Freie Universität Berlin

Kommentierte
IT-Grundschutzmaßnahmen für IT-Anwender

Auszug aus der IT-Sicherheitsrichtlinie
für die Freie Universität Berlin

August 2009

Inhaltsverzeichnis

Inhaltsverzeichnis 2

1. IT-Grundschutz 3

1.1. Maßnahmen des IT-Grundschutzes für IT-Anwender 3
1.1.1. Allgemeines 3
- Anwenderqualifizierung (M1.1) 3
- Meldung von Sicherheitsproblemen (M1.2) 3

1.1.2. Sicherung der Infrastruktur 4
- Räumlicher Zugangsschutz (M1.3) 4
- Brandschutz (M1.4) 5
- Sicherung mobiler Computer (M1.5) 5

1.1.3. Hard- und Software 6
- Kontrollierter Softwareeinsatz (M1.6) 6
- Einsatz von privater Hard- und Software (M1.7) 7
- Virenschutz (M1.8) 7

1.1.4. Zugriffsschutz 8
- Abmelden und ausschalten (M1.9) 8
- Personenbezogene Kennungen (M1.10) 9
- Gebrauch von Passwörtern (M1.11) 9
- Zugriffsrechte (M1.12) 11
- Netzzugänge (M1.13) 12

1.1.5. Kommunikationssicherheit 12
- Sichere Netzwerknutzung (M1.14) 12

1.1.6. Datensicherung 13
- Datensicherung (M1.15) 13

1.1.7. Umgang mit Datenträgern 14
- Sichere Aufbewahrung (M1.16) 14
- Datenträgerkennzeichnung (M1.17) 14
- Gesicherter Transport (M1.18) 15
- Physisches Löschen von Datenträgern (M1.19) 15

1.1.8. Schützenswerte Daten 16
- Schützenswerte Daten auf dem Arbeitsplatz-PC (M1.20) 16
- Sichere Entsorgung vertraulicher Papiere (M1.21) 17

1. IT-Grundschutz

1.1. Maßnahmen des IT-Grundschutzes für IT-Anwender

1.1.1. Allgemeines

- **Anwenderqualifizierung (M1.1)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)

Die Mitarbeiter sind aufgabenspezifisch zu schulen und dürfen erst dann mit IT-Verfahren arbeiten. Dabei sind sie insbesondere auch mit den für sie geltenden Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes vertraut zu machen.

Kommentar:

Die Maßnahme „Anwenderqualifizierung" zielt darauf ab, die fehlerhafte Bedienung von Software-Anwendungen und PCs aufgrund mangelnder Kenntnisse zu minimieren. Fehlerhafte Bedienungen können unter Umständen relativ große Schäden nach sich ziehen. Besonders das Wissen um die an der Freien Universität Berlin geltenden IT-Sicherheitsmaßnahmen und deren fachgemäße Umsetzung ist für einen sicheren IT-Betrieb unverzichtbar.

Beispiel: Bei Nutzung des E-Mail-Dienstes sind einfache Verhaltensweisen zu beachten. Angenommen man korrespondiert nur mit deutschsprachigen Partnern und dies ausschließlich dienstlich. Bei Empfang einer englischsprachigen E-Mail mit Anhang von einem unbekannten Absender in dessen Betreff „I LOVE YOU" steht, sollten alle Alarmsirenen angehen. In diesem Fall wäre es am besten, die E-Mail ungelesen zu löschen, um das Infizieren des PCs mit Viren zu verhindern.

- **Meldung von Sicherheitsproblemen (M1.2)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)

Auftretende Sicherheitsprobleme aller Art (Systemabstürze, Fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u.ä.) sind dem zuständigen IT-Personal mitzuteilen.

Kommentar:

Die IT-Anwender sind durch ihren tagtäglichen Umgang mit den Softwareprogrammen und den entsprechenden Daten viel eher in der Lage, Manipulationen und fehlerhaftes Programmverhalten zu erkennen als z.B. ein Administrator, der nur gelegentlich mit den Anwendungsprogrammen arbeitet. Aus diesem Grund ist die Meldung von Sicherheitsvorfällen im Sinne einer raschen Beseitigung ganz besonders auch Aufgabe der IT-Anwender.

Wird beispielsweise der Virenbefall eines PCs unverzüglich der zuständigen Stelle gemeldet, haben die dortigen Mitarbeiter die Möglichkeit, durch intervenierende Maßnahmen die Verbreitung der Viren in das gesamte Netz der Freien Universität Berlin zu verhindern.

1.1.2. Sicherung der Infrastruktur

- **Räumlicher Zugangsschutz (M1.3)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Der unbefugte Zugang zu Geräten und die Benutzung der Informationstechnik muss verhindert werden. Bei Abwesenheit sind Mitarbeiter-Räume mit Informationstechnologie verschlossen zu halten. Bei der Anordnung und baulichen Einrichtung der Geräte ist darauf zu achten, dass schützenswerte Daten nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

Kommentar:

Das Verschließen von nicht besetzten Räumen (besonders in Bereichen mit Publikumsverkehr) soll verhindern, dass es Unbefugten gelingt, Einsicht bzw. Zugriff auf schützenswerte Unterlagen und IT-Systeme zu erlangen und evtl. Schäden zu verursachen. Das Bekannt werden von hochschützenswerten Daten, z.B. Personaldaten, kann zu einem Ansehensverlust der Freien Universität Berlin in der breiten Öffentlichkeit führen; eine finanzielle bzw. Rufschädigung von Personen kann ebenfalls nicht ausgeschlossen werden. Ein weiterer nicht zu vernachlässigender Aspekt ist der Schutz der Hardware vor Diebstahl.

- **Brandschutz (M1.4)**

Verantwortlich für Initiierung:	Brandschutzbeauftragter, IT-Verantwortlicher
Verantwortlich für Umsetzung:	Brandschutzbeauftragter, Technische Abteilung

Alle Maßnahmen und Einrichtungen, die dem vorbeugenden Brandschutz dienen, sind einzuhalten bzw. zu nutzen. Lüftungsöffnungen an den Geräten dürfen nicht verstellt oder verdeckt werden. In allen Räumen, in denen Server und Netzwerkkomponenten untergebracht sind, sind alle Tätigkeiten zu unterlassen, die zu einer Rauchentwicklung führen.

Kommentar:

Häufig entstehen Brände aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros finden sich eine Reihe brennbarer Materialien, wie z.B. Papier, Holzmöbel und Kunststoffe, die die rasche Ausbreitung eines Feuers begünstigen. Demzufolge ist die Sofortbekämpfung von Bränden besonders wichtig. Jeder Mitarbeiter ist deshalb dazu aufgefordert, die Brandschutzbestimmungen zu befolgen und sicherzustellen, dass beispielsweise Feuerlöscher nicht zugestellt werden. Detaillierte Regelungen und Informationen zum Thema Brandschutz erhalten Sie auf der Homepage der Dienststelle für Arbeitssicherheit der Freien Universität Berlin unter http://www.fu-berlin.de/das/Brandschutz.htm.

Damit Brände erst gar nicht entstehen bzw. schon bei Ausbruch eines Feuers entsprechende Maßnahmen ergriffen werden können, empfiehlt sich die Teilnahme an Brandschutzübungen, die an der Freien Universität Berlin angeboten werden.

- **Sicherung mobiler Computer (M1.5)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Anwender

Bei der Speicherung von schützenswerten Daten auf mobilen Computern (Notebooks) sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Derartige Daten müssen verschlüsselt werden.
Notebooks sind möglichst verschlossen aufzubewahren.

Kommentar:

Die Verpflichtung zur Verschlüsselung von Daten auf mobilen Computern verfolgt die Absicht, bei Verlust oder Diebstahl von Notebooks den Schutz der Daten vor unbefugtem Zugriff, vor Manipulation sowie vor widerrechtlicher Bekanntgabe zu gewährleisten. Verschlüsselte Daten können selbst von den leistungsfähigsten Computeranlagen der Welt in einem vernünftigen Zeitraum nicht geknackt werden.

Beispiel: Auf einer Geschäftsreise wird einem Mitarbeiter der Universität aufgrund von Unachtsamkeit das Notebook gestohlen. Auf dem Notebook waren Daten über die Sicherheitsinfrastruktur der Freien Universität Berlin unverschlüsselt gespeichert.

Der Dieb ist an den Informationen über den Aufbau und die Struktur der an der Freien Universität Berlin installierten Sicherheitssysteme nicht interessiert, jedoch veröffentlicht er die Daten böswillig im Internet. Mit dem Bekannt werden der Daten wird potentiellen Angreifern Tür und Tor zum Universitätsnetz geöffnet; die Wiederherstellung der Sicherheit ist mit erheblichem finanziellen und zeitlichen Aufwand verbunden.

Für Informationen zum Thema Verschlüsselung wenden Sie sich bitte an das zuständige IT-Personal oder den IT-Verantwortlichen Ihres Bereichs. Programme zur Verschlüsselung von Dateien und Ordnern können in der Regel von dem zuständigen IT-Personal bereitgestellt werden.

1.1.3. Hard- und Software

- **Kontrollierter Softwareeinsatz (M1.6)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Anwender

Auf Rechnersystemen der Freien Universität Berlin darf zum Zweck des Schutzes von universitätseigener Hardware und dem Universitätsnetz nur Software installiert werden, die von der zuständigen Stelle dafür freigegeben wurde. Das eigenmächtige Einspielen, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn eine Erlaubnis oder pauschale Freigabe der zuständigen Stelle vorliegt.

Kommentar:

Ziel der Maßnahme ist es, zu verhindern, dass durch das unbefugte Installieren nicht freigegebener Computerprogramme Schadsoftware (Viren, Trojaner usw.) in das Netz der Universität eingeschleust wird. So verlockend das schnelle Herunterladen und Installieren von Software auch sein mag, die Konsequenzen können aufgrund der miteinander vernetzten Computer immens sein.

Eine der Aufgaben der IT-Verantwortlichen ist es, die an ihrem Bereich eingesetzte Soft- und Hardware zu erfassen und zu dokumentieren. Ein umfassender Überblick zum Zwecke der IT-Sicherheit ist durch das eigenmächtige Installieren von Software durch nicht befugte Mitarbeiter dann nicht mehr möglich.

- **Einsatz von privater Hard- und Software (M1.7)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Anwender

Der Einsatz von privater Hard- und Software im Bereich Forschung und Lehre richtet sich im Allgemeinen nach den fachbereichsinternen Regelungen. Bei Fehlen entsprechender Regelungen sollte nach Möglichkeit nur universitätseigene Hard- und Software eingesetzt werden. In speziell gekennzeichneten Bereichen, wie z.B. im Bereich des Wireless LAN der Freien Universität oder in Bibliotheken, ist der Einsatz von privater Hard- und Software erlaubt.

In besonders geschützten Bereichen und im Umgang mit Verwaltungsdaten, wie zum Beispiel alle personenbezogenen Daten der Beschäftigten und Studierenden und Daten der Ressourcenverwaltung, ist die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der Freien Universität Berlin und deren Netzen nicht gestattet. Sondergenehmigungen, zum Beispiel im Rahmen von Schulungsveranstaltungen oder Vorträgen, können auf Antrag durch die zuständigen IT-Verantwortlichen der Organisationseinheit oder dafür zuständiges IT-Personal erteilt werden.

Kommentar:

Nicht freigegebene Hard- und Software ist weder in organisatorische Abläufe noch in Kontrollen bezüglich der IT-Sicherheit eingebunden und stellen somit ein großes Sicherheitsrisiko dar. Die Computer der Freien Universität Berlin genügen hinsichtlich der Sicherheit bestimmten Mindestanforderungen. Beispielsweise kann davon ausgegangen werden, dass auf jedem Computer ein aktualisierter Virenscanner installiert ist. Inwieweit private Computer den Sicherheitsmindestanforderungen der Freien Universität Berlin genügen, ist hingegen unbekannt. Diese dürfen deshalb nur in Bereichen eingesetzt werden, in denen nicht mit besonders schützenswerten Daten umgegangen wird.

- **Virenschutz (M1.8)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal , IT-Anwender

Auf allen Arbeitsplatz-PCs ist ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden und zu öffnenden Dateien überprüft. Damit soll bereits das Eindringen von schädlichen Programmen erkannt und verhindert werden. Wenn aus technischen Gründen die Installation von Anti-Viren-Soft-ware nicht möglich ist (zum Beispiel bei Prozessrechnern mit Netzanschluss), müssen alternative Schutzmaßnahmen, beispielsweise die Abschottung von Netzsegmenten, ergriffen werden.

Bei Verdacht auf Vireninfektion ist das zuständige IT-Personal zu informieren.

Kommentar:

Die Gefahr durch Computerviren ist in den letzten Jahren stetig gewachsen und inzwischen eine der wesentlichsten Bedrohungen für einen sicheren IT-Betrieb. Dabei reicht das Spektrum der Auswirkungen von relativ harmlosen Belästigungen bis hin zum Ausfall zentraler IT-Systeme. Der Einsatz von Virenscannern soll bewirken, dass schon im Vorfeld Viren erkannt und beseitigt werden, mit dem Ziel, einen Systembefall bzw. die Ausbreitung der Viren über das Campusnetz zu verhindern.

Häufig sind die Computer der Freien Universität Berlin vom IT-Personal bereits mit aktualisierten Virenscannern ausgestattet. In vielen Fällen ist der aktive Virenscanner an einer bestimmten Stelle auf dem Desktop als Symbol sichtbar. Bei Windows XP beispielsweise befindet sich das Symbol des Virenscanners im Infobereich der Taskleiste am unteren rechten Rand. Jedoch ist es möglich, dass auf einigen Computern noch kein Virenscanner installiert ist. In diesen Fällen sollte der Anwender sich an das zuständige IT-Personal wenden.

1.1.4. Zugriffsschutz

- **Abmelden und ausschalten (M1.9)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal , IT-Anwender

Bei kürzerem Verlassen des Zimmers, d.h. bis ca. 10 Minuten, muss der Arbeitsplatz-PC durch einen Kennwortschutz gesperrt werden. Bei längerem Verlassen des Zimmers muss sich der Benutzer aus den laufenden Anwendungen und dem Betriebssystem abmelden. Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen. (Beispielsweise kann die Rechenzeit von Arbeitsplatz-PCs in den Ruhephasen zu wissenschaftlichen Zwecken genutzt werden.)

Kommentar:

Die Sperrung des Rechners ist schnell und einfach möglich. Das Aktivieren des Kennwortschutzes erfolgt bei Windows-PCs über die Tastenkombination „Windowstaste + L“. Die Entsperrung des Arbeitsplatz-PCs wird über die Tastenkombination „Strg + Alt + Entf“ ausgelöst. Die Umsetzung der Maßnahme soll vor allem auch dazu dienen, den Anwender vor ungerechtfertigten Anschuldigungen zu schützen. Im Regelfall sind die Computer an der Freien Universität Berlin so konfiguriert, dass die Programme bzw. das gesamte System erst nach Anmeldung genutzt werden können. In diesem Zustand kann der Rechner bereits missbraucht werden. Zum Beispiel können unter der Kennung des angemeldeten Mitarbeiters Spaß-E-Mails versendet oder Internetforen besucht werden, in denen beispielsweise beleidigende Aussagen geäußert werden. Insbesondere bei IT-Systemen (SAP-HR, SAP-CM usw.), die von verschiedenen Benutzern mit unterschiedlichen

Zugriffsrechten genutzt werden, ist das Missbrauchspotential groß, wenn jemand unter einem anderen Benutzernamen im System agiert.

Wird der Kennwortschutz nicht aktiviert bzw. erfolgt keine Abmeldung am System, so kann im Schadensfall nicht nachvollzogen werden, wer die Schäden verursacht und ggf. die Konsequenzen zu tragen hat. Im Zweifelsfall liegt die Verantwortlichkeit stets bei demjenigen, der angemeldet war.

- **Personenbezogene Kennungen (M1.10)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal , IT-Anwender

Alle Rechnersysteme werden durch das IT-Personal in der Form eingerichtet, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine persönliche Anmeldung mit Benutzerkennung und Passwort oder einem anderen Authentifizierungsverfahren erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen erfolgt in der Regel personenbezogen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Kennungen und Passwörter weiterzugeben.

Kommentar:

Wie die vorherige Maßnahme dient auch diese zum einen dazu, den Benutzer vor ungerechtfertigten Anschuldigungen zu schützen, indem verhindert wird, dass andere unter seiner Kennung Schäden verursachen. Zum anderen soll die Zuordnung von Verantwortlichkeiten möglichst eindeutig sein. Wenn z.B. unter einer Kennung die von mehreren Personen verwendet wird, häufig Fehlbedienungen festgestellt werden, die auf Schulungsbedarf hindeuten, ist nicht unmittelbar klar, welcher Mitarbeiter geschult werden muss. Außerdem soll diese Maßnahme einer grundsätzlichen Unsicherheit bei der Wahrung der Passwortsicherheit entgegenwirken. Je mehr Personen ein Passwort kennen, desto größer ist die Gefahr, dass das Passwort weitergeben wird.

- **Gebrauch von Passwörtern (M1.11)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Der Benutzer hat sein Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden.
Sofern die technischen Gegebenheiten dies zulassen, sind Passwörter nach den folgenden Regeln zu gestalten:

  - Das Passwort muss mindestens 8 Stellen lang sein.
  - Das Passwort muss mindestens einen Buchstaben und mindestens

eine Ziffer oder ein Sonderzeichen enthalten.

- Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln und sollte eine Mindestgültigkeitsdauer von einem Tag haben.
- Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.

Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt.

Erhält ein Benutzer beim Anmelden mit seinem Passwort keinen Zugriff auf das System, besteht die Gefahr, dass sein Passwort durch Ausprobieren ermittelt werden sollte, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem zuständigen Vorgesetzten und dem IT-Personal zu melden. (Siehe M1.2)

Bei Vergessen des Passwortes bzw. nach mehrfacher fehlerhafter Passworteingabe hat der Benutzer die für diesen Fall vorgesehene Verfahrensweise zu befolgen. Die Zahl der erlaubten Fehlversuche wird von der zuständigen Stelle festgelegt. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird. In vielen Systemen muss das Zurücksetzen des Passworts durch den Administrator veranlasst werden. Andere Systeme sehen für diesen Fall vor, dass der Benutzer sich selbst wieder registriert.

Kommentar:

Die besten technischen Authentifizierungsverfahren verlieren ihre Schutzwirkung, wenn die Anwender nicht sorgfältig mit den Passwörtern umgehen. Sicherheitslücken finden sich hauptsächlich in den folgenden drei Punkten:

Das Problem der Weitergabe:
Gelegentlich kommt es vor, dass Passwörter weitergegeben oder unter Kollegen geteilt werden. Diese Gepflogenheiten verstoßen elementar gegen die geltenden Sicherheitsvorschriften und bergen all die Gefahren in sich, die in den Erläuterungen zu den Maßnahmen M 1.9 und M 1.10 dargelegt wurden.

Das Problem der unsicheren Aufbewahrung:
Gerade bei mehreren Passwörtern, die meist unterschiedlich häufig benötigt werden, fällt es Mitarbeitern verständlicherweise schwer, sich jedes Einzelne zu merken. Um dies zu verhindern, werden Passwörter auf Zetteln vermerkt. Gegen diese Art der Gedächtnisstütze ist dann nichts einzuwenden, wenn die Merkzettel sicher aufbewahrt werden. Die Vorgehensweise, das Passwort unter der Tastatur zu verstauen bzw. an den Bildschirm zu kleben, erfüllt dieses Kriterium nicht.

Das Problem der Wahl des Passworts:
Um ein Passwort ausreichend sicher zu gestalten, so dass es mit den Mitteln der Technik in einem angemessenen Zeitraum nicht erraten bzw. „geknackt“ werden

kann, muss es gewisse Anforderungen erfüllen und darf nicht zu einfach aufgebaut sein. Ungeeignete Passwörter sind z.B. das eigene Geburtsdatum, der Name der Frau bzw. des Mannes oder einfache Zahlenfolgen wie 12345.

***Schwierige Passwörter leicht zu merken**:*
Viele Internetnutzer stehen vor der Problematik sich zu viele Passwörter merken zu müssen. Immer dasselbe Passwort zu verwenden, wäre zu riskant. Ein so genannter Algorithmus kann dabei helfen, immer ein anderes Passwort zu haben, das sich aber einfach herleiten lässt.

Beispiel: Sie haben zwei feste Bestandteile eines Passworts. In diesem Falle ZEDAT 07. Wenn Sie beispielsweise einen Account bei Amozon anlegen, könnten sie zwischen ZEDAT und 07 noch ein zon einfügen. (ZEDATzon07). Das Passwort könnte noch komplizierter gemacht werden, wenn Sie die Buchstabenanzahl von Amazon auch noch einfügen würden.

Genauere Informationen finden Sie unter: http://www.fu-berlin.de/zuv/eas/it-sicherheit/Tipps/index.html

- **Zugriffsrechte (M1.12)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal (bereichsspezifisch)

Der Benutzer darf nur mit den Zugriffsrechten ausgestattet werden, die unmittelbar für die Erledigung seiner Aufgaben vorgesehen sind.
Im Bereich der Universitätsverwaltung erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer auf schriftlichen Antrag.

In allen anderen Organisationseinheiten sind die dort geltenden Regelungen zu beachten.

Kommentar:

Zugriffrechte werden vom Administrator bzw. von dem dafür verantwortlichen Mitarbeiter vergeben und bezeichnen die Möglichkeit, bestimmte Daten und Verfahren verwenden und bearbeiten (z.B. lesen, ausführen, ändern, löschen) zu dürfen. Jeder Benutzer wird mit den individuell zur Aufgabenerfüllung notwendigen Zugriffsrechten auf Daten, Verzeichnisse und weitere Ressourcen wie z.B. Drucker ausgestattet. Die „richtige" Vergabe von Zugriffsrechten soll verhindern, dass beispielsweise durch versehentliches Klicken Daten gelöscht oder verändert werden, ohne dass man es u. U. selbst bemerkt.

- **Netzzugänge (M1.13)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal , IT-Anwender

Der Anschluss von Systemen an das Datennetz der Freien Universität Berlin hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems o. ä.) ist unzulässig. Ausnahmen dürfen nur die zuständigen Rechenzentren der Freien Universität Berlin in Absprache mit dem IT-Verantwortlichen der Organisationseinheit und ggf. mit dem Datenschutzbeauftragten einrichten.

Kommentar:

Die Freie Universität Berlin versucht durch eine Reihe von organisatorischen und technischen Maßnahmen sicherheitskritische Ereignisse zu verhindern bzw. zu minimieren. So sind beispielsweise viele Netzbereiche an der Freien Universität Berlin durch verschiedene Firewall-Systeme untereinander, vom Campusnetz und vom Internet abgeschottet. Durch das eigenmächtige Installieren von Netzzugängen werden diese Sicherheitsmaßnahmen unterlaufen und damit unwirksam gemacht.

Beispiel: In einem besonders geschützten Verwaltungsnetz der Freien Universität Berlin ist der Zugang zum Internet gar nicht oder nur sehr eingeschränkt möglich. Alle Übergänge von diesem Verwaltungsnetz in andere Netzbereiche der Freien Universität Berlin oder ins Internet werden durch technische Einrichtungen kontrolliert. Um trotzdem einen ungehinderten Zugang ins World Wide Web zu erhalten, könnten findige Mitarbeiter auf die Idee kommen, den Computer über ein Modem und die vorhandenen Telefonanschlüsse mit dem Internet zu verbinden. Damit wäre eine klassische Hintertür geöffnet, durch die völlig unbeaufsichtigt und unkontrolliert Daten aller Art aus dem Internet in das geschützte Verwaltungsnetz fließen können und umgekehrt. Alle aufwändigen Sicherheitsmaßnahmen laufen damit ins Leere, da über die Modemleitung Computerviren und andere Schadprogramme ungehindert in den gesicherten Bereich eindringen und sich dort verbreiten können.

1.1.5. Kommunikationssicherheit

- **Sichere Netzwerknutzung (M1.14)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Der Einsatz von verschlüsselten Kommunikationsdiensten ist, nach Möglichkeit, den unverschlüsselten Diensten vorzuziehen. Schützenswerte Daten sollten verschlüsselt übertragen werden.

Kommentar:

Da sich das IT-Personal weniger mit der Verarbeitung von Daten, als vielmehr u. a. mit der Installation und Wartung der technischen Infrastruktur beschäftigt, kann die Bewertung der Daten hinsichtlich ihres Schutzbedarfs sowie die Einschätzung der Notwendigkeit zur Verschlüsselung häufig nur durch die Anwender erfolgen. Programme zur Verschlüsselung von Dateien und Ordnern können von dem zuständigen IT-Personal bereitgestellt werden.

Auch bei der elektronischen Kommunikation stehen meistens verschlüsselte Varianten zur Verfügung. Beispielsweise können E-Mails auch verschlüsselt versendet werden. Voraussetzung ist jedoch, dass sowohl Sender als auch Empfänger über ein Verschlüsselungsprogramm verfügen. Unverschlüsselte E-Mails können am ehesten mit einer Postkarte verglichen werden, denn jeder, der Netze abhören kann, kann auch fremde E-Mails problemlos lesen.

1.1.6. Datensicherung

- **Datensicherung (M1.15)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen o. ä. schützen. Grundsätzlich sind Daten auf zentralen Servern zu speichern. Ist die Sicherung auf zentralen Servern noch nicht möglich, ist der Benutzer für die Sicherung seiner Daten selbst verantwortlich.

Den in den jeweiligen Organisationseinheiten geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung ist Folge zu leisten.

Kommentar:

Das Speichern auf zentralen Servern hat den Vorteil, dass in der Regel von den dort gespeicherten Daten in regelmäßigen Abständen Sicherheitskopien erstellt werden, die im Falle eines Serverabsturzes bzw. Serverdefekts wieder eingespielt werden können. Der Anwender muss sich somit um die Sicherung seiner gespeicherten Dateien nicht mehr selbst kümmern. Im Gegensatz zur Datensicherung auf Servern, ist das dauerhafte Speichern von Daten auf dem Arbeitsplatz-PC nicht empfehlenswert. Im Falle eines Defekts der Festplatte gehen die dort gespeicherten Daten verloren, da es häufig nicht möglich ist, sie zu rekonstruieren. Aus Erfahrung ist bekannt, dass sich schwerwiegende Festplattenausfälle häufig vorher nicht ankündigen.

1.1.7. Umgang mit Datenträgern

- **Sichere Aufbewahrung (M1.16)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Mobile Datenträger mit schützenswerten Daten sind verschlossen und vor unbefugtem Zugriff geschützt aufzubewahren. Die Lagerungsbedingungen gemäß den Herstellerangaben sind einzuhalten. Insbesondere ist darauf zu achten, dass ein hinreichender Schutz gegen Hitze, Feuchtigkeit und magnetische Felder besteht.

Kommentar:

Beispiele:
Eine im Auto auf der Windschutzscheibe liegen gelassene CD wird durch direkte Sonneneinstrahlung einer großen Hitze ausgesetzt. Die Speicher- und Lesefähigkeit der CD kann dadurch beschädigt werden.

Ein auf dem Rücksitz eines Autos vergessener Laptop ist für Diebe geradezu einladend. Ein nicht von außen sichtbarer Ablageort, wie beispielsweise der Kofferraum, sollte bevorzugt werden.

- **Datenträgerkennzeichnung (M1.17)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Alle mobilen Datenträger, auf denen schützenswerte Daten dauerhaft gespeichert werden, sind soweit möglich eindeutig zu kennzeichnen. Aus der Beschriftung soll die Verwendung (Verfahren, Dateien, Inhalt), Datum der ersten Ingebrauchnahme sowie das Datum der ersten Ingebrauchnahme sowie das Datum des letztmaligen Beschreibens hervor gehen. Bei besonders schützenswerten Daten ist die Beschriftung so zu wählen, dass ein Rückschluss auf den Inhalt für Unbefugte nicht möglich ist.

Kommentar:

Diese Maßnahme zielt besonders auf die Speicherung von schützenswerten oder hoch schützenswerten Daten auf mobilen Datenträgern ab. Grundsätzlich soll mit der Umsetzung der Maßnahme sichergestellt werden, dass auch nach mehreren Monaten oder Jahren stets erkennbar ist, dass auf bestimmten Datenträgern hochsensible Daten gespeichert sind. Damit lässt sich beispielsweise verhindern, dass CDs mit vertraulichen Daten einfach weggeschmissen werden.

- **Gesicherter Transport (M1.18)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Die Übermittlung von Datenträgern mit schützenswerten Daten hat persönlich, per Kurier, per Wertbrief oder mit vergleichbaren Transportdiensten zu erfolgen. Während des Transports müssen sich die Datenträger in einem verschlossenen Behältnis befinden, dessen unbefugte Öffnung festgestellt werden kann. Die Weitergabe dieser Datenträger erfolgt nur gegen Quittung.

Kommentar:

Um Manipulationen und die unbefugte Einsichtnahme von Daten auf Datenträgern verhindern bzw. erkennen zu können, muss die Übermittlung der Datenträger auf einem der genannten Wege erfolgen. Vergleichbar ist dieses Vorgehen mit einem Beispiel aus dem alltäglichen Leben. Es soll ein wichtiges Dokument (z.B. Kündigung des Mietvertrages) versendet werden. Um in solch einem Fall sicherzustellen, dass das Kündigungsschreiben rechtzeitig den Empfänger erreicht, wählt man anstatt eines normalen Briefes entweder die Variante des Einschreibens mit Rückschein oder gibt die Unterlagen persönlich beim Vermieter ab.

- **Physisches Löschen von Datenträgern (M1.19)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Datenträger mit schützenswerten Daten müssen vor einer Weitergabe an nicht autorisierte Personen physisch gelöscht werden. Das kann mit geeigneten Programmen oder mit einem Gerät zum magnetischen Durchflutungslöschen erfolgen.

Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Vorzugsweise ist auch hier das Durchflutungslöschen und die daran anschließende mechanische Zerstörung anzuwenden.

Geeignete Werkzeuge und Anleitungen werden u. a. vom Rechenzentrum der Freien Universität Berlin bereitgestellt. Diese Aufgabe kann auch von geeigneten externen Dienstleistern erledigt werden.

Kommentar:

Bei unsachgemäßem Löschen besteht die Gefahr, dass Daten ausgelesen bzw. rekonstruiert werden können. Um das Bekannt werden dieser Daten auszuschließen, müssen Datenträger adäquat, wie in Maßnahme 1.19 geschildert, gelöscht werden. Der Begriff „Datenträger“ umfasst u. a. Disketten, CD-Roms, Festplatten, USB-Sticks, DVDs.

Beispiel: Eine ausgesonderte Festplatte wird vor der Entsorgung nicht oder nur unzureichend gelöscht. Über Umwege gelangt die Festplatte auf einer Auktionsplattform im Internet in den Verkauf. Mit etwas technischem Geschick ist der Käufer in der Lage, die auf der Festplatte gespeicherten Daten auszulesen. Nicht nur, dass bei Bekannt werden dieses Vorfalls die Freie Universität Berlin einen Ansehensverlust erleiden würde, auch hätte der Käufer Zugang zu Daten, die in Händen krimineller Dritter ggf. Schäden verursachen könnten.

1.1.8. Schützenswerte Daten

- **Schützenswerte Daten auf dem Arbeitsplatz-PC (M1.20)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Das Speichern schützenswerter Daten auf der Festplatte des Arbeitsplatz-PCs oder anderer lokaler Speicher- oder Übertragungsmedien und deren Übertragung ist nur verschlüsselt zulässig. Die Zugriffsrechte der verschlüsselten Dateien sind so zu setzen, dass Unbefugte keinen Zugriff erlangen können.

Kommentar:

Das oberste Ziel von IT-Sicherheitsmaßnahmen an der Freien Universität Berlin ist es, die Vertraulichkeit, Integrität (die Gewährleistung, dass die Daten nicht verändert wurden) und Verfügbarkeit der Daten sicherzustellen. Die Maßnahme zur Verschlüsselung von schützenswerten Daten, wie z.B. Personaldaten, dient dem Schutz der Daten vor unberechtigtem Zugriff, Bearbeitung und Manipulation.

Beispiel: Ein PC mit einem Windows-Betriebssystem bietet in der Regel keinen ausreichenden Schutz für besonders sensible Daten, die auf der Festplatte des PCs abgelegt sind. Jeder Benutzer, der im Besitz von Administratorrechten ist, kann auf alle Daten zugreifen, gleichgültig wer der Eigentümer der Daten ist. Darüber hinaus sind PCs unabhängig vom Betriebssystem keine besonders sicheren Aufbewahrungsorte für sensible Daten, da häufig die Möglichkeit besteht, dass mit Hilfe von externen Datenträgern der Rechner gebootet werden kann und anschließend alle unverschlüsselt gespeicherten Daten von der Festplatte auslesen werden können.

Sichere Entsorgung vertraulicher Papiere (M1.21)

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Papiere mit vertraulichem Inhalt (einschließlich Testausdrucke) sind mit Hilfe eines Aktenvernichters zu vernichten. Alternativ kann die Entsorgung auch zentral über einen Dienstleister erfolgen. Bei der Entsorgung über einen Dienstleister sind die universitären Regelungen zu beachten.

Kommentar:

Die unsachgemäße Vernichtung von vertraulichen Papieren kann zur Folge haben, dass unbefugte Dritte schützenswerte Daten einsehen können. Um die Vertraulichkeit der Daten sicherzustellen sowie die missbräuchliche Nutzung zu vermeiden, sollten z.B. weder Testausdrucke von Lohnbezügen der Mitarbeiter am Drucker liegen gelassen, noch Akten mit sensiblen Daten achtlos in den Papierkorb geworfen werden.

In bestimmten Bereichen der Freien Universität Berlin existieren speziell zu dieser Maßnahme bereichsinterne Regelungen (Arbeitsanweisungen), die die Art und Weise der Entsorgung festlegen. Diese Regelungen sind zusätzlich zu beachten.