-Sicherheitsleitlinie (engl. security policy)	Im Sinne offizieller Vorgaben von der Hochschule in Kraft gesetzte grundsätzliche Regelung zur IT-Sicherheit an der Hochschule. Die IT-Sicherheitsordnung bestimmt die für den IT-Sicherheitsprozess erforderliche Organisationsstruktur und definiert Aufgaben, Verantwortlichkeiten und Zuständigkeiten.
IT-Sicherheitsprozess	Geplantes und organisiertes Vorgehen zur Durchsetzung und Aufrechterhaltung des angestrebten IT-Sicherheitsniveaus. Der IT-Sicherheitsprozess wird durch das SMT initiiert und gesteuert. Die empfohlene Vorgehensweise für die Etablierung eines funktionierenden IT-Sicherheitsprozesses ist in Abschnitt 4.6 beschrieben.
SMT (Sicherheits-Management-Team)	Aus mehreren Personen gebildetes Strukturelement der IT-Sicherheits-organisation an der Hochschule. Das SMT ist für die Richtlinienerstellung, Fortschreibung, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.
Spam/ Junk-Mail	Bezeichnung für unverlangte und unerwünschte Werbe- oder Massenmails, sowie inhaltslose oder massenhaft verbreitete Postings in Internetforen.
TDG	Gesetz über die Nutzung von Telediensten (Artikel 1 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste) http://bundesrecht.juris.de/bundesrecht/tdg/index.html
TDDSG	Gesetz über den Datenschutz bei Telediensten (Artikel 2 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste) http://bundesrecht.juris.de/bundesrecht/tddsg/index.html
TKG	Telekommunikationsgesetz http://bundesrecht.juris.de/bundesrecht/tkg_2004/index.html
Trojanisches Pferd/ Trojaner	Schadprogramm, das in der Regel als verborgene Funktion in einem Anwendungsprogramm häufig vom Nutzer unbewusst in das IT-System eingebracht wird. Das Trojanische Pferd wird mit dem Start der eigentlichen Anwendung aktiviert und führt meist schädigende Aktionen aus, wie das

	Ausspionieren persönlicher Daten und die Öffnung einer Schwachstelle oder Hintertür im System.
Verbindlichkeit (engl. liability)	charakterisiert einen Zustand, in dem die Durchführung einer Handlung mittels eines IT-Systems durch die agierende Instanz im Nachhinein nicht abgestritten werden kann.
Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein)	Betreiber des DFN. Stellt seine Weiterentwicklung und Betrieb sicher.
Verfügbarkeit (engl. availability)	kennzeichnet einen Zustand, in dem Daten, Dienste und Funktionen eines IT-Systems und seiner Komponenten von den berechtigten Personen zum geforderten Zeitpunkt, in der vorgesehenen Zeit und in zugesicherter Form und Qualität nutzbar sind.
Vermeidung von Missbrauch	Durchsetzung des Rechtes der Betreiber und/ oder Nutzer die eigenen IT Systeme nur für den vorgesehenen Zweck zu gebrauchen.
Verschlüsselung/ Chiffrierung (engl. encryption)	Bezeichnung für den Vorgang, bei dem aus einem Klartext durch Einsatz eines Verschlüsselungsalgorithmus und unter Zuhilfenahme eines Schlüssels ein Geheimtext (Chiffretext) generiert wird. Der umgekehrte Vorgang wird Entschlüsselung genannt.
Vertraulichkeit (engl. confidentiality)	kennzeichnet einen Zustand, in dem eine Informationsgewinnung aus sensiblen Daten nur berechtigten Personen und in der zulässigen Weise möglich ist.
Virus	Nichtselbstständige Programmroutine, die ursprünglich durch einen Nutzer gestartet wurde, mit der Fähigkeit sich selber zu vervielfältigen und so andere IT-Systeme oder Netzwerke zu infizieren. Viren enthalten häufig Schadfunktionen.
Visual Spoofing	Im Zusammenhang mit Phishing verwendete Technik, bei der dem potentiellen Opfer die imitierte Oberfläche seines Standard-Web-Browsers mit allen Sicherheitsfeatures untergeschoben wird, so dass dieser sich in seiner gesicherten, vertrauten Umgebung wähnt und vertrauliche Informationen preisgibt. Schutz vor dieser Angriffsform bietet eine Personalisierung der Oberfläche des genutzten Web-Browsers.
Whitelist	Filterliste, die als restriktive Postivliste (Erlaubnisliste) die vollständige Aufzählung aller zulässigen Bedingungen enthält und nach dem Prinzip arbeitet, dass alles was nicht explizit erlaubt ist, verboten ist. Whitelists können u.a. bei Firewalls und Spam-Filtern eingesetzt werden.
Wurm	Vollständiges, lauffähiges Programm, das sich selbstständig (ohne Nutzeraktion) vervielfältigen kann und sich in IT-Systemen und vor allem in Netzen ausbreitet. Würmer enthalten häufig Schadfunktionen.
ZKI (Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V.)	Verein, in dem die Leiter der wissenschaftlichen Rechenzentren der Hochschulen und Forschungseinrichtungen Deutschlands organisiert sind.