

Konzept zur Sicherheit von IT-Systemen und Daten

Teil Lehre und Forschung

(Sicherheitskonzept der Hochschule Anhalt)

Das Konzept wurde von verschiedenen Arbeitsgruppen der DV-Kommission unter Einbeziehung von Fachkräften aus den Fachbereichen der Hochschule entworfen.

Inhalt

- 1 Vorbemerkungen
- 2 Begriffe und Abkürzungen
- 3 Gegenstand des Konzepts
- 4 Instanzen der Sicherheit im Bereich IT an der Hochschule Anhalt
 - 4.1 Aufteilung der Verantwortung
 - 4.2 Aufgabenbereiche der IT-Verantwortlichen bezüglich der Sicherheit
 - 4.3 Verantwortlichkeit der Nutzer von IT-Systemen
- 5 Schutzmaßnahmen an der Hochschule
 - 5.1 Grundsätze
 - 5.2 Festlegung der Schutzmaßnahmen
- 6 Anlagen
 - 6.1 Anlage 1a: Verantwortlichkeitsbereiche der IT-Verantwortlichen in den Struktureinheiten
 - 6.2 Anlage 1b: Verantwortungsbereiche der IT-Betreuer in den Struktureinheiten
 - 6.3 Anlage 2: Hinweise an Nutzer für einen sicheren Betrieb des IT-Systems

1 Vorbemerkungen

Die zunehmende Durchdringung aller Lebensbereiche mit modernen Informationstechniken, insbesondere deren Vernetzung mit dem Internet als die am meisten genutzte Form der Kommunikation, hat den Bedarf und die Notwendigkeit nach einer zuverlässigen Sicherheit der Informationen und Schutz der Personen vor Missbrauch ihrer Daten stark wachsen lassen.

An der Hochschule Anhalt findet das seinen Ausdruck darin, dass bei wachsender Zahl der Arbeitsplätze mit Internetzugang, bei Einbeziehung weiterer Bereiche des wissenschaftlichen Lebens wie E-Learning, Tagungen und Kolloquien in die Kommunikation mittels Internet, der Ruf nach besserem Schutz vor Attacken aus dem Internet von Seiten der Mitarbeiter immer mehr zunimmt.

Da die alltägliche Arbeit in Lehre, Forschung und Verwaltung an der Hochschule in einer engen Abhängigkeit vom sicheren Funktionieren der Informations- und Kommunikationstechniken geworden ist, wirken Störungen im Rechnernetz immer mehr in Richtung der Arbeitsunfähigkeit der Person.

Gleichzeitig wächst das Gefährdungspotential durch die wachsende Vernetzung der Arbeitsplätze, weil immer weitere Anwendungen aus dem Internet erschlossen werden und weil eine höhere Verantwortung des Einzelnen für die Umsetzung der Sicherheitsmaßnahmen zwar erforderlich ist – dieses mangels Wissen beim normalen Mitarbeiter um den Grad der Gefährdung und den Schutzmöglichkeiten jedoch nicht anerkannt wird.

Es soll herausgestellt sein, dass IT-Sicherheit nicht nur eine Frage der Hardware und Software ist – IT-Sicherheit

ist vor allem auch eine personelle, organisatorische, bauliche Aufgabe sowie im besonderen Maße eine Aufgabe des Managements.

Diesen Anforderungen soll mit dem vorliegenden Konzept eine erste Antwort gegeben werden. Hier sollen prinzipielle Aufgaben und erste Festlegungen zu personellen, organisatorischen und Aspekten des Management festgeschrieben werden, die zur Verbesserung der Sicherheit im IT-Bereich führen. Im Zentrum steht dabei die Identität der Nutzer zu schützen, das Kommunikationsnetz mit den integrierten Rechnern vor Missbrauch sowie die Daten vor Missbrauch, Verlust und Verfälschung zu bewahren. Als ein äußerst innovativer Bereich erfordert die Informationstechnik die ständige Weiterentwicklung der Schutzmaßnahmen. Im Konzept wird dem durch verschiedene Regelungen zur Nachhaltigkeit Rechnung getragen.

Ein Konzept zur IT-Sicherheit steht im engen Zusammenhang mit der Datenschutzordnung der Hochschule. Dort formulierte Richtlinien sollen hiermit ergänzt werden.

2 Begriffe und Abkürzungen

| | |
|-----------------------------------|--|
| IT-Beauftragter | Ein Professor im Fachbereich, der im Auftrag des Dekans für die organisatorischen und inhaltlichen Fragen der IT des Fachbereichs zuständig ist |
| IT-Verantwortlicher | Ein Mitarbeiter im Fachbereich, der im IT-Bereich die technisch, administrativen Aspekte für den Fachbereich vertritt. Das kann der PC-Pool-Betreuer oder der IT-Administrator im Fachbereich sein |
| IT-Betreuer | IT – Betreuer administrieren die IT-Systeme der Nutzer im Fachbereich. Es liegt im Ermessensspielraum des Fachbereiches, ob und wie viele IT-Betreuer benannt werden |
| Nutzer | Mitglieder und Angehörige der Hochschule, die Computer oder Netzkomponenten an der Hochschule nutzen |
| IT-System | Rechentchnik in Form von Servern, Arbeitsplatzrechnern, Computern in Geräten und Laboren, in Pools, Hörsälen, Seminarräumen und Projekträumen |
| Kommunikationsnetz der Hochschule | Alle durch ein Medium (Kabel, LWL, Funk oder anderes) verbundenen Komponenten der Rechen- und Kommunikationstechnik im Verantwortungsbereich der Hochschule Anhalt (Campusnetz). |
| Server | Computer mit einer Serversoftware, die anderen Rechnern gewisse Dienste zur Verfügung stellen |
| Datenklassen | Daten mit ähnlichen Eigenschaften, hier hinsichtlich der Sicherheit, werden zu Datenklassen zusammengefasst. |
| Update | Die überarbeitete Version eines Softwareproduktes, in welcher die Funktionalität verbessert und Fehler korrigiert wurden |
| Virens Scanner | Programm zum Auffinden von Computerviren, indem jede Datei des Computers auf auffällige Bitkombinationen durchmustert wird |
| Firewall | Teile eines Netzwerkes werden durch einen Firewall vor unberechtigtem Zugriff geschützt, indem sie die Datenströme ana- |

| | |
|--------------|--|
| | lysieren und situationsabhängig reagieren |
| Reborn-Card | Die Reborn-Card ist eine zusätzliche Hardwarekomponente. Sie stellt beim Neustart des IT-Systems einen definierten Systemzustand her. Alle seit dem letzten Neustart vorgenommenen Systemänderungen werden rückgängig gemacht |
| Backup | Sicherheitskopie eines Datenbestandes, die bei Datenverlust eine Möglichkeit bietet, die ursprünglichen Datenbestände wiederherzustellen |
| IP-Nummer | Jeder Computer im Internet hat eine eindeutige Nummer, die IP-Nummer (IP – Internet Protocoll) |
| Proxy-Server | Server zur Zwischenspeicherung von Internetseiten |
| DMZ | Abkürzung für "demilitarized zone". Unter DMZ versteht man ein "Grenznetzwerk" (ein entkoppeltes, isoliertes Teilnetzwerk), das zwischen ein zu schützendes Netz (z.B. ein LAN) und ein unsicheres Netz (z.B. das Internet) geschaltet wird |
| VPN | Abkürzung für "Virtual Private Network". Ein VPN ist ein Netzwerk, bestehend aus virtuellen Verbindungen, über die zu schützende Daten sicher übertragen werden |

3 Gegenstand des Konzepts

- (1) Mit dem vorliegenden Dokument werden die Grundsätze der Sicherheitspolitik bezüglich der IT-Systeme in Lehre und Forschung an der Hochschule formuliert. Mit dem Konzept sollen verbindliche Regelungen getroffen werden, die ein möglichst störungsfreies Arbeiten mit den IT-Systemen im Kommunikationsnetz der Hochschule ermöglichen.
- (2) Gegenstand dieses Konzeptes sind alle mit dem Campusnetz verbundenen IT-Systeme und die darauf verwendeten Daten in den Fachbereichen, soweit die Bereitstellung von Diensten bzw. der Transport von Daten für die Aufgaben in Lehre und Forschung betroffen sind, sie aber nicht selbst Gegenstand einer experimentellen Lehre bzw. Forschung sind.
Nicht in diesem Konzept werden die Regelungen der Sicherheit für die zentralen Bereiche und die Verwaltung der Hochschule behandelt. Darunter sind hier Präsidium, Dezernate und zentrale Einrichtungen zusammengefasst. Diese äußerst wichtige Thematik soll in einem gesonderten Dokument dargestellt werden¹.
- (3) Das Konzept gilt auch für private IT-Systeme von Mitgliedern und Angehörigen der Hochschule, wenn sie für die Erfüllung von dienstlichen Belangen mit dem Campusnetz verbunden werden sollen. Hierfür werden vom HRZ gesonderte Betriebsregelungen getroffen.
- (4) Im Sicherheitskonzept werden Maßnahmen für eine Verbesserung der IT-Sicherheit genannt und Teile zur Umsetzung empfohlen. Technische und administrative Details sind in Anlagen zum Sicherheits-

¹ Die Reihenfolge der Dokumentenerarbeitung wurde gewählt, um Erfahrungen zu sammeln, weil die Spezifik der Verwaltung eine andere Zusammensetzung des Autorenteam erfordert und in der Verwaltung die Verknüpfungen zu den „vertikalen“ und „horizontalen“ Systemen gesehen werden muss.

konzept formuliert. Sie werden unter Verantwortung des HRZ regelmäßig, entsprechend dem aktuellen weltweiten Stand der Datensicherheit, angepasst.

4 Instanzen der Sicherheit im Bereich IT an der Hochschule Anhalt

4.1 Aufteilung der Verantwortung

- (1) Grundsätzlich ist die Verantwortlichkeit für den Betrieb der IT-Systeme an der Hochschule Anhalt geteilt in zentrale Komponenten, die durch das HRZ wahrgenommen werden und dezentrale Komponenten, die durch die Struktureinheiten (Fachbereiche) wahrgenommen werden. Diese Aufgabenteilung ist im Standortprinzip der Hochschule begründet.
- (2) Das HRZ trägt die Betriebsverantwortung für
 - a) das passive Kommunikationsnetz;
 - b) die aktiven Komponenten in diesem Kommunikationsnetz;
 - c) zentrale Sicherheitseinrichtungen, die im Netz installiert sind;
 - d) den Zugang zu externen Netzen.
 Das hier beschriebene Kommunikationsnetz ist ein Betriebsnetz und unterliegt den Festlegungen dieses Konzepts. Es ist gegen Störungen, Ausfall und Missbrauch zu sichern.
- (3) Zuständig für die Sicherheit dezentraler IT-Systeme ist die Struktureinheit, in deren Verantwortungsbereich das System betrieben wird.
- (4) Die Struktureinheiten (Fachbereiche) sind insbesondere dafür zuständig, dass
 - a) ein IT-Beauftragter (i.d.R. ein Professor aus dem Fachbereich) und ein IT-Verantwortlicher (i.d.R. ein technischer Mitarbeiter) für die Struktureinheit benannt und
 - b) jedem IT-System ein IT-Betreuer zugeordnet wird;
 - c) diese Zuordnung dokumentiert und beim HRZ hinterlegt wird.
- (5) Vom HRZ wird eine Dokumentation der im Kommunikationsnetz integrierten IT-Systeme, deren Netzadressen und der zugeordneten IT-Verantwortlichen geführt.

4.2 Aufgabenbereiche der IT-Verantwortlichen bezüglich der Sicherheit

- (1) Die weiter unten aufgeführten Aufgabenbereiche bezüglich der Sicherheit in IT-Systemen müssen mit den Tätigkeitsmerkmalen bzw. mit den Aufgabenfeldern der betroffenen Mitarbeiter abgeglichen und in den Tätigkeitsbeschreibungen verankert werden. Auftretende Konflikte sind als Einzelfälle durch den Dekan bzw. Vorgesetzten zu lösen.
- (2) Zu den generellen Aufgabenbereichen des IT-Verantwortlichen gehören:
 - a) Die Sicherstellung des Betriebs aller Komponenten der Datensicherung durch Updates, Sicherungskopien oder andere geeignete Maßnahmen.
 - b) Auf jede Art von Anormalität beim Betrieb des IT-Systems in angemessener Form zu reagieren, insbesondere im Sinne einer Schadensverhinderung bzw. Schadensbegrenzung.
 - c) Bei der regelmäßigen Sicherstellung der Aktualität aller Komponenten, insbesondere bei Beschaffungen, mitzuwirken.

- d) Die Nutzer im Fachbereich in den Fragen der Sicherheit zu beraten.
- e) Ständige Selbstqualifizierung und Teilnahme an angebotenen Veranstaltungen zu dieser Thematik.

Weitere Aufgabenbereiche und Details regelt die Anlage 1.

- (3) Zur Verhinderung eines Schadens bzw. zur Eingrenzung eines aufgetretenen Schadens haben die IT-Verantwortlichen das Recht, in den Betrieb eines IT-Systems ihres Verantwortungsbereiches einzugreifen. Im Extremfall ist das IT-System vom Kommunikationsnetz zu trennen. Das sollte nach Möglichkeit in Absprache und im Beisein des Betreibers erfolgen und mit möglichst geringen Folgeschäden. Der Dekan ist umgehend zu informieren.
- (4) Weitere Festlegungen werden vom HRZ in Betriebsregelungen formuliert.

4.3 Verantwortlichkeit der Nutzer von IT-Systemen

- (1) Jeder Hochschulangehörige hat das ihm übergebene IT-System so zu betreiben, dass Schäden vermieden werden. Dazu hat er insbesondere die geltenden Regelungen einzuhalten und durch vorbeugendes Verhalten das Sicherheitsrisiko zu minimieren sowie mögliche Schäden gering zu halten.
- (2) Es ist allgemein anerkannt, dass die Wirksamkeit und Durchsetzung von Sicherheitsregeln letztlich von den Nutzern abhängt. Aus diesem Grunde wird ein „Regelwerk“ bezüglich des Umgangs mit Systemen und Komponenten der Informationstechnologien für alle Nutzer verfasst. Die Einzelheiten sind in Anlage 2 formuliert. Es gehört zu den Pflichten der Nutzer diese Regeln einzuhalten.
- (3) Die Mitarbeiter der Hochschule sind regelmäßig in geeigneter Form über die geltenden Regelungen zu informieren. Sie haben andererseits die Pflicht, sich selbst darüber zu informieren.
- (4) Zu den weiteren Grundsätzen eines sicherheitsbewussten Arbeitens mit IT-Systemen auf Nutzerebene, die in Anlage 2 weiter untersetzt werden, gehören:
 - a) Reagieren in angemessener Form auf jede Art von Anormalität, insbesondere im Sinne einer Schadensverhinderung bzw. Schadensbegrenzung. Über Anormalitäten ist umgehend der IT-Verantwortliche zu informieren.
 - b) Sicherheitsbewusster Umgang mit Passwörtern: Dazu gehören insbesondere die entsprechende Auswahl des Passwortes, die regelmäßige Änderung und die Geheimhaltung.
 - c) Dem Nutzer ist es nicht erlaubt, Komponenten in das IT-System zu integrieren, die den an der Hochschule erlassenen Regelungen für einen sicheren Betrieb widersprechen.
 - d) Das Installieren und Betreiben von Servern, die im Internet öffentlich zugängliche Informationen bereitstellen, ist nur nach Anmeldung beim HRZ und nach Genehmigung durch den Präsidenten der Hochschule erlaubt.
 - e) Es ist nur im Rahmen der betrieblichen Regelungen erlaubt, private Computer oder deren Komponenten

im Kommunikationsnetz der Hochschule zu nutzen.

5 Schutzmaßnahmen an der Hochschule

5.1 Grundsätze

- (1) Die Anforderungen an die Sicherheit des einzelnen IT-Systems und die Maßnahmen ihrer Gewährleistung richten sich nach der Bedeutung des Systems für den Betrieb der Hochschule, d.h. nach dem Schutzbedarf für das System. Generell muss hierbei die Verhältnismäßigkeit beachtet werden. Die Sicherheit kann nur mit einem vertretbaren finanziellen und personellen Aufwand realisiert werden.
- (2) Der Schutzbedarf eines IT-Systems der Hochschule richtet sich danach, welche Daten mit dem System verwaltet werden. So sind personenbezogene Daten anders zu sichern als Projektdaten einer studentischen Übung.
- (3) Ein zweiter Aspekt des Schutzbedarfs sind die betrachteten IT-Systeme. Für Poolrechner gilt ein anderes Sicherheitsregime als für Daten-server.
- (4) Welche Datenklassen auf dem einzelnen IT-System gespeichert oder verarbeitet werden ist unter Beachtung der Regelungen in der Datenschutzordnung der Hochschule festzulegen. Die Entscheidung darüber ist im jeweiligen Verantwortungsbereich des IT-Systems zu fällen.
- (5) Prinzipiell gilt, dass für die hier betrachteten IT-Systeme bis auf Ausnahmen die Herstellung eines definierten, sicheren Zustandes Vorrang hat vor der unbedingten Abwehr von Angriffen.
- (6) Konflikte zwischen den Anforderungen der Sicherheit und der Erfüllung der Aufgaben für Lehre und Forschung sind so zu lösen, dass keine Minderung der Sicherheit für die Allgemeinheit auftritt, sondern höchstens für das in den Sicherheitsanforderungen herabgestufte einzelne IT-System und das auch erst nach Belehrung des betreibenden Wissenschaftlers. Die daraus entstehenden materiellen und finanziellen Anforderungen trägt der Fachbereich.

5.2 Festlegungen für Schutzmaßnahmen

- (1) Die Verantwortung für die Realisierung der Schutzmaßnahmen unterliegt den in 4. beschriebenen Regeln. Das hat zur Konsequenz, dass dementsprechend auch die Ressourcen der Realisierung vorzuhalten sind.
- (2) Von den im IT-Grundschutzhandbuch der BSI² aufgeführten Maßnahmenkataloge zum Schutz der IT-Systeme, die als Referenzen einen umfassenden Geltungsbereich haben müssen, kommen unter den gegenwärtigen konkreten Bedingungen der Hochschule die folgenden in Betracht:
 - a) Einsatz eines Virenscanners auf den Endgeräten
 - b) Passwortgeschützter Zugang
 - c) Einsatz einer Personal Firewall auf den Endgeräten
 - d) Anlegen von Kopien

² „IT-Grundschutzhandbuch“, Bundesanzeiger Köln, 2003

- e) Einsatz einer Reborn-Card
 - f) Nutzung eines Backup-Systems
 - g) Vergabe interner IP-Nummern
 - h) Anwendung eines Proxy-Servers
 - i) Anwendung einer netzbasierten Firewall
 - j) Einrichtung einer DMZ
 - k) Einsatz eines VPN
 - l) Trennung des IT-Systems vom öffentlichen Netz
- (3) Als Mindestmaß der Realisierung an Schutzmaßnahmen in allen hier geltenden Bereichen werden diese festgelegt:
- a) Passwortgeschützte personalisierter Zugang zu den IT-Systemen (zeitlich begrenzte und technisch begründete Ausnahmen werden vom IT-Beauftragten des Fachbereiches genehmigt);
 - b) Einsatz eines Virenschanners auf den Endgeräten;
 - c) Anwendung einer Firewall oder Personal Firewall (zeitlich begrenzte und technisch begründete Ausnahmen werden vom IT-Beauftragten des Fachbereiches genehmigt).

Weitere Maßnahmen liegen im Verantwortungsbereich des Betreibers eines IT-Systems.

- (4) Das HRZ hat den Auftrag,
- a) ein zentrales Backup-System für Server zu betreiben und
 - b) die Fachbereiche bei der Erarbeitung eines Konzepts für die Sicherheit in IT-Systemen zu unterstützen.
- (5) Zu den Maßnahmen der physischen Datensicherung gehören
- a) Diebstahlsicherungen an den Geräten
 - b) Einbruchsicherungen an Türen und Fenstern
 - c) unterbrechungsfreie Stromversorgung
 - d) Einsatz von Videokameras

Die Anwendung dieser Maßnahmen erfolgt in Abstimmung mit der Verwaltung der Hochschule Anhalt.

- (6) An der Hochschule wird ein Sicherheitskomitee eingerichtet, das sich aus den IT-Verantwortlichen der Fachbereiche und dem Leiter des HRZ zusammensetzt. Aufgabe des Komitees ist die Ausarbeitung von Empfehlungen zur Sicherheit im IT-Bereich, die diese Konzeption untersetzen und sich konkret auf den Fachbereich und das IT-System beziehen.

6 Anlagen

Anlage 1a: Verantwortungsbereiche der IT-Verantwortlichen in den Struktureinheiten

Anlage 1b: Verantwortungsbereiche der IT-Betreuer in den Struktureinheiten

Anlage 2: Hinweise an die Nutzer für einen sicheren Betrieb des IT-Systems

6.1 Anlage 1a: Verantwortungsbereiche der IT-Verantwortlichen in den Struktureinheiten

Die IT-Verantwortlichen in den Struktureinheiten sind zuständig für

- die Verwaltung der ihnen vom HRZ im Block zugewiesenen Parameter für das Netzwerk (IP-Adressen, u.a.);
- die Koordinierung operativer Angelegenheiten zur Administration des Campusnetzes und Beschaffungsfragen mit dem HRZ;
- die Anleitung der IT-Betreuer
- die Beratung der Nutzer.

Im Rahmen der Ausübung dieser Verantwortung haben die IT-Verantwortlichen insbesondere folgende Kompetenzen:

- Vorgabe von insbesondere sicherheitsrelevanten Parametern an den IT-Systemen;
- Anordnung von Nutzungseinschränkungen für die Systeme bei akuter Gefährdung der Sicherheit des betroffenen bzw. anderer am Hochschulnetz betriebener Systeme;
- Rekonfiguration der Systeme bei Notwendigkeit.

6.2 Anlage 1b: Verantwortungsbereiche der IT-Betreuer in den Struktureinheiten

Die IT-Betreuer in den Struktureinheiten sind zuständig für

- die korrekte Installation der Betriebssysteme auf die von der Struktureinheit betriebenen IT-Systemen;
- die korrekte Installation der Sicherheitsfeatures (z.B. Virenschanner, Personal Firewall, ...) nach Vorgaben zur Nutzung der Systeme;
- die Organisation der Datensicherung;
- regelmäßige Aktualisierung der Systeme (insbes. bei aktueller Notwendigkeit oder bei Fehlfunktion);
- die Beseitigung von Fehlfunktionen der IT-Systeme;
- die Pflege der Software;
- die Beratung der Nutzer.

6.3 Anlage 2: Hinweise an die Nutzer für einen sicheren Betrieb des IT-Systems

Die DV-Kommission hält es für erforderlich, die unten beschriebenen Regeln als empfehlenswert für alle Nutzer zu publizieren.

- (1) Grundlage für die Nutzung von IT-Systemen an der Hochschule Anhalt sind die Ordnungen der Hochschule, insbesondere die Betriebsregelungen des HRZ, die unter Berücksichtigung der jeweiligen Dienstaufgaben beim Betrieb von arbeitsplatzbezogenen IT-Systemen der Nutzer anzuwenden sind.
- (2) Mit den hier formulierten Verhaltensregeln sollen eine weitestgehend störungsfreie Nutzung der Informations- und Kommunikationssysteme und die Einhaltung von Copyright-, Urheber- und Nutzungsrechten gesichert werden. Gleichzeitig ist die Sicherheit und Vertraulichkeit der Daten zu gewährleisten.
- (3) Eine wesentliche personelle Voraussetzung für die Durchsetzung der Verhaltensregeln ist die fachliche Unterstützung der Nutzer durch IT-Verantwortliche und IT-Betreuer in den Fachbereichen. In der Regel sind nur IT-Betreuer zur Installation und Wartung der arbeitsplatzbezogenen Rechentechnik sowie der Server in Zusammenarbeit mit den Mitarbeitern des HRZ berechtigt. Ausnahmen sind durch den Dekan zu genehmigen.
- (4) Bei der Beschaffung von Hard- und Software in den Fachbereichen sollten die IT-Verantwortlichen vom Dekan konsultiert werden, um die Passfähigkeit

neuer Systeme in das Gesamtkonzept des Fachbereichs und der Hochschule zu sichern.

- (5) Für Systempflegearbeiten ist den IT-Betreuern jederzeit Zugriff auf die Systeme zu gewährleisten. Dabei ist der Einsatz von Systemen zur Fernwartung in Absprache mit dem Nutzer anzustreben. Kurzfristige Sperren von Systemen bei Notsituationen, im Auftrag des Präsidiums der Hochschule und nach Anweisung des HRZ können ohne Rücksprache mit den Nutzern durchgeführt werden. Der Nutzer ist über Ursache und Dauer der Sperrung zu informieren.
- (6) Zur Sicherung der Nutzeridentität und zur Wahrung der Vertraulichkeit der gespeicherten Daten sind solche Betriebs- und Dateisysteme einzusetzen, die eine autorisierte Anmeldung sowie eine gestufte Rechtevergabe ermöglichen.
- (7) Die Aktualisierung der Betriebssysteme sollte automatisiert werden, für Microsoft-Systeme ist ein zentraler Update-Dienst an der Hochschule einzurichten.
- (8) Auf dem Nutzer-PC darf durch die IT-Betreuer nur solche lizenzierte Soft- und Freeware installiert werden, die durch dienstliche Anforderungen bedingt ist. Vor der Installation neuer Programme bzw. Programmversionen sind die Notfalldiskette und der Virens Scanner zu aktualisieren sowie eine Sicherung der Nutzerdaten durchzuführen. Die IT-Verantwortlichen der Struktureinheiten informieren die Nutzer über aktuelle Versionen und Updates der installierten Software und weisen sie in deren Handhabung ein.

- (9) Beim unnormalen Verhalten des Computers sollte der Nutzer Fehlermeldungen möglichst exakt notieren sowie wichtige Daten sichern. Es sind keine "Selbst"-Reparaturen durchzuführen, sondern in jedem Fall der IT-Betreuer zu konsultieren. Für bekannte, mehrfach auftretende Fehlfunktionen formulieren die IT-Betreuer Verhaltensregeln und informieren die Nutzer über Aktualisierungen. Die folgende Übersicht dient als Beispiel:

| Fehler | Reaktion des Nutzers |
|---|---|
| Betriebssystem wird nicht geladen | IT-Betreuer konsultieren |
| Virenwarnung (ohne Nutzung externer Datenträger) | 1. Virendefinitionsdateien aktualisieren 2. PC scannen 3. IT-Betreuer informieren |
| Virenwarnung beim Zugriff auf externe Datenträger | 1. Datenträger entfernen 2. Virendefinitionsdateien aktualisieren 3. PC scannen 4. Datenträger scannen 5. IT-Betreuer informieren |
| doppelte Abfrage des Passwortes bei der Anmeldung | 1. Wenn der Nutzer sicher ist, keine Fehleingabe getätigt zu haben, sofort abmelden und den PC ohne Netzanbindung neu starten 2. anmelden und PC scannen 3. Passwort ändern |

- (10) In den Fachbereichen sollten unter Federführung des IT-Beauftragten und in Zusammenarbeit mit den IT-Verantwortlichen und IT-Betreuern sowie unter Berücksichtigung der hochschulweit gültigen Ordnungen bereichsspezifische Nutzerregeln festgelegt werden. Insbesondere sind die folgenden Regelungen für verbindlich zu erklären und einzuhalten:

- o Verschließen des Dienstzimmers bei Abwesenheit;
- o Herunterfahren und Ausschalten des Computers bei längerer Abwesenheit;
- o Einsatz eines Bildschirmschoners mit Passwortschutz;
- o das Passwort ist sicher auszuwählen, sorgsam zu verwahren und nicht weiterzugeben;
- o Deaktivieren des Bootens von FD/CD/Netz/USB ;
- o regelmäßige Datensicherungen auf geeignete externe Speichermedien durch die Nutzer;
- o der Virens Scanner ist aktuell zu halten;
- o in "Netzwerkzeugen" bzw. Firewalls sind defensive Einstellungen vorzunehmen;
- o Anwenden der Filterwerkzeuge in den Mail-Clients.