B 3.203 Laptop

Beschreibung

Unter einem Laptop oder Notebook wird ein PC verstanden, der aufgrund seiner Bauart transportfreundlich ist und mobil genutzt werden kann. Ein Laptop hat eine kompaktere Bauform als Arbeitsplatzrechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden. Er verfügt über eine Festplatte und meist auch über weitere Speichergeräte wie ein Disketten-, CD-ROM- oder DVD-Laufwerke sowie über Schnittstellen zur Kommunikation über verschiedene Medien (beispielsweise Modem, ISDN, LAN, USB, Firewire, WLAN). Laptops können mit allen üblichen Betriebssystemen wie Windows oder Linux betrieben werden. Daher ist zusätzlich der betriebssystemspezifische Client-Baustein zu betrachten.

Typischerweise wird ein Laptop zeitweise allein, ohne Anschluss an ein Rechnernetz betrieben, und von Zeit zu Zeit wird er zum Abgleich der Daten sowie zur Datensicherung mit dem Behörden- oder Unternehmensnetz verbunden. Häufig wird er auch während der mobilen Nutzung über Modem direkt mit externen Netzen, insbesondere mit dem Internet, verbunden, so dass er indirekt als Brücke zwischen dem LAN und dem Internet wirken kann.

Die Einrichtungen zur Datenfernübertragung (über Modem, ISDN-Karte, etc.) werden hier nicht behandelt (siehe Baustein B 4.3). Für den Laptop wird vorausgesetzt, dass er innerhalb eines bestimmten Zeitraums nur von einem Benutzer gebraucht wird. Ein anschließender Benutzerwechsel wird berücksichtigt.

Gefährdungslage

Für den IT-Grundschutz eines Laptops werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:

-	G 1.2	Ausfall des IT-Systems
-	G 1.15	Beeinträchtigung durch wechselnde Einsatzumgebung

Organisatorische Mängel:

-	G 2.7	Unerlaubte Ausübung von Rechten
-	G 2.8	Unkontrollierter Einsatz von Betriebsmitteln
-	G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs

Menschliche Fehlhandlungen:

-	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
-	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
-	G 3.8	Fehlerhafte Nutzung des IT-Systems
-	G 3.38	Konfigurations- und Bedienungsfehler

-	G 3.76	Fehler bei der Synchronisation mobiler Endgeräte

Technisches Versagen:

-	G 4.9	Ausfall der internen Stromversorgung
-	G 4.13	Verlust gespeicherter Daten
-	G 4.22	Software-Schwachstellen oder -Fehler
-	G 4.19	Informationsverlust bei erschöpftem Speichermedium

-	G 4.52	Datenverlust bei mobilem Einsatz

Vorsätzliche Handlungen:

-	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
-	G 5.2	Manipulation an Daten oder Software
-	G 5.4	Diebstahl
-	G 5.9	Unberechtigte IT-Nutzung
-	G 5.18	Systematisches Ausprobieren von Passwörtern
-	G 5.21	Trojanische Pferde
-	G 5.22	Diebstahl bei mobiler Nutzung des IT-Systems
-	G 5.23	Computer-Viren
-	G 5.43	Makro-Viren
-	G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
-	G 5.123	Abhören von Raumgesprächen über mobile Endgeräte
-	G 5.124	Missbrauch der Informationen von mobilen Endgeräten

-	G 5.125	Unberechtigte Datenweitergabe über mobile Endgeräte
-	G 5.126	Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des Einsatzes von Laptops sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

1.	Richtlinien für die Nutzung von Laptops

	Um Laptops sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe M 2.36 *Geregelte Übergabe und Rücknahme eines tragbaren PC* sowie Baustein B 3.201 *Allgemeiner Client*).

	Darauf aufbauend ist die Laptop-Nutzung zu regeln und Sicherheitsrichtlinien dafür zu erarbeiten (siehe M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*). Dies umfasst beispielsweise, wer das System wann und wofür nutzen darf und ob und in welcher Weise ein Anschluss an das Unternehmens- bzw. Behördennetz gestattet wird. Ebenso ist zu regeln, ob und in welcher Form bei mobiler Nutzung eine direkte Verbindung des Laptops mit dem Internet zulässig ist.

2. Beschaffung von Laptops

Für die Beschaffung von Laptops müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden (siehe M 2.310 *Geeignete Auswahl von Laptops*).

3. Sichere Installation von Laptops

Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist notwendig, um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der Laptops auszuschließen. Die hier zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine, beispielsweise B 3.206 *Unix-System* oder B 3.209 *Client unter Windows XP* , zu realisieren.

Dabei ist die Maßnahme M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme* von besonderer Bedeutung, da bei Laptops ein relativ hohes Diebstahlsrisiko besteht und die normalen Funktionen der Zugangs- und Zugriffskontrolle ihre Wirksamkeit verlieren, wenn der Laptop unter der Kontrolle des Diebes steht.

4. Sichere Konfiguration der installierten Komponenten

	Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Die hier zu treffenden Maßnahmen sind ebenfalls abhängig vom eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine zu realisieren. Auch hier sind zusätzliche Maßnahmen erforderlich, wenn eine Trennung der Rechte mehrerer Benutzer erforderlich ist. Zu beachten ist auch die Maßnahme M 4.7 *Änderung voreingestellter Passwörter*, weil nur zu häufig jede Zugangskontrolle dadurch illusorisch ist, dass die verwendeten Passwörter allgemein bekannt sind.

5. Sicherer Betrieb von Laptops

	Eine der wichtigsten IT-Sicherheitsmaßnahmen beim Betrieb heutiger Laptops ist die Installation und permanente Aktualisierung eines Virenschutzprogramms. Laptops werden häufig über längere Zeit losgelöst vom Firmen- oder Behördennetz oder auch mit temporären Verbindungen zum Internet betrieben. Somit sind unter Umständen einerseits ihre Virendefinitionsdateien veraltet und sie sind andererseits einem hohen Infektionsrisiko ausgesetzt. Die im Baustein B 1.6 *Computer-Virenschutzkonzept* vorgesehenen Maßnahmen, vor allem die Maßnahme M 2.159 *Aktualisierung der eingesetzten Computer-Viren-Suchprogramme*, sind daher für Laptops ganz besonders wichtig. Diese Geräte können sonst bei Anschluss an ein Firmen- oder Behördennetz Infektionsquellen ersten Grades darstellen.

	Sofern Laptops bei mobiler Nutzung direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Laptops auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Soll ein Laptop, der direkt am Internet betrieben wurde, wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieser Laptop nicht infiziert ist. Erst wenn dies sichergestellt ist, darf der Anschluss an das lokale Netz erfolgen (siehe M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*). Dies gilt auch für den Fall, dass der Anschluss an das Unternehmens- bzw. Behördennetz über ein Virtual Private Network (VPN) erfolgt, da Viren auch über verschlüsselte Kommunikationsverbindungen weiter verbreitet werden können.

	Bei einem Wechsel zwischen netzgebundenem und mobilem Betrieb müssen die Datenbestände zwischen dem Server und dem Laptop synchronisiert werden. Es muss dabei gewährleistet werden, dass jederzeit erkennbar ist, ob sich die aktuellste Version der bearbeiteten Daten auf dem Laptop oder im Netz befindet (siehe M 4.235 *Abgleich der Datenbestände von Laptops*).

	Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sind bei Laptops vor allem organisatorische Maßnahmen notwendig. Die notwendigen Maßnahmen werden im Rahmen der Umsetzung des Bausteins B 1.9 *Hard- und Software-Management* realisiert und brauchen daher hier nicht weiter betrachtet zu werden. Um einen Überblick über die aktuell in das lokale Netz eingebundenen Laptops zu behalten und die Konfiguration aller Laptops jederzeit nachvollziehen zu können, ist eine zentrale Verwaltung dieser Geräte wichtig (siehe M 4.236 *Zentrale Administration von Laptops*).

	Weitere spezifische Maßnahmen für Einzelsysteme sind vor allem M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern* und M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen* .

	Je nach der in einem Gebäude oder Büroraum gegebenen physischen Sicherheit kann es auch sinnvoll oder sogar notwendig sein, die Maßnahme M 1.46 *Einsatz von Diebstahl-Sicherungen* umzusetzen. Bei mobiler Nutzung ist in jedem Fall die Maßnahme M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz* anzuwenden, um den Laptop vor Diebstahl zu schützen.

6.	Aussonderung

	Bei Übergabe von Laptops an andere Benutzer, sei es im Rahmen des normalen Betriebs oder auch bei ihrer Aussonderung, ist darauf zu achten, dass keine schützenswerten Informationen mehr auf der Festplatte vorhanden sind. Hier sind vor allem die Maßnahmen M 2.36 *Geregelte Übergabe und Rücknahme eines tragbaren PC* sowie gegebenenfalls auch M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops* zu beachten.

7.	Datensicherung von Laptops

	Die Vorgehensweise und der erforderliche Umfang der Datensicherung richten sich nach dem Einsatzszenario des Laptops (siehe Maßnahme M 6.71 *Datensicherung bei mobiler Nutzung des IT-Systems*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Laptop" vorgestellt.

Planung und Konzeption

-	M 2.36	(B)	Geregelte Übergabe und Rücknahme eines tragbaren PC
-	M 2.218	(Z)	Regelung der Mitnahme von Datenträgern und IT-Komponenten
-	M 2.309	(A)	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
-	M 4.29	(Z)	Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme

Beschaffung

-	M 2.310	(A)	Geeignete Auswahl von Laptops

Umsetzung

-	M 4.40	(A)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons

Betrieb

-	M 1.33	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
-	M 1.34	(A)	Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
-	M 1.35	(Z)	Sammelaufbewahrung tragbarer IT-Systeme
-	M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
-	M 4.3	(A)	Regelmäßiger Einsatz eines Viren-Suchprogramms
-	M 4.27	(A)	Zugriffsschutz am Laptop
-	M 4.28	(Z)	Software-Reinstallation bei Benutzerwechsel eines Laptops
-	M 4.31	(A)	Sicherstellung der Energieversorgung im mobilen Einsatz
-	M 4.235	(B)	Abgleich der Datenbestände von Laptops
-	M 4.236	(Z)	Zentrale Administration von Laptops
-	M 4.255	(A)	Nutzung von IrDA-Schnittstellen
-	M 5.91	(A)	Einsatz von Personal Firewalls für Internet-PCs
-	M 5.121	(A)	Sichere Kommunikation von unterwegs
-	M 5.122	(A)	Sicherer Anschluss von Laptops an lokale Netze

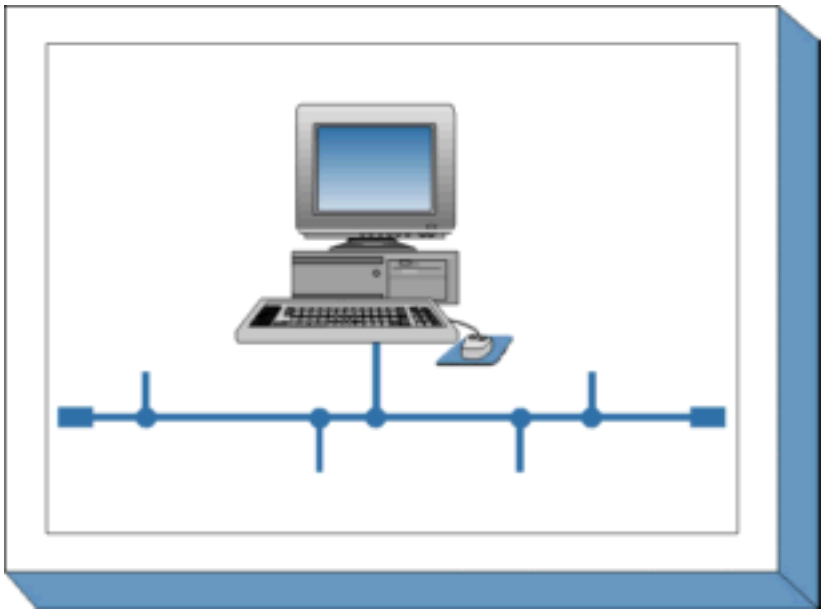
Aussonderung

-	M 2.306	(B)	Verlustmeldung

Notfallvorsorge

-	M 6.71	(A)	Datensicherung bei mobiler Nutzung des IT-Systems

B 3.201 Allgemeiner Client



Beschreibung

Betrachtet wird ein IT-System mit einem beliebigen Betriebssystem, das die Trennung von Benutzern zulässt (es sollte mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können). Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben.

Das IT-System kann auf einer beliebigen Plattform betrieben werden, es kann sich dabei um einen PC mit oder ohne Festplatte, aber auch um eine Unix-Workstation oder einen Apple Macintosh handeln. Das IT-System kann über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist.

Dieser Baustein bietet einen Überblick über Gefährdungen und IT-Sicherheitsmaßnahmen, die für alle Clients unabhängig von der verwendeten Plattform und vom eingesetzten Betriebssystem

zutreffen. Je nach dem eingesetzten Betriebssystem sind zusätzlich die weiterführenden Bausteine der IT-Grundschutz-Kataloge (zum Beispiel B 3.206 *Unix-System*) zu beachten.

Gefährdungslage

Für den IT-Grundschutz eines allgemeinen Clients werden folgende Gefährdungen angenommen:

Organisatorische Mängel:

-	G 2.1	Fehlende oder unzureichende Regelungen
-	G 2.7	Unerlaubte Ausübung von Rechten
-	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern
-	G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
-	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
-	G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen

Menschliche Fehlhandlungen:

-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
-	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
-	G 3.8	Fehlerhafte Nutzung des IT-Systems
-	G 3.9	Fehlerhafte Administration des IT-Systems
-	G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel

Technisches Versagen

-	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
-	G 4.13	Verlust gespeicherter Daten

Vorsätzliche Handlungen:

-	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
-	G 5.2	Manipulation an Daten oder Software
-	G 5.4	Diebstahl

-	G 5.7	Abhören von Leitungen
-	G 5.9	Unberechtigte IT-Nutzung
-	G 5.20	Missbrauch von Administratorrechten
-	G 5.21	Trojanische Pferde
-	G 5.23	Computer-Viren
-	G 5.40	Abhören von Räumen mittels Rechner mit Mikrofon
-	G 5.43	Makro-Viren
-	G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
-	G 5.85	Integritätsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz von Arbeitsplatzrechnern sollten im Hinblick auf die IT-Sicherheit von Clients folgende Schritte durchlaufen werden:

Planung des Einsatzes von Clients

Für die sichere Nutzung von IT-Systemen müssen vorab die Rahmenbedingungen festgelegt werden. Dabei müssen die Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie die geplanten Einsatzszenarien von Anfang an mit einbezogen werden (siehe M 2.321 *Planung des Einsatzes von Client-Server-Netzen*). Schon vor der Beschaffung der Rechner und Software sollte eine Sicherheitsrichtlinie für die Clients erstellt werden (siehe M 2.322 *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz*).

Übergreifende Fragen der sicheren Nutzung von IT-Systemen werden im Baustein B 1.9 *Hard- und Software-Management* betrachtet.

Beschaffung

Für die Beschaffung von Clients, die typischerweise in größeren Mengen erfolgt, müssen ausgehend von den Einsatzszenarien Kriterien für die Auswahl geeigneter Produkte formuliert werden (siehe hierzu B 1.10 *Standardsoftware*). Auch bei der Beschaffung von Einzelsystemen ist es wichtig, dass das System zur vorhandenen Struktur passt, damit nicht für ein einzelnes System wegen dessen Besonderheiten ein unangemessen hoher Aufwand bei Integration und Betrieb entsteht.

Falls Hard- oder Software nicht die festgelegten Sicherheitsanforderungen erfüllen, sind weitere Maßnahmen erforderlich. Diese können organisatorischer Art sein (beispielsweise durch Regelungen, dass der Client ausschließlich hinter verschlossener Bürotür betrieben werden darf) oder es können Zusatzkomponenten beschafft werden, um die identifizierten Mankos auszugleichen (siehe hierzu M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*).

Bei besonders hohen Anforderungen an die Verfügbarkeit der Clients ist für diese der Einsatz einer Unterbrechungsfreien Stromversorgung (USV) empfehlenswert. Dabei kann es sich

beispielsweise um eine "Einzelplatz-USV" handeln, falls die hohen Anforderungen nur für einzelne Clients gelten, oder aber um einen eigenen entsprechend abgesicherten Stromkreis ("rote Steckdose"). Weitere Informationen finden sich in M 1.28 *Lokale unterbrechungsfreie Stromversorgung* .

Umsetzung

Um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der IT-Systeme auszuschließen, sind eine sorgfältige Auswahl der Betriebssystem- und Softwarekomponenten, eine sichere Installation und sorgfältige Konfiguration wichtig. Die dabei zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem. Näheres dazu findet sich deswegen in spezifischen Bausteinen, beispielsweise in B 3.204 *Client unter Unix* oder B 3.205 *Client unter Windows NT* .

-	Sichere Installation

	Der Grundstein für die Sicherheit wird bereits bei der Vorbereitung der Installation gelegt. Vor der Installation sollte festgelegt werden, welche Komponenten des Betriebssystems und welche Anwendungsprogramme und Tools installiert werden sollen. Die getroffenen Entscheidungen müssen so dokumentiert werden, dass gegebenenfalls nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für das System gewählt wurde (siehe M 4.237 *Sichere Grundkonfiguration eines IT-Systems*).

	Für die Installation sollten nur Installationsmedien benutzt werden, die aus einer sicheren Quelle stammen (beispielsweise direkt vom Hersteller oder Distributor des Betriebssystems oder Programms). Die Installation des Betriebssystems sollte wenn möglich durchgeführt werden, ohne dass das System an das Netz angeschlossen ist (Offline-Installation). Falls bei der Installation Teile der Pakete über das Netz geladen werden sollen, sollte für die Installation ein eigenes Netz (Testnetz) genutzt werden, das vom übrigen Netz getrennt ist. Von einem Nachladen von Paketen über das Internet wird dringend abgeraten. Falls es in Ausnahmefällen erforderlich ist, ein System direkt im Produktionsnetz zu installieren, so muss durch geeignete zusätzliche Maßnahmen sichergestellt werden, dass auf das System während der Installation nicht von außen zugegriffen werden kann.

	Bereits im Verlauf der Installation werden meist einige Grundeinstellungen zur Systemkonfiguration (unterschiedlich je nach Betriebssystem) vorgenommen.

-	Sichere Konfiguration

	An die eigentliche Installation schließt sich die Grundkonfiguration eines Clients an. In dieser Phase wird die vorläufige Konfiguration, wie sie im Verlauf der Installation vom Installationsprogramm eingerichtet wurde, an die tatsächlichen Gegebenheiten und Anforderungen des IT-Verbunds angepasst, in dem der Client eingesetzt werden soll. Oft werden dabei weitere Programme installiert oder es werden Programme aus einer Standardkonfiguration entfernt, die Einstellungen für den Zugriff auf das Netz werden festgelegt und der Client wird für den Zugriff auf Verzeichnisdienste oder ähnliches konfiguriert. Außerdem werden nicht benötigte Benutzer-Kennungen gelöscht oder deaktiviert, und die Benutzer-Kennungen für die eigentlichen Benutzer werden angelegt.

	In dieser Phase werden auch die benötigten Anwendungsprogramme installiert und konfiguriert. Für die Installation und Konfiguration der Anwendungsprogramme sind analoge Sicherheitsaspekte wie für die Installation des Betriebssystems selbst zu beachten.

	Falls eine größere Anzahl ähnlich konfigurierter Clients installiert und konfiguriert werden soll, so bietet es sich an, dies nicht für jeden Client einzeln durchzuführen, sondern eine "generische" Installation zu erstellen, die anschließend auf die einzelnen Clients übertragen wird, und an der nur noch minimale Änderungen vor der Inbetriebnahme erforderlich sind. Eine solche generische Konfiguration kann erheblich zur Effizienz beitragen und das Risiko von Fehlern verringern helfen. Andererseits ist bei der Erstellung der Referenzinstallation besondere Sorgfalt erforderlich. Die vorgenommenen Einstellungen müssen nachvollziehbar dokumentiert sein.

	Ein wichtiger Grundsatz bei der Konfiguration von Clients ist, dass normale Bedienungsfehler der Anwender zu keinen gravierenden Schäden am System und an Daten anderer Benutzer führen sollten, und dass Anwender nicht durch einfache Neugierde Zugriff auf Informationen erlangen dürfen, die nicht für sie bestimmt sind. Mehr dazu findet sich in M 4.237 *Sichere Grundkonfiguration eines IT-Systems* .

	Nachdem der Client fertig konfiguriert ist, kann der Rechner an die Anwender übergeben werden. Falls die Anwender keine ausreichenden Kenntnisse des eingesetzten Betriebssystems, einzelner Anwendungsprogramme oder Tools besitzen, so müssen sie vorab geschult werden. Allgemeine Aspekte hierzu finden sich im Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung* .

Betrieb

Eine der wichtigsten IT-Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme ist es, die Systeme durch zeitnahes Einspielen von Sicherheitspatches stets auf einem aktuellen Stand zu halten (siehe M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*), sowie die Installation und permanente Aktualisierung eines Virenscanners (siehe dazu auch B 1.6 *Computer-Virenschutzkonzept*). Daneben ist eine regelmäßige Datensicherung (siehe auch B 1.4 *Datensicherungskonzept*) eine grundlegende Voraussetzung dafür, dass Hardwaredefekte und Programm- oder Benutzerfehler nicht zu gravierenden Datenverlusten führen.

Ein Mittel zur Erkennung von Angriffen oder missbräuchlicher Nutzung ist die Überwachung des Systems. Dafür relevante Maßnahmen finden sich in M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes* , sowie im Baustein B 1.9 *Hard- und Software-Management* .

Auch bei Clients ist es wichtig, dass die Administration auf sicheren Wegen erfolgt und dass die Arbeit der Administratoren nachvollziehbar ist. Die entsprechenden Aspekte sind in M 4.234 *Aussonderung von IT-Systemen* .

Aussonderung

Bei der Aussonderung eines Clients muss zunächst sichergestellt werden, dass alle Benutzerdaten gesichert oder auf ein Ersatzsystem übertragen werden. Anschließend muss dafür gesorgt werden, dass keine sensitiven Daten auf den Festplatten des Rechners zurück bleiben. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder ein reines logisches Löschen noch das Neuformatieren der Platten mit den Mitteln des installierten Betriebssystems die Daten wirklich von den Festplatten entfernt. Mit geeigneter Software können Daten, die auf diese Weise gelöscht wurden wieder rekonstruiert

werden, oft sogar ohne großen Aufwand. Hinweise zum sicheren Löschen finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* , die im Rahmen des übergeordneten Bausteins B 1.1 *Organisation* behandelt wird, und in M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung* . Nach der Aussonderung eines Clients müssen Bestandsverzeichnisse und Netzpläne aktualisiert werden.

Notfallvorsorge

Das notwendige Maß an Notfallvorsorge für einen allgemeinen Client ist stark vom individuellen Einsatzszenario abhängig. Oft wird als Notfallvorsorge für einen Client eine regelmäßige Datensicherung (siehe M 6.32 *Regelmäßige Datensicherung*) und das Erstellen eines bootfähigen Datenträgers für Notfälle (siehe M 6.24 *Erstellen eines Notfall-Bootmediums*) ausreichend sein. Für Clients mit besonderen Anforderungen an die Verfügbarkeit kann es sinnvoll sein, weitere Maßnahmen zu ergreifen, beispielsweise ein Austauschsystem bereit zu halten.

Abhängig vom eingesetzten Betriebssystem sind bei der Anwendung dieses Bausteins gegebenenfalls weitere Maßnahmen erforderlich. Diese finden sich in den jeweiligen Bausteinen.

Für den allgemeinen Client sind folgende Maßnahmen umzusetzen:

Planung und Konzeption

-	M 2.22	(A)	Hinterlegen des Passwortes
-	M 2.23	(Z)	Herausgabe einer PC-Richtlinie
-	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
-	M 2.321	(A)	Planung des Einsatzes von Client-Server-Netzen
-	M 2.322	(A)	Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz

-	M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz

Umsetzung

-	M 2.25	(A)	Dokumentation der Systemkonfiguration
-	M 4.237	(A)	Sichere Grundkonfiguration eines IT-Systems

Betrieb

-	M 2.273	(A)	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
-	M 3.18	(A)	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
-	M 4.2	(A)	Bildschirmsperre
-	M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
-	M 4.4	(C)	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
-	M 4.40	(A)	Verhinderung der unautorisierten Nutzung des Rechnermikrofons
-	M 4.41	(C)	Einsatz angemessener Sicherheitsprodukte für IT-Systeme
-	M 4.93	(B)	Regelmäßige Integritätsprüfung
-	M 4.200	(Z)	Umgang mit USB-Speichermedien
-	M 4.236	(Z)	Zentrale Administration von Laptops
-	M 4.238	(A)	Einsatz eines lokalen Paketfilters
-	M 4.241	(A)	Sicherer Betrieb von Clients
-	M 4.242	(Z)	Einrichten einer Referenzinstallation für Clients
-	M 5.45	(B)	Sicherheit von WWW-Browsern

Aussonderung

-	M 4.234	(A)	Aussonderung von IT-Systemen
-	M 2.323	(A)	Geregelte Außerbetriebnahme eines Clients

Notfallvorsorge

-	M 6.24	(A)	Erstellen eines Notfall-Bootmediums
-	M 6.32	(B)	Regelmäßige Datensicherung

3.209 Client unter Windows XP

Beschreibung

Betrachtet werden Arbeitsplatz-PCs (APCs) mit dem Betriebssystem Windows XP Professional. Windows XP ist das Nachfolgeprodukt von Windows 2000 Professional. Die Sicherheit eines solchen Betriebssystems spielt eine wichtige Rolle für die Sicherheit in einem IT-Verbund, da Schwachstellen auf der Betriebssystemebene die Sicherheit aller Anwendungen und des gesamten Netzes beeinträchtigen können. Der vorliegende Baustein beschreibt die Sicherheitsmaßnahmen, die für einen APC mit Windows XP umzusetzen sind. Die Maßnahmen beziehen sich insbesondere auf die Planung und den Betrieb eines Windows XP Clients in einer Domänenumgebung, auf Installationen von Windows XP auf Einzelplatzrechnern wird nur am Rande eingegangen. Die serverspezifischen Sicherheitsmaßnahmen, die beim Betrieb der Clients in einer Domänenumgebung relevant sind, sind in den Server-Bausteinen der Schicht 3 beschrieben (siehe z. B. Baustein B 3.106 *Server unter Windows 2000*).

Gefährdungslage

Wie jedes IT-System sind auch Clients unter Microsoft Windows XP vielfältigen Gefährdungen ausgesetzt. Oft nutzen erfolgreiche Angriffe Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten aus. Daher kommt der korrekten Konfiguration des Systems und seiner Komponenten eine wichtige Rolle zu. Generell gilt, dass die Gefährdungslage einzelner Rechner immer auch vom Einsatzszenario abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen. Es ist zu beachten, dass bei nicht vernetzten PCs alle Angriffe (siehe "Vorsätzliche Handlungen") den lokalen Zugang zum Gerät (Konsole) erfordern.

Für den IT-Grundschutz einzelner PCs unter dem Betriebssystem Windows XP werden folgende typische Gefährdungen angenommen.

Höhere Gewalt:

-	G 1.1	Personalausfall
-	G 1.2	Ausfall des IT-Systems
-	G 1.4	Feuer
-	G 1.5	Wasser
-	G 1.8	Staub, Verschmutzung

Organisatorische Mängel:

-	G 2.7	Unerlaubte Ausübung von Rechten
-	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

Menschliche Fehlhandlungen:

-	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen

-	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
-	G 3.8	Fehlerhafte Nutzung des IT-Systems
-	G 3.9	Fehlerhafte Administration des IT-Systems
-	G 3.22	Fehlerhafte Änderung der Registrierung
-	G 3.48	Fehlkonfiguration von Windows 2000/XP Rechnern

Technisches Versagen:

-	G 4.1	Ausfall der Stromversorgung

-	G 4.7	Defekte Datenträger
-	G 4.8	Bekanntwerden von Softwareschwachstellen
-	G 4.23	Automatische CD-ROM-Erkennung

Vorsätzliche Handlungen:

-	G 5.2	Manipulation an Daten oder Software
-	G 5.4	Diebstahl
-	G 5.7	Abhören von Leitungen
-	G 5.9	Unberechtigte IT-Nutzung
-	G 5.18	Systematisches Ausprobieren von Passwörtern
-	G 5.21	Trojanische Pferde
-	G 5.23	Computer-Viren
-	G 5.43	Makro-Viren
-	G 5.52	Missbrauch von Administratorrechten im Windows NT/2000/XP System
-	G 5.71	Vertraulichkeitsverlust schützenswerter Informationen

-	G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
-	G 5.83	Kompromittierung kryptographischer Schlüssel
-	G 5.85	Integritätsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Die in den folgenden Listen mit dem Zusatz "optional" gekennzeichneten Maßnahmen gehen zumindest teilweise über den IT-Grundschutz hinaus, oder sie beziehen sich auf spezielle Einsatzumgebungen. Sie sind dann zu realisieren, wenn die betreffenden Einsatzbedingungen gegeben sind, insbesondere dann, wenn mehrere Benutzer mit demselben System arbeiten und gegeneinander geschützt werden sollen bzw. wenn die Kontrolle sicherheitskritischer Funktionen nicht beim Benutzer selbst liegt, sondern zentral verwaltet werden soll.

Aufgrund der oben aufgeführten besonderen Gefährdungen für vernetzte Geräte werden einige Maßnahmen ausdrücklich herausgestellt. Vor allem Maßnahmen zum Schutz gegen Angriffe aus dem Netz müssen hierbei sorgfältig durchgeführt werden. Eine effiziente, zentralisierte Verwaltung der Clients leistet einen wichtigen Beitrag zur Aufrechterhaltung eines hohen Sicherheitsstandards. Einheitliche Konfigurationsvorgaben erleichtern die Überwachung von ungewollten Änderungen der Konfiguration, Änderungen der Sicherheitsvorgaben können schneller auf allen Clients wirksam werden und Softwareaktualisierungen können schneller verteilt werden. Die Mehrzahl der empfohlenen Maßnahmen aus dem Bereich Hardware/ Software lassen sich mit zentral vorgegebenen Gruppenrichtlinien umsetzen. Wenn in der Organisation der Einsatz von Microsoft

Active Directory vorgesehen ist, muss dieser Einsatz gründlich geplant werden.

Einen Sonderfall stellt die Verwaltung von Windows XP Clients in Windows NT Domänenumgebungen dar. In diesem Fall stehen als Werkzeug zur zentralen Verwaltung nur die Windows NT Systemrichtlinien zur Verfügung. In der Maßnahme M 4.51 *Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT* werden die Möglichkeiten der Systemadministration mit Windows NT Systemrichtlinien erläutert. Aufgrund der technischen Beschränkungen dieser Lösung wird der Einsatz von Systemrichtlinien für Windows XP jedoch nicht empfohlen. Für die Verwaltung von Clients unter Windows XP sollte der Einsatz von Active Directory Gruppenrichtlinien erwogen werden.

Clients unter Windows XP können anstatt in Domänen auch in Arbeitsgruppen verwendet werden. Die Verwaltung sämtlicher Sicherheitsmerkmale erfolgt in diesem Fall lokal auf jedem einzelnen Client. Freigegebene Ressourcen auf einzelnen Rechnern lassen sich nur schwer zentral verwalten und überwachen. Ein Problem stellt auch die Datensicherung dar. Aufgrund der Vernetzung können jedoch einige netzbasierte Maßnahmen angewendet werden, z. B. die Verwendung von Sicherheitsvorlagen zur Konfiguration und die automatische Aktualisierung des Betriebssystems mithilfe des Software Update Service. Weitere Ausführungen zu diesem Einsatz-Szenario enthält der Baustein B 5.1 *Peer-to-Peer-Dienste* .

Für die erfolgreiche und sichere Konfiguration von Clients unter Windows XP sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Nach der Entscheidung, Windows XP als Client-Betriebssystem einzusetzen, sollte zunächst der Einsatz geplant werden (siehe Maßnahme M 2.324 *Einführung von Windows XP planen*). Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.325 *Planung der Windows XP Sicherheitsrichtlinie*), die einerseits die bereits bestehenden Sicherheitsrichtlinien im Windows XP-Kontext umsetzt und andererseits die für Windows XP spezifischen Erweiterungen definiert.

In einer vernetzten Umgebung wird der Einsatz eines zentralen Verwaltungssystems empfohlen. Hierfür kann z. B. Microsoft Active Directory zum Einsatz kommen. Insbesondere die Verwendung von Gruppenrichtlinien ermöglicht eine relativ einfache zentrale Umsetzung von Sicherheitsvorgaben. Beim Betrieb eines Windows XP Einzelsystems ist der Einsatz lokaler Gruppenrichtlinien empfehlenswert. Die Maßnahme M 2.326 *Planung der Windows XP Gruppenrichtlinien* enthält die entsprechenden Empfehlungen zum Einsatz von Gruppenrichtlinien zur Konfiguration und Verwaltung eines Windows XP Systems.

Weitere Aspekte müssen in der Planungsphase berücksichtigt werden. Diese betreffen vor allem die sichere Konfiguration eines Windows XP Systems. Folgende Maßnahmen sind hierfür relevant:

-	M 4.244	Sichere Windows XP Systemkonfiguration
-	M 4.245	Basiseinstellungen für Windows XP GPOs
-	M 4.246	Konfiguration der Systemdienste unter Windows XP
-	M 5.123	Absicherung der Netzwerkkommunikation unter Windows XP
-	M 4.247	Restriktive Berechtigungsvergabe unter Windows XP

Wird in einem Unternehmen bzw. einer Behörde der Einsatz von

Windows XP spezifischen Fernzugriffsmöglichkeiten beabsichtigt, so müssen in der Planungsphase die entsprechenden Technologien ausgewählt und damit verbundene Sicherheitsaspekte evaluiert werden (siehe dazu die Maßnahme M 2.327 *Sicherheit beim Fernzugriff unter Windows XP*).

Soll Windows XP zum Einsatz auf mobilen Rechnern kommen, so müssen bereits in der Planungsphase spezifische Sicherheitsaspekte berücksichtigt werden. Die Maßnahme M 2.328 *Einsatz von Windows XP auf mobilen Rechnern* fasst die für Windows XP spezifischen Aspekte zusammen.

Windows XP bietet einige Verwaltungswerkzeuge an, die bereits in der Planungs- bzw. Testphase helfen können, Konfigurationsfehler zu vermeiden, was zweifellos einen Sicherheitsgewinn bringt.

Die Maßnahme M 4.243 *Windows XP Verwaltungswerkzeuge* fasst die wichtigsten Werkzeuge zusammen.

Umsetzung

In der Umsetzungsphase werden alle Maßnahmen ergriffen, die den sicheren Betrieb vorbereiten und gewährleisten. Dazu zählen insbesondere Maßnahmen zur Sicherheit bei der Installation und Grundkonfiguration des Systems.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation von Windows XP Systemen erfolgen. Die Installation muss mit besonderer Sorgfalt durchgeführt werden. In M 4.248 *Sichere Installation von Windows XP* sind die relevanten Empfehlungen zusammengefasst. Die für die Konfiguration eines Windows XP Systems zu beachtenden Aspekte müssen während der Planungsphase ermittelt worden sein.

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind

dabei folgende Aspekte zu beachten:

-	Ein Windows XP System ändert sich in der Regel täglich. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei zu beachtenden Aspekte sind in M 4.146 *Sicherer Betrieb von Windows 2000/XP* zusammengefasst.

-	Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Windows XP Netzes ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Maßnahmen finden sich in M 4.148 *Überwachung eines Windows 2000/XP Systems* . Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle.

-	Windows XP Systeme sind wie auch andere IT-Systeme den allgemeinen Sicherheitsrisiken ausgesetzt. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs entschieden zu verringern, müssen Windows XP Systeme aktuell gehalten werden. Die entsprechenden Empfehlungen sind in M 4.249 *Windows XP Systeme aktuell halten* zu finden.

-	Für die bereits im Betrieb befindlichen Windows XP Systeme müssen die aus dem Einspielen des Service Packs 2 resultierende Auswirkungen berücksichtigt werden (siehe dazu M 2.329 *Einführung von Windows XP SP2*).

-	Eine regelmäßige Prüfung der geltenden Sicherheitseinstellungen und generell der existierenden Sicherheitsrichtlinien ist maßgebend für die Sicherheit der Windows XP Systeme im laufenden Betrieb. Die dabei zu beachtenden Aspekte sind in M 2.330 *Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung* zusammengefasst.

-	Windows XP bietet einige Verwaltungswerkzeuge an, deren Einsatz auch aus Sicherheitssicht empfehlenswert ist, da mit ihrer Hilfe unter anderem auch Konfigurationsfehler vermieden werden können. Im Weiteren sind diese Werkzeuge bei der Fehleranalyse bzw. bei der Revision nützlich (siehe dazu M 4.243 *Windows XP Verwaltungswerkzeuge*).

Aussonderung / Stilllegung

Wenn ein Windows XP APC stillgelegt wird, ist dafür Sorge zu tragen, dass die gespeicherten Daten nicht in falsche Hände geraten oder missbräuchlich verwendet werden können. Zu den gespeicherten Daten gehören auch Passwörter, Cookies, temporäre Internetdateien usw. Gleichzeitig ist zu beachten, dass bei Archivierung der Daten der Zugriff erhalten bleibt, auch wenn beispielsweise der bisherige Benutzer eines APCs die Organisation verlassen hat. Die gleichen Anforderungen gelten, wenn ein APC von einem Benutzer zu einem anderen Benutzer umgesetzt wird.

Notfallvorsorge

Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich in M 6.76 *Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes* . Hinweise zur Datensicherung sind in M 6.78 *Datensicherung unter Windows 2000/XP* enthalten.

Maßnahmenbündel

Nachfolgend wird das Maßnahmenbündel für den Baustein "Windows XP Client" vorgestellt.

Planung und Konzeption

-	M 2.324	(A)	Einführung von Windows XP planen

-	M 2.325	(A)	Planung der Windows XP Sicherheitsrichtlinie
-	M 2.326	(A)	Planung der Windows XP Gruppenrichtlinien
-	M 2.327	(B)	Sicherheit beim Fernzugriff unter Windows XP
-	M 2.328	(B)	Einsatz von Windows XP auf mobilen Rechnern
-	M 3.28	(A)	Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
-	M 4.48	(A)	Passwortschutz unter Windows NT/2000/ XP
-	M 4.57	(A)	Deaktivieren der automatischen CD-ROM-Erkennung
-	M 4.75	(A)	Schutz der Registrierung unter Windows NT/2000/XP
-	M 4.147	(Z)	Sichere Nutzung von EFS unter Windows 2000/XP
-	M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP
-	M 4.243	(Z)	Windows XP Verwaltungswerkzeuge
-	M 4.244	(A)	Sichere Windows XP Systemkonfiguration
-	M 4.245	(A)	Basiseinstellungen für Windows XP GPOs
-	M 4.246	(A)	Konfiguration der Systemdienste unter Windows XP
-	M 4.247	(A)	Restriktive Berechtigungsvergabe unter Windows XP
-	M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
-	M 5.89	(A)	Konfiguration des sicheren Kanals unter Windows 2000/XP
-	M 5.90	(Z)	Einsatz von IPSec unter Windows 2000/ XP

-	M 5.123	(B)	Absicherung der Netzwerkkommunikation unter Windows XP

Umsetzung

-	M 2.32	(Z)	Einrichtung einer eingeschränkten Benutzerumgebung
-	M 4.248	(A)	Sichere Installation von Windows XP

Betrieb

-	M 2.329	(A)	Einführung von Windows XP SP2
-	M 2.330	(B)	Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung
-	M 4.49	(A)	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
-	M 4.52	(A)	Geräteschutz unter Windows NT/2000/ XP
-	M 4.146	(A)	Sicherer Betrieb von Windows 2000/XP
-	M 4.148	(B)	Überwachung eines Windows 2000/XP Systems
-	M 4.249	(A)	Windows XP Systeme aktuell halten

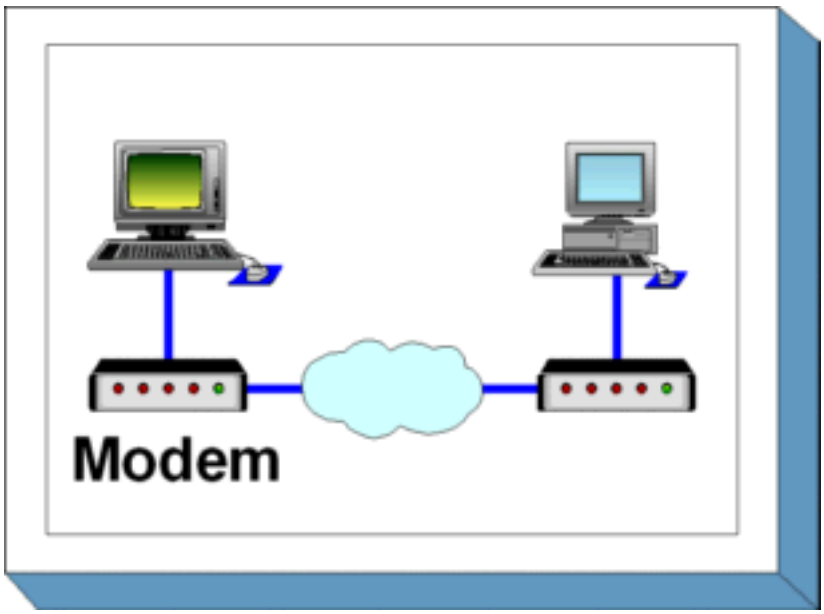
Aussonderung / Stilllegung

-	M 4.56	(C)	Sicheres Löschen unter Windows-Betriebssystemen

Notfallvorsorge

-	M 6.76	(C)	Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
-	M 6.78	(A)	Datensicherung unter Windows 2000/XP

B 4.3 Modem



Beschreibung

Über ein Modem wird eine Datenendeinrichtung, z. B. ein PC, über das öffentliche Telefonnetz mit anderen Datenendeinrichtungen verbunden, um Informationen austauschen zu können. Ein Modem wandelt die digitalen Signale aus der Datenendeinrichtung in analoge elektrische Signale um, die über das Telefonnetz übertragen werden können. Damit zwei IT-Systeme über Modem kommunizieren können, muss auf den IT-Systemen die entsprechende Kommunikationssoftware installiert sein.

Unterschieden werden externe, interne und PCMCIA-Modems. Ein externes Modem ist ein eigenständiges Gerät mit eigener Stromversorgung, das üblicherweise über eine serielle Schnittstelle mit dem IT-System verbunden wird. Als internes Modem werden Steckkarten mit Modem-Funktionalität, die über keine eigene Stromversorgung verfügen, bezeichnet. Ein PCMCIA-Modem ist eine scheckkartengroße Einsteckkarte, die über eine PCMCIA-Schnittstelle üblicherweise in Laptops eingesetzt wird.

In diesem Baustein wird Datenübertragung über ISDN nicht betrachtet, dazu siehe die Bausteine B 3.401 *TK-Anlage* und B 4.5

LAN-Anbindung eines IT-Systems über ISDN .

Gefährdungslage

In diesem Kapitel werden für den IT-Grundschutz beim Einsatz eines Modems folgende Gefährdungen angenommen:

Höhere Gewalt:

-	G 1.2	Ausfall des IT-Systems

Menschliche Fehlhandlungen:

-	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
-	G 3.5	Unbeabsichtigte Leitungsbeschädigung

Technisches Versagen:

-	G 4.6	Spannungsschwankungen/ Überspannung/Unterspannung

Vorsätzliche Handlungen:

-	G 5.2	Manipulation an Daten oder Software
-	G 5.7	Abhören von Leitungen
-	G 5.8	Manipulation an Leitungen
-	G 5.9	Unberechtigte IT-Nutzung
-	G 5.10	Missbrauch von Fernwartungszugängen
-	G 5.12	Abhören von Telefongesprächen und Datenübertragungen
-	G 5.18	Systematisches Ausprobieren von Passwörtern

-	G 5.23	Computer-Viren
-	G 5.25	Maskerade
-	G 5.39	Eindringen in Rechnersysteme über Kommunikationskarten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz eines Modems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Beschaffung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Schon vor dem Einsatz eines Modems sollte geprüft werden, ob die lokalen Gegebenheiten die Installation eines Überspannungsschutzes erforderlich machen. Auch sollte festgelegt werden, wer unter welchen Umständen das Modem benutzen darf.

Beschaffung

Die Maßnahme M 2.59 *Auswahl eines geeigneten Modems in der Beschaffung* nennt die wesentlichen Kriterien, die bei der Auswahl eines Modems zu beachten sind.

Umsetzung

Vor der Inbetriebnahme ist das Modem geeignet zu konfigurieren, wobei unbedingt darauf zu achten ist, dass eventuell vorhandene, vom Hersteller vorgegebene Passwörter geändert werden. Die Installation eines Modems darf nicht dazu führen, dass hierdurch ein zusätzlicher, ungesicherter Zugang zu einem Rechnernetz, beispielsweise an einer Firewall vorbei, entsteht.

Betrieb

Damit nicht durch die Nutzung eines Modems ein zusätzliches Sicherheitsrisiko entsteht, muss für eine sichere Administration und Nutzung gesorgt werden. Dies lässt sich nur dann erreichen, wenn das Personal in diesem Bereich entsprechend geschult wird. Dazu gehört auch, dass sich die Mitarbeiter bewusst sind, dass über eine Modem-Verbindung Viren eingeschleppt werden können und dass sie daher besonders dafür Sorge zu tragen haben, dass alle übertragenen Daten auf Viren geprüft werden.

Um externe Angriffe über die Modem-Verbindung zu erschweren, sollte überlegt werden, ob das Modem so konfiguriert werden kann, dass alle Verbindungen von innen nach außen aufgebaut werden müssen und eingehende Verbindungen über ein Callback-Verfahren durchgeschaltet werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Modem" vorgestellt.

Planung und Konzeption

-	M 1.25	(Z)	Überspannungsschutz
-	M 2.42	(B)	Festlegung der möglichen Kommunikationspartner
-	M 2.46	(Z)	Geeignetes Schlüsselmanagement
-	M 2.61	(A)	Regelung des Modem-Einsatzes
-	M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
-	M 5.32	(A)	Sicherer Einsatz von Kommunikationssoftware

Beschaffung

-	M 2.59	(A)	Auswahl eines geeigneten Modems in der Beschaffung

Umsetzung

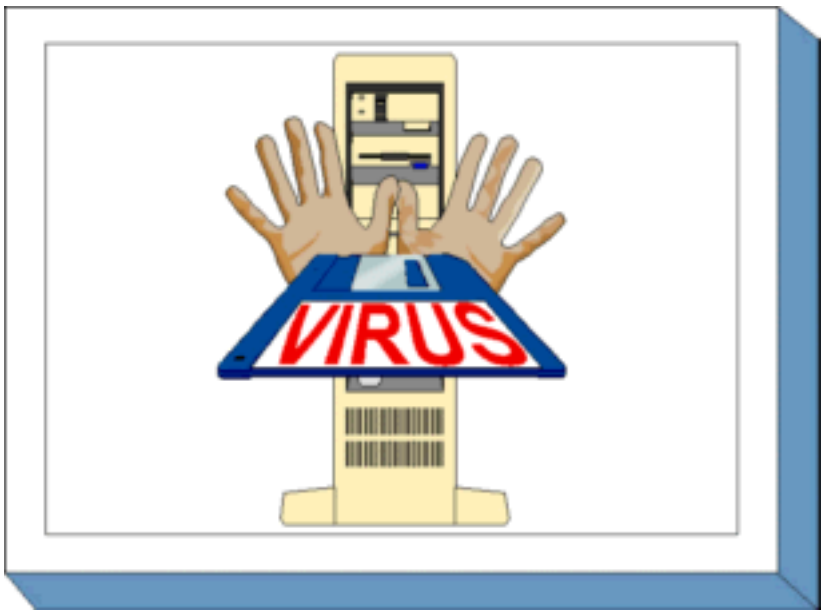
-	M 1.38	(A)	Geeignete Aufstellung eines Modems
-	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
-	M 4.7	(A)	Änderung voreingestellter Passwörter
-	M 5.30	(Z)	Aktivierung einer vorhandenen Callback-Option

-	M 5.31	(A)	Geeignete Modem-Konfiguration

Betrieb

-	M 2.60	(A)	Sichere Administration eines Modems
-	M 3.17	(A)	Einweisung des Personals in die Modem-Benutzung
-	M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
-	M 5.33	(A)	Absicherung der per Modem durchgeführten Fernwartung
-	M 5.44	(Z)	Einseitiger Verbindungsaufbau

B 1.6 Computer-Viren-Schutzkonzept



Beschreibung

Ziel eines Computer-Viren-Schutzkonzeptes ist es, geeignete Maßnahmen zum Schutz vor Schadprogrammen zusammenzustellen. Es soll gewährleistet sein, dass das Auftreten von Computer-Viren verhindert oder so früh wie möglich erkannt wird. Zusätzlich sind Maßnahmen zu benennen, die Schäden minimieren helfen, wenn ein Schadprogramm nicht rechtzeitig entdeckt werden konnte. Wesentlich ist die konsequente Anwendung der Maßnahmen und die ständige Aktualisierung der eingesetzten technischen Methoden. Diese Forderung begründet sich durch die täglich neu auftretenden Computer-Viren bzw. der Variation schon bekannter Computer-Viren. Durch die Weiterentwicklung von Betriebssystemen, Programmiersprachen und Anwendungssoftware entstehen weitere mögliche Angriffspotentiale für Computer-Viren, so dass rechtzeitig geeignete Gegenmaßnahmen eingeleitet werden müssen.

Wenn Behörden oder Unternehmen an öffentliche Kommunikationsnetze angeschlossen sind, ist die Gefahr durch Computer-Viren besonders groß. Die eingesetzten Rechner müssen daher permanent auf Computer-Viren kontrolliert werden.

Um für eine Gesamtorganisation einen effektiven Computer-Virenschutz zu erreichen, wird in diesem Kapitel die Vorgehensweise zur Erstellung und Realisierung eines Viren-Schutzkonzeptes in einzelnen Schritten erläutert. Maßnahmenempfehlungen zum Computer-Virenschutz für einzelne IT-Systeme finden sich in den systemspezifischen Bausteinen.

Gefährdungslage

Für den IT-Grundschutz werden bezüglich Computer-Viren die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel:

-	G 2.1	Fehlende oder unzureichende Regelungen
-	G 2.2	Unzureichende Kenntnis über Regelungen
-	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
-	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
-	G 2.8	Unkontrollierter Einsatz von Betriebsmitteln
-	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
-	G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren

Menschliche Fehlhandlungen:

-	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen

-	G 3.44	Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:

-	G 4.22	Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:

-	G 5.2	Manipulation an Daten oder Software
-	G 5.21	Trojanische Pferde

-	G 5.23	Computer-Viren
-	G 5.43	Makro-Viren
-	G 5.80	Hoax
-	G 5.127	Spyware

Maßnahmenempfehlungen

Bei der Erstellung eines Computer-Viren-Schutzkonzepts (siehe M 2.154 *Erstellung eines Computer-Virenschutzkonzept* ,) muss zunächst ermittelt werden, welche der vorhandenen oder geplanten IT-Systeme in das Computer-Viren-Schutzkonzept einzubeziehen sind (siehe M 2.155 *Identifikation potentiell von Computer-Viren betroffener IT-Systeme*). Für diese IT-Systeme müssen die für die Umsetzung von Sicherheitsmaßnahmen relevanten Einflussfaktoren betrachtet werden. Darauf aufbauend können dann die technischen und organisatorischen Maßnahmen ausgewählt werden. Hierzu ist insbesondere die Auswahl geeigneter technischer Gegenmaßnahmen wie Computer-Viren-Suchprogramme zu beachten (siehe M 2.156 *Auswahl einer geeigneten Computer-Virenschutz-Strategie* und M 2.157 *Auswahl eines geeigneten Computer-Viren-Suchprogramms*). Neben der Einrichtung eines Meldewesens (siehe M 2.158 *Meldung von Computer-Virusinfektionen*) und der Koordinierung der Aktualisierung eingesetzter Schutzprodukte (siehe M 2.159 *Aktualisierung der eingesetzten Computer-Viren-Suchprogramme*)

sind für die Umsetzung des Konzeptes eine Reihe von Regelungen zu vereinbaren (siehe M 2.11 *Regelung des Passwortgebrauchs*), in denen zusätzlich notwendige Maßnahmen zum Virenschutz festgelegt werden.

Eine der wichtigsten Vorbeugemaßnahmen gegen Schäden durch Computer-Viren ist die regelmäßige Datensicherung (siehe M 6.32 *Regelmäßige Datensicherung*).

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Planung und Konzeption

-	M 2.154	(A)	Erstellung eines Computer-Virenschutzkonzepts
-	M 2.155	(A)	Identifikation potentiell von Computer-Viren betroffener IT-Systeme
-	M 2.156	(A)	Auswahl einer geeigneten Computer-Virenschutz-Strategie
-	M 2.160	(A)	Regelungen zum Computer-Virenschutz

Beschaffung

-	M 2.157	(A)	Auswahl eines geeigneten Computer-Viren-Suchprogramms

Umsetzung

-	M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen

Betrieb

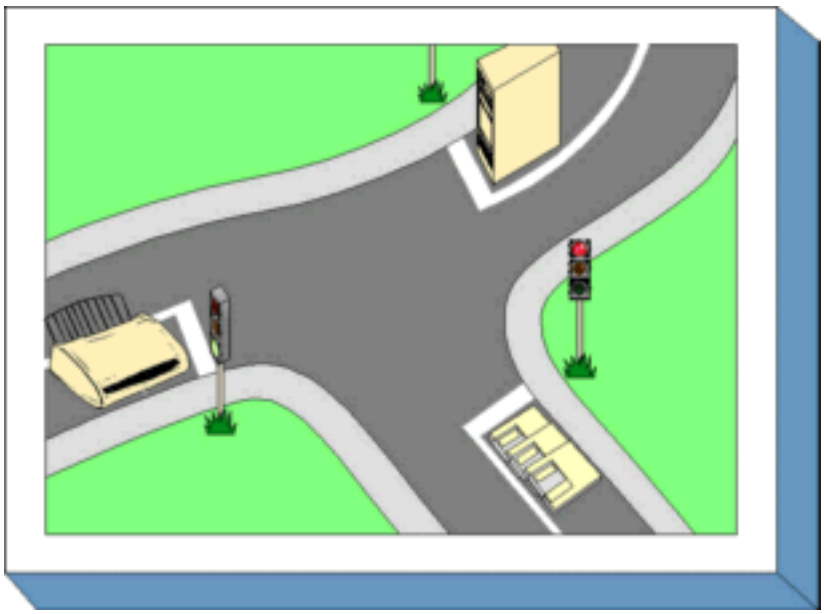
-	M 2.158	(A)	Meldung von Computer-Virusinfektionen

-	M 2.159	(A)	Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
-	M 2.224	(A)	Vorbeugung gegen Trojanische Pferde
-	M 4.3	(A)	Regelmäßiger Einsatz eines Anti-Viren-Programms
-	M 4.33	(A)	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
-	M 4.253	(A)	Schutz vor Spyware

Notfallvorsorge

-	M 6.23	(A)	Verhaltensregeln bei Auftreten eines Computer-Virus

B 1.9 Hard- und Software-Management



Beschreibung

Um den notwendigen und erwünschten Sicherheitsgrad für die gesamte IT-Organisation zu erreichen, genügt es nicht, nur die einzelnen IT-Komponenten zu sichern. Es ist vielmehr erforderlich, auch alle Abläufe und Vorgänge, die diese IT-Systeme berühren, so zu gestalten, dass das angestrebte IT-Sicherheitsniveau erreicht und beibehalten wird. Es sind daher für alle diese Vorgänge Regelungen einzuführen und zu pflegen, die die Wirksamkeit der Sicherheitsmaßnahmen gewährleisten.

Den Schwerpunkt dieses Bausteins bilden dabei Regelungen, die sich spezifisch auf informationstechnische Hardware- oder Software-Komponenten beziehen, mit dem Ziel, einen ordnungsgemäßen IT-Betrieb in Bezug auf Management bzw. Organisation sicherzustellen. Sicherheit sollte integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein.

Gefährdungslage

In diesem Kapitel werden für den IT-Grundschutz die folgenden

typischen Gefährdungen betrachtet:

Höhere Gewalt:

-	G 1.1	Personalausfall
-	G 1.2	Ausfall des IT-Systems
-	G 1.4	Feuer
-	G 1.5	Wasser
-	G 1.8	Staub, Verschmutzung

Organisatorischer Mängel:

-	G 2.1	Fehlende oder unzureichende Regelungen
-	G 2.2	Unzureichende Kenntnis über Regelungen
-	G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
-	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
-	G 2.7	Unerlaubte Ausübung von Rechten
-	G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
-	G 2.10	Nicht fristgerecht verfügbare Datenträger
-	G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
-	G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern
-	G 2.22	Fehlende Auswertung von Protokolldaten
-	G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz
-	G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten

Menschliche Fehlhandlungen:

-	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
-	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten
-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
-	G 3.5	Unbeabsichtigte Leitungsbeschädigung
-	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
-	G 3.8	Fehlerhafte Nutzung des IT-Systems
-	G 3.9	Fehlerhafte Administration des IT-Systems
-	G 3.11	Fehlerhafte Konfiguration von sendmail

-	G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel
-	G 3.35	Server im laufenden Betrieb ausschalten
-	G 3.44	Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:

-	G 4.8	Bekanntwerden von Softwareschwachstellen
-	G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
-	G 4.13	Verlust gespeicherter Daten
-	G 4.22	Software-Schwachstellen oder -Fehler
-	G 4.31	Ausfall oder Störung von Netzkomponenten
-	G 4.35	Unsichere kryptographische Algorithmen

-	G 4.38	Ausfall von Komponenten eines Netz- und Systemmanagementsystems
-	G 4.39	Software-Konzeptionsfehler
-	G 4.43	Undokumentierte Funktionen

Vorsätzliche Handlungen:

-	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
-	G 5.2	Manipulation an Daten oder Software
-	G 5.4	Diebstahl
-	G 5.9	Unberechtigte IT-Nutzung
-	G 5.21	Trojanische Pferde
-	G 5.23	Computer-Viren
-	G 5.26	Analyse des Nachrichtenflusses
-	G 5.43	Makro-Viren
-	G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
-	G 5.71	Vertraulichkeitsverlust schützenswerter Informationen
-	G 5.79	Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
-	G 5.82	Manipulation eines Kryptomoduls
-	G 5.83	Kompromittierung kryptographischer Schlüssel
-	G 5.84	Gefälschte Zertifikate
-	G 5.87	Web-Spoofing

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein IT-Verbund besteht aus einer Vielzahl von IT-Komponenten, die zunächst als Einzelkomponenten gemäß der Maßnahmenvorschläge aus den entsprechenden Bausteinen abgesichert werden sollten. Damit für alle eingesetzten IT-Komponenten das gleiche Sicherheitsniveau erreicht wird, sollten durch das Hard- und Software-Management einheitliche Regelungen vorgegeben werden.

Im Rahmen des Hard- und Software-Managements sind unabhängig von der Art der eingesetzten IT-Komponenten eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Aspekte der IT-Sicherheit müssen frühzeitig in die strategische Ausrichtung und die Beschaffung von IT-Systemen mit einfließen, da sie ganz konkrete Auswirkungen auf die Aufgabendurchführung und den Ablauf von Geschäftsprozessen haben. Hierbei müssen die definierten Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie die Anforderungen aus den geplanten Einsatzszenarien konsolidiert werden (siehe M 2.214 *Konzeption des IT-Betriebs*). Die Beschaffung und der Einsatz

von Hardware und Software erfordern spezifische Regelungen für die verschiedenen Benutzer. Hierbei müssen die für einen sicheren Geschäftsablauf erforderlichen Sicherheitsparameter der IT-Systeme den Benutzern transparent gemacht werden (siehe M 2.223 *Sicherheitsvorgaben für die Nutzung von Standardsoftware*). Trotz intensiver Schulung müssen die Benutzer im laufenden Betrieb hinsichtlich Funktionalität der Programme und Sicherheit sowie bei auftretenden Problemen zielgerichtet und zügig unterstützt werden (siehe M 2.12 *Betreuung und Beratung von IT-Benutzern*). Hierzu sind Benutzerbetreuer und Help-Desks einzurichten.

Die für den sicheren Betrieb aller IT-Komponenten notwendigen Maßnahmen müssen in einer Sicherheitsrichtlinie festgelegt werden.

Die Einhaltung des darin spezifizierten Sicherheitsniveaus erfordert neben den technischen Maßnahmen auch ein umfangreiches Regelwerk für den Benutzer, das diesem Hilfestellung und eine verbindliche und präzise Anleitung gibt. Potentielle Risikofaktoren und Schwachstellen wie Passwörter, Fremdpersonal, nicht freigegebene IT-Komponenten, Zugang zu den IT-Systemen müssen durch organisatorische Regelungen (siehe M 2.226 *Regelungen für den Einsatz von Fremdpersonal*) oder durch eine Kombination von organisatorischen und technischen Maßnahmen (siehe M 2.11 *Regelung des Passwortgebrauchs*) minimiert werden. Die Benutzer müssen regelmäßig für den sorgfältigen Umgang mit sicherheitskritischen Informationen und IT-Komponenten sensibilisiert werden (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Der effiziente und sichere Betrieb heterogener Netze erfordert strikte Richtlinien hinsichtlich Test, Installation und Dokumentation neuer Hardware und Software (siehe M 2.216 *Genehmigungsverfahren für IT-Komponenten*) sowie eine effiziente Benutzerverwaltung (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*). Der physikalische Zugang zu IT-Systemen sowie eine Authentisierung der Benutzer gegenüber den Anwendungen und Systemen (siehe M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*) sollte grundsätzlich unter Beachtung des Need-to-Know-Prinzips erfolgen.

Der Einsatz von externen Datenträgern kann ein hohes Sicherheitsrisiko darstellen, da vermeintliche Sicherheitsbarrieren häufig einfach ausgehebelt werden können. Regelungen der Verwendung, Kennzeichnung und Prüfungen - z. B. auf Viren - für Disketten, CD-ROMs, Memory-Sticks und andere über USB anschließbare Geräte für den Datenaustausch, dienen ebenfalls zur Aufrechterhaltung eines sicheren IT-Betriebs (siehe M 2.3 *Datenträgerverwaltung*).

Aufgabe des Änderungsmanagements ist es, Änderungen an den aktuellen Konfigurationen einem formalen Dokumentations- und

Freigabeprozess zu unterziehen (siehe M 2.221 *Änderungsmanagement*). Sicherheitskritische Aspekte müssen hierbei ebenso bewertet werden wie die Durchführung nach dem Vier-Augen-Prinzip und die aktuelle Dokumentation der Änderungen. Hierzu gehört auch, dass nur zugelassene Komponenten zum Einsatz kommen dürfen, da sonst ein kontrollierbarer Betrieb nicht möglich ist (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

Beschaffung

Für die Beschaffung von IT-Systemen müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden. Der formalen Freigabe eines neuen Produktes (siehe M 2.62 *Software-Abnahme- und Freigabe-Verfahren*) sollte eine funktionale Prüfung und eine Konsistenzprüfung hinsichtlich der geforderten Sicherheitseigenschaften vorausgehen (siehe M 4.65 *Test neuer Hard- und Software*).

Umsetzung

Die Umsetzung der Sicherheitsrichtlinie für den Betrieb erfordert Festlegungen für Sicherheitsmaßnahmen im Rahmen der Installation und ersten Konfiguration (siehe M 4.135 Restriktive Vergabe von

Zugriffsrechten auf Systemdateien) sowie für den laufenden Betrieb der IT-Systeme. Die strukturierte Datenhaltung mit konsequenter Trennung von Programm- und Arbeitsdateien (siehe M 2.138 *Strukturierte Datenhaltung*) sollte auf einer weitgehend einheitlichen Konfiguration der Systeme aufsetzen. Diese wiederum unterstützt eine zentral durchführbare Systemverwaltung (siehe M 2.69 *Einrichtung von Standardarbeitsplätzen*).

Die Sicherstellung einer durchgängigen Systemadministration - auch in Ausfallzeiten wie bei Krankheit oder Urlaub - lässt sich durch entsprechende Vertretungsregelungen erreichen (siehe M 2.26

Ernennung eines Administrators und eines Vertreters). Die Kompetenzen des Vertreters müssen transparent gemacht werden.

Die Dokumentation der Systemkonfiguration muss aktuell und verständlich sein und sollte werkzeugunterstützt erfolgen (siehe M 2.25 *Dokumentation der Systemkonfiguration*). Neben den physikalischen IT-Komponenten sind auch die logischen Netzstrukturen sowie die Rollen und Zugriffsrechte zu dokumentieren.

Betrieb

Durch die Systemadministration ist der laufende Betrieb mit unterschiedlichen Schwerpunkten aufrecht zu erhalten. Die durch Migration, Ausfall und Neuanschaffung erforderlichen Änderungen des IT-Bestandes (siehe M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen) müssen nach erfolgter Freigabe im IT-Bestandsverzeichnis zeitnah nachgeführt werden (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System* und M 2.219 *Kontinuierliche Dokumentation der Informationsverarbeitung*).

Die laufende Beobachtung und Auswertung des Betriebes (siehe M 2.10 *Überprüfung des Hard- und Software-Bestandes* und M 2.64 *Kontrolle der Protokolldateien*) hinsichtlich Konformität und eventuellen Sicherheitsverletzungen sowie die Durchführung der entsprechenden Sicherheitsmaßnahmen (siehe M 2.215 *Fehlerbehandlung*) erfordern eine permanente Informationsbeschaffung über entsprechende Updates der unterschiedlichen Hersteller (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Durch Einspielen der erforderlichen Sicherheitspatches sollte die geforderte Sicherheit auch schon präventiv erreicht werden.

Die für die Bereiche Organisation und Personal festgelegten Sicherheitsmaßnahmen müssen durch Kontrollen auf ihre Anwendbarkeit, Akzeptanz und Wirksamkeit hin untersucht werden (M 2.182 *Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen*).

Aussonderung

Bei der Außerbetriebnahme von IT-Systemen ist dafür zu sorgen, dass wichtige Daten nicht verloren gehen, sondern vor der Abgabe bzw. Verschrottung der IT-Systeme gesichert werden (siehe Maßnahme M 4.234 *Aussonderung von IT-Systemen*). Fast noch wichtiger ist es jedoch, die Datenträger dieser Systeme anschließend so gründlich zu löschen (siehe Maßnahme M 2.167 *Sicheres Löschen von Datenträgern*), dass nicht im Nachhinein Unbefugte auf sensible Daten Zugriff erhalten, da in der Regel nach der Aussonderung keine Kontrolle darüber besteht, was mit den IT-Systemen weiter geschieht.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Hard- und Software-Management" vorgestellt:

Planung und Konzeption

-	M 2.3	(B)	Datenträgerverwaltung
-	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
-	M 2.11	(A)	Regelung des Passwortgebrauchs
-	M 2.12	(C)	Betreuung und Beratung von IT-Benutzern

-	M 2.30	(A)	Regelung für die Einrichtung von Benutzern / Benutzergruppen
-	M 2.214	(A)	Konzeption des IT-Betriebs
-	M 2.216	(C)	Genehmigungsverfahren für IT-Komponenten
-	M 2.217	(B)	Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
-	M 2.218	(C)	Regelung der Mitnahme von Datenträgern und IT-Komponenten

-	M 2.220	(A)	Richtlinien für die Zugriffs- bzw. Zugangskontrolle
-	M 2.221	(B)	Änderungsmanagement
-	M 2.223	(B)	Sicherheitsvorgaben für die Nutzung von Standardsoftware
-	M 2.226	(A)	Regelungen für den Einsatz von Fremdpersonal
-	M 4.133	(Z)	Geeignete Auswahl von Authentikationsmechanismen
-	M 4.134	(C)	Wahl geeigneter Datenformate
-	M 5.68	(Z)	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
-	M 5.77	(Z)	Bildung von Teilnetzen
-	M 5.87	(C)	Vereinbarung über die Anbindung an Netze Dritter
-	M 5.88	(C)	Vereinbarung über Datenaustausch mit Dritten

Beschaffung

-	M 2.62	(B)	Software-Abnahme- und Freigabe-Verfahren

Umsetzung

-	M 1.29	(Z)	Geeignete Aufstellung eines IT-Systems (optional)
-	M 2.25	(A)	Dokumentation der Systemkonfiguration
-	M 2.26	(A)	Ernennung eines Administrators und eines Vertreters
-	M 2.38	(B)	Aufteilung der Administrationstätigkeiten
-	M 2.69	(B)	Einrichtung von Standardarbeitsplätzen
-	M 2.111	(A)	Bereithalten von Handbüchern
-	M 2.138	(B)	Strukturierte Datenhaltung

-	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
-	M 4.1	(A)	Passwortschutz für IT-Systeme
-	M 4.65	(C)	Test neuer Hard- und Software
-	M 4.7	(A)	Änderung voreingestellter Passwörter
-	M 4.84	(A)	Nutzung der BIOS-Sicherheitsmechanismen
-	M 4.135	(A)	Restriktive Vergabe von Zugriffsrechten auf Systemdateien

Betrieb

-	M 1.46	(Z)	Einsatz von Diebstahl-Sicherungen
-	M 2.9	(A)	Nutzungsverbot nicht freigegebener Hard- und Software
-	M 2.10	(C)	Überprüfung des Hard- und Software-Bestandes
-	M 2.22	(Z)	Hinterlegen des Passwortes
-	M 2.34	(A)	Dokumentation der Veränderungen an einem bestehenden System
-	M 2.35	(B)	Informationsbeschaffung über Sicherheitslücken des Systems
-	M 2.64	(A)	Kontrolle der Protokolldateien
-	M 2.65	(C)	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
-	M 2.110	(A)	Datenschutzaspekte bei der Protokollierung
-	M 2.182	(A)	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
-	M 2.215	(B)	Fehlerbehandlung
-	M 2.219	(A)	Kontinuierliche Dokumentation der Informationsverarbeitung
-	M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT

-	M 4.78	(A)	Sorgfältige Durchführung von Konfigurationsänderungen

-	M 4.107	(B)	Nutzung von Hersteller-Ressourcen
-	M 4.109	(Z)	Software-Reinstallation bei Arbeitsplatzrechnern
-	M 4.254	(Z)	Sicherer Einsatz von drahtlosen Tastaturen und Mäusen

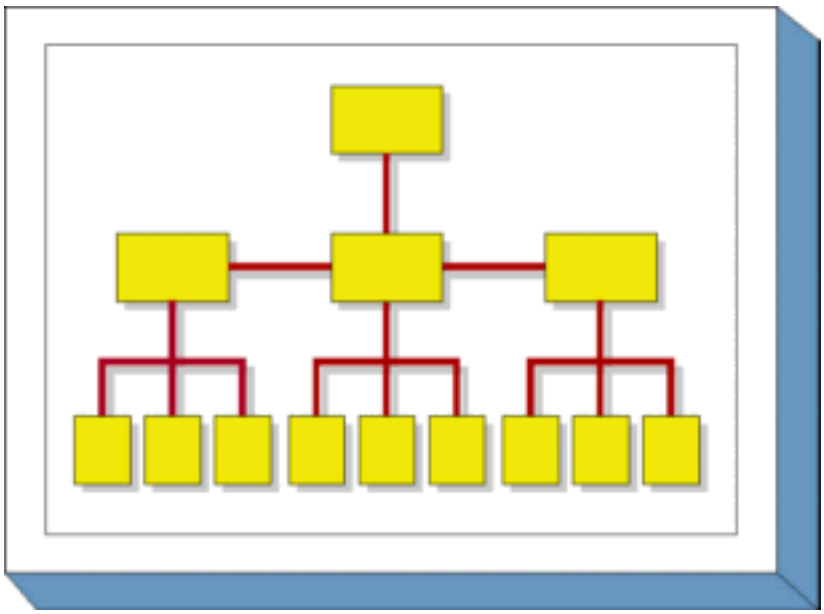
Aussonderung

-	M 2.167	(B)	Sicheres Löschen von Datenträgern
-	M 4.234	(B)	Aussonderung von IT-Systemen

Notfallvorsorge

-	M 6.27	(C)	Sicheres Update des BIOS

B 1.1 Organisation



Beschreibung

In diesem Baustein werden allgemeine und übergreifende Empfehlungen im Organisationsbereich aufgeführt, die als organisatorische Standardmaßnahmen zur Erreichung eines Mindestschutzniveaus erforderlich sind. Spezielle Maßnahmen organisatorischer Art, die in unmittelbarem Zusammenhang mit anderen Themen stehen (z. B. LAN-Administration), werden in den entsprechenden Bausteinen aufgeführt. Auf das ordnungsgemäße Management informationstechnischer Komponenten (Hardware oder Software) ausgerichtete Standard-Sicherheits-Maßnahmen befinden sich im Baustein B 1.9 *Hard- und Software-Management* .

Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:

-	G 1.4	Feuer

-	G 1.5	Wasser
-	G 1.7	Unzulässige Temperatur und Luftfeuchte

Organisatorische Mängel:

-	G 2.1	Fehlende oder unzureichende Regelungen
-	G 2.2	Unzureichende Kenntnis über Regelungen
-	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
-	G 2.5	Fehlende oder unzureichende Wartung
-	G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
-	G 2.7	Unerlaubte Ausübung von Rechten
-	G 2.8	Unkontrollierter Einsatz von Betriebsmitteln

Menschliche Fehlhandlungen:

-	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal

Technisches Versagen:

-	G 4.1	Ausfall der Stromversorgung
-	G 4.2	Ausfall interner Versorgungsnetze
-	G 4.3	Ausfall vorhandener Sicherungseinrichtungen

Vorsätzliche Handlungen:

-	G 5.1	Manipulation/Zerstörung von IT-Geräten oder Zubehör
-	G 5.2	Manipulation an Daten oder Software

-	G 5.3	Unbefugtes Eindringen in ein Gebäude
-	G 5.4	Diebstahl
-	G 5.5	Vandalismus
-	G 5.6	Anschlag
-	G 5.12	Abhören von Telefongesprächen und Datenübertragungen
-	G 5.13	Abhören von Räumen
-	G 5.16	Gefährdung bei Wartungs-/ Administrierungsarbeiten durch internes Personal
-	G 5.17	Gefährdung bei Wartungsarbeiten durch externes Personal
-	G 5.68	Unberechtigter Zugang zu den aktiven Netzkomponenten
-	G 5.102	Sabotage

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Mindestschutzniveau kann nur erreicht werden, wenn übergreifende Regelungen zur IT-Sicherheit verbindlich festgelegt werden. Hierzu sind eine Reihe von Maßnahmen umzusetzen, beginnend mit Festlegung und Zuweisung von verantwortlichen Personen für einzelne IT-Objekte (z. B. Anwendungen, IT-Komponenten) über entsprechende organisatorische Handlungsanweisungen bis hin zur Behandlung von schützenswerten Betriebsmitteln. Die Schritte, die dabei im Sinne eines kontinuierlichen IT-Sicherheitsprozesses durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Für die Initiierung und die Umsetzung der sich aus den Sicherheitszielen und Sicherheitsrichtlinien ergebenden Prozesse sind organisatorische und personelle Festlegungen zu treffen. Hierbei sind gegebenenfalls die Mitbestimmungsrechte des Personal- bzw. Betriebsrates zu wahren (siehe M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates*). Die verschiedenen Organisationsebenen und die hier tätigen Personen benötigen konkrete Handlungsanweisungen und Verantwortlichkeiten zur Abwicklung der sie betreffenden Prozesse (siehe M 2.225 *Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten*).

Die strategischen Überlegungen sind in einem Betriebskonzept bezüglich ihrer Umsetzung im Unternehmen bzw. in der Behörde zu detaillieren.

Der Einsatz der erforderlichen Betriebsmittel ist auf die Aufgabenerfüllung und die Sicherheitsanforderungen abzustimmen und über eine Betriebsmittelverwaltung (siehe M 2.2 *Betriebsmittelverwaltung*) zu dokumentieren. Diese muss vollständig sein und durch entsprechende Prozesse auch jederzeit aktuell gehalten werden.

Voraussetzung für eine funktionierende IT-Infrastruktur, die auch auf Störungen adäquat reagieren kann, sind Regelungen für Ersatzteilbeschaffung, Reparaturen und Wartungsarbeiten (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*). In Wartungsverträgen ist die terminliche und inhaltliche Wartung einzelner IT-Systeme (oder Gruppen) verbindlich zu regeln, ebenso wie die erforderlichen Zugänge (Remote, vor Ort) und die an die Sicherheitsanforderungen angepassten Reaktionszeiten des mit der Wartung beauftragten Personals.

Die Aufgabenverteilung und die hierfür erforderlichen Funktionen (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*) sind so zu

strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu minimieren oder ganz auszuschalten.

Betrieb

Die festgelegten Konzeptionen werden in konkrete Handlungsanweisungen gefasst und für den Betrieb verbindlich verabschiedet. Mitarbeiterbezogene Regelungen müssen hierbei die komplette Laufbahn eines Mitarbeiters im Unternehmen vom Eintritt bis zum Austritt betrachten. Durch Anwendung des Need-to-Know-Prinzips und des Vier-Augen-Prinzips ist sicher zu stellen, das Berechtigungen auf den verschiedenen Ebenen (z. B. Zutritt zu Räumen, Zugang zu IT-Systemen) zielgerichtet vergeben werden und auch praktikabel sind (siehe M 2.6 *Vergabe von Zutrittsberechtigungen* und M 2.7 *Vergabe von Zugangsberechtigungen*).

Diese Berechtigungen sind zu dokumentieren und durch verschiedene Methoden zu unterstützen, wie z. B. kontrollierte und nachweisbare Ausgabe von Schlüsseln nur an Berechtigte (siehe M 2.14 *Schlüsselverwaltung*), Authentisierung von Zugriffen, Zutrittskontrollsysteme für speziell gesicherte Bereiche und Kontrolle der Aktionen Betriebsfremder (siehe M 2.16 *Beaufsichtigung oder Begleitung von Fremdpersonen*). Die Zuordnung von Personen oder Personengruppen zu Rollen erleichtert die Verwaltung von Berechtigungen (siehe M 2.8 *Vergabe von Zugriffsrechten*). Werden Regelungen bewusst oder unbewusst verletzt, so müssen die hieraus ableitbaren Informations- und Eskalationsprozesse den Mitarbeitern bekannt sein, so dass eine zielgerichtete Reaktion auf die Verletzung erfolgen kann (siehe M 2.39 *Reaktion auf Verletzungen der Sicherheitspolitik*).

Aussonderung

Betriebs- und Sachmittel, die besonderen Schutzbedingungen unterliegen, sind so zu entsorgen, dass keine Rückschlüsse auf ihre

Verwendung oder Inhalte gemacht werden können (siehe M 2.13 *Ordnungs*gemäße Entsorgung von schützenswerten Betriebsmitteln). Hierzu sind entsprechende Regelungen, gegebenenfalls auch mit externen Firmen, zu treffen. Entsprechende Bestimmungen des Datenschutzes sind zu beachten.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Organisation" vorgestellt:

Planung und Konzeption

-	M 2.1	(A)	Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
-	M 2.2	(C)	Betriebsmittelverwaltung
-	M 2.4	(B)	Regelungen für Wartungs- und Reparaturarbeiten
-	M 2.5	(A)	Aufgabenverteilung und Funktionstrennung
-	M 2.40	(A)	Rechtzeitige Beteiligung des Personal-/ Betriebsrates
-	M 2.225	(B)	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten

Betrieb

-	M 2.6	(A)	Vergabe von Zutrittsberechtigungen
-	M 2.7	(A)	Vergabe von Zugangsberechtigungen
-	M 2.8	(A)	Vergabe von Zugriffsrechten
-	M 2.14	(A)	Schlüsselverwaltung
-	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
-	M 2.18	(Z)	Kontrollgänge
-	M 2.37	(Z)	"Der aufgeräumte Arbeitsplatz"

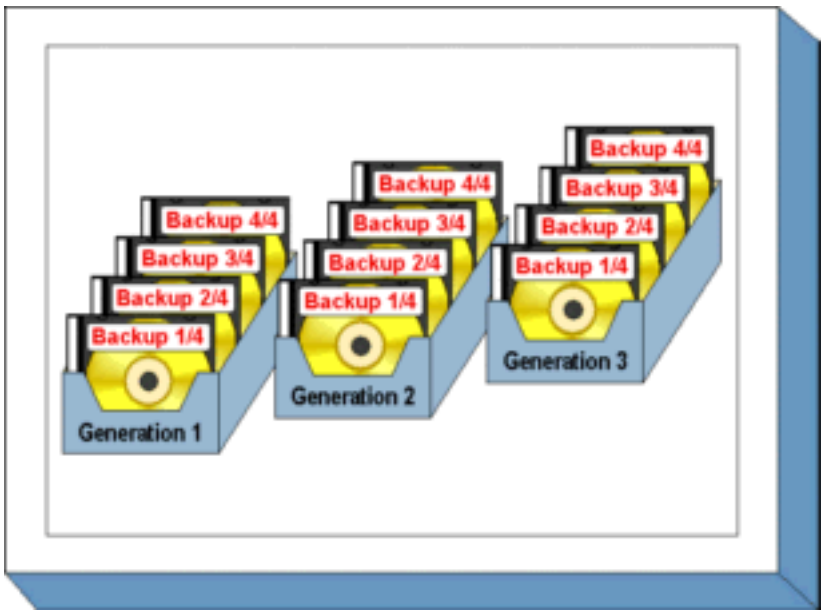
-	M 2.39	(B)	Reaktion auf Verletzungen der Sicherheitspolitik
-	M 2.177	(Z)	Sicherheit bei Umzügen

Aussonderung

-	M 2.13	(A)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

---

B 1.4 Datensicherungskonzept



Beschreibung

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Die Konzeption einer angemessenen und funktionstüchtigen Datensicherung bedarf allerdings aufgrund der Komplexität einer geordneten Vorgehensweise. In diesem Baustein wird ein Weg beschrieben, wie für ein IT-System ein Datensicherungskonzept erstellt werden kann.

Gefährdungslage

Für die mittels eines Datensicherungskonzepts zu schützenden Daten wird für den IT-Grundschutz folgende typische Gefährdung angenommen:

Technisches Versagen:

-	G 4.13	Verlust gespeicherter Daten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um eine effektive Datensicherung einzurichten, sind eine Reihe von Schritten zu durchlaufen. Diese sind in der Maßnahme M 6.33 *Entwicklung eines Datensicherungskonzepts* beschrieben und werden durch die dort aufgeführten Maßnahmen erläutert. Daher sollte mit der Umsetzung der Maßnahme M 6.33 begonnen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datensicherungskonzept" vorgestellt, das vor allem für größere IT-Systeme oder IT-Systeme mit großem Datenvolumen sinnvoll ist. Die Bearbeitung der Maßnahmen sollte in der angegebenen Reihenfolge geschehen, um systematisch ein Datensicherungskonzept zu erarbeiten.

Planung und Konzeption

-	M 6.33	(B)	Entwicklung eines Datensicherungskonzepts
-	M 6.34	(B)	Erhebung der Einflussfaktoren der Datensicherung
-	M 6.35	(B)	Festlegung der Verfahrensweise für die Datensicherung
-	M 6.36	(A)	Festlegung des Minimaldatensicherungskonzeptes

Beschaffung

-	M 2.137	(A)	Beschaffung eines geeigneten Datensicherungssystems

Umsetzung

-	M 2.41	(A)	Verpflichtung der Mitarbeiter zur Datensicherung
-	M 6.21	(C)	Sicherungskopie der eingesetzten Software
-	M 6.37	(A)	Dokumentation der Datensicherung

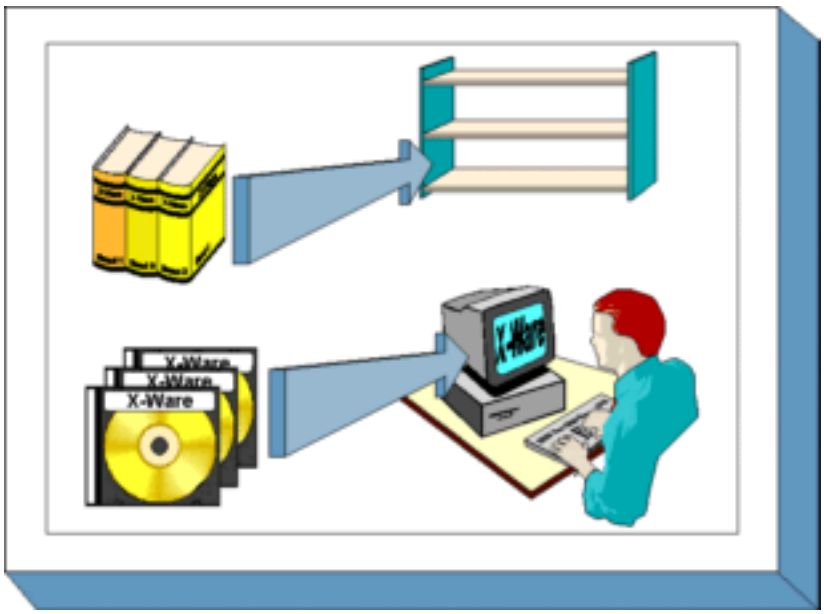
Betrieb

-	M 6.20	(A)	Geeignete Aufbewahrung der Backup-Datenträger
-	M 6.22	(A)	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
-	M 6.32	(A)	Regelmäßige Datensicherung

Notfallvorsorge

-	M 6.41	(A)	Übungen zur Datenrekonstruktion

B 1.10 Standardsoftware



Beschreibung

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

In diesem Baustein wird eine Vorgehensweise für den Umgang mit Standardsoftware unter Sicherheitsgesichtspunkten dargestellt. Dabei wird der gesamte Lebenszyklus von Standardsoftware betrachtet: Erstellung eines Anforderungskataloges, Vorauswahl eines geeigneten Produktes, Test, Freigabe, Installation, Lizenzverwaltung und Deinstallation.

Das Qualitätsmanagementsystem des Entwicklers der Standardsoftware fällt nicht in den Anwendungsbereich dieses Bausteins. Es wird vorausgesetzt, dass die Entwicklung der Software unter Beachtung gängiger Qualitätsstandards erfolgte.

Die beschriebene Vorgehensweise dient der Orientierung, um einen Sicherheitsprozess bezüglich Standardsoftware zu etablieren. Gegebenenfalls kann die hier aufgezeigte Vorgehensweise auch zum Vergleich mit einem bereits eingeführten Verfahren herangezogen werden.

Gefährdungslage

Für den IT-Grundschutz von "Standardsoftware" werden die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:

-	G 1.2	Ausfall des IT-Systems

Organisatorische Mängel:

-	G 2.1	Fehlende oder unzureichende Regelungen
-	G 2.2	Unzureichende Kenntnis über Regelungen
-	G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel
-	G 2.7	Unerlaubte Ausübung von Rechten
-	G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren
-	G 2.27	Fehlende oder unzureichende Dokumentation
-	G 2.28	Verstöße gegen das Urheberrecht
-	G 2.29	Softwaretest mit Produktionsdaten
-	G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten

Menschliche Fehlhandlungen:

-	G 3.2	Fahrlässige Zerstörung von Gerät oder Daten

-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
-	G 3.8	Fehlerhafte Nutzung des IT-Systems
-	G 3.16	Fehlerhafte Administration von Zugangs- und Zugriffsrechten
-	G 3.17	Kein ordnungsgemäßer PC-Benutzerwechsel

Technisches Versagen:

-	G 4.7	Defekte Datenträger

-	G 4.8	Bekanntwerden von Softwareschwachstellen
-	G 4.22	Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:

-	G 5.2	Manipulation an Daten oder Software
-	G 5.9	Unberechtigte IT-Nutzung
-	G 5.21	Trojanische Pferde
-	G 5.23	Computer-Viren
-	G 5.43	Makro-Viren

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Standardsoftware sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung des Einsatzes über die Beschaffung bis zu ihrer Außerbetriebnahme. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Vor der Auswahl einer bestimmten Standardsoftware sollte ein Anforderungskatalog erstellt werden, anhand dessen ein Produkt nach objektiven und nachvollziehbaren Kriterien ausgewählt werden kann, so dass man ein gewisses Vertrauen haben kann, dass ein einigermaßen optimales Produkt zum Einsatz kommt. In dieser Phase sollten bei komplexeren Produkten auch die Verantwortlichen für deren Beschaffung und Einsatz festgelegt werden.

Beschaffung

Für die Beschaffung kann anhand der konkreten Vorgaben des Anforderungskatalogs geprüft werden, welches der am Markt vorhandenen Produkte die am besten geeignete Funktionalität aufweist.

Umsetzung

Durch Tests in angemessener Tiefe ist sicherzustellen, dass das ausgewählte Produkt über die in der Dokumentation angegebene Funktionalität auch tatsächlich verfügt. Sofern das Produkt auf breiter Basis einzusetzen ist, muss es in die vorhandenen Installationsverfahren eingebunden werden, und die Installation selbst ist zu dokumentieren. Eine Nutzung in der Fläche darf erst erfolgen, wenn das Produkt nach erfolgreichem Durchlaufen der Tests und nach Abschluss der Vorbereitungsarbeiten dafür freigegeben wurde.

Betrieb

Die Kontrolle der installierten Versionen und die Nachverfolgung der verfügbaren Lizenzen und deren Abgleich mit der installierten Anzahl der Produkte ist eine permanente Aufgabe während der Nutzung der Standardsoftware.

Aussonderung

Eine saubere Deinstallation von Standardsoftware erfordert häufig umfangreiche und komplexe Arbeiten, in einzelnen Fällen bis hin zur

Neuinstallation von Rechnern.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Standardsoftware" vorgestellt. Je nach Art und Umfang der jeweiligen Standardsoftware muss erwogen werden, ob einzelne Maßnahmen nur reduziert umgesetzt werden. Die Maßnahmen M 2.79 bis M 2.89 stellen in der angegebenen Reihenfolge eine umfassende Beschreibung dar, wie der Lebenszyklus von Standardsoftware gestaltet werden kann. Sie werden durch die anderen genannten Maßnahmen ergänzt.

Planung und Konzeption

-	M 2.79	(A)	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
-	M 2.80	(A)	Erstellung eines Anforderungskatalogs für Standardsoftware
-	M 2.82	(B)	Entwicklung eines Testplans für Standardsoftware
-	M 4.34	(Z)	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

Beschaffung

-	M 2.66	(Z)	Beachtung des Beitrags der Zertifizierung für die Beschaffung
-	M 2.81	(A)	Vorauswahl eines geeigneten Standardsoftwareproduktes

Umsetzung

-	M 2.83	(B)	Testen von Standardsoftware
-	M 2.84	(A)	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
-	M 2.85	(A)	Freigabe von Standardsoftware

-	M 2.86	(B)	Sicherstellen der Integrität von Standardsoftware
-	M 2.87	(A)	Installation und Konfiguration von Standardsoftware
-	M 2.90	(A)	Überprüfung der Lieferung
-	M 4.42	(Z)	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

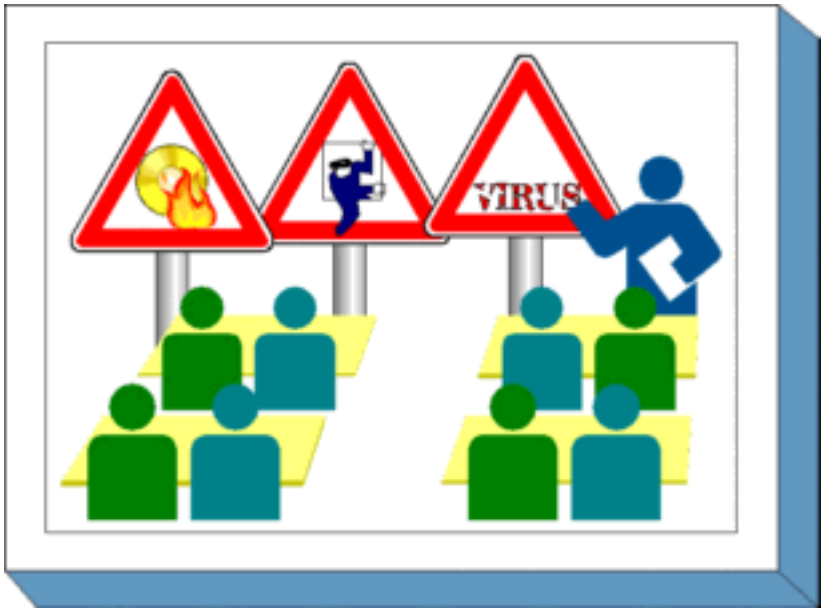
Betrieb

-	M 2.88	(A)	Lizenzverwaltung und Versionskontrolle von Standardsoftware

Aussonderung

-	M 2.89	(C)	Deinstallation von Standardsoftware

B 1.13 IT-Sicherheitssensibilisierung und -schulung



Beschreibung

Um IT-Sicherheitsmaßnahmen wirkungsvoll umsetzen zu können, muss in einem Unternehmen bzw. einer Behörde eine IT-Sicherheitskultur aufgebaut und ein IT-Sicherheitsbewußtsein gebildet werden. Alle Mitarbeiter müssen davon überzeugt sein, dass IT-Sicherheit einen wesentlichen Teil des Erfolges der jeweiligen Organisation ausmacht. Dazu muss auch kommuniziert werden, warum bestimmte IT-Sicherheitsmaßnahmen notwendig und sinnvoll sind. Ebenso muss allen Mitarbeitern bekannt sein, was von ihnen im Hinblick auf IT-Sicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten. Dies setzt in vielen Bereichen eine langfristige Verhaltensänderung der Mitarbeiter voraus und kann nur in einem langen und kontinuierlichen Prozess erreicht werden. Einmalige Schulungen oder Sensibilisierungsveranstaltungen reichen hier nicht aus.

Informierte und geschulte Mitarbeiter sind Voraussetzungen dafür, dass eine Behörde oder ein Unternehmen die gesteckten Ziele erreichen kann. Außerdem wird durch Information und Schulung

sichergestellt, dass alle Mitarbeiter die Folgen und Auswirkungen ihrer Tätigkeit im beruflichen und privaten Umfeld einschätzen können. Ziel der IT-Sicherheitssensibilisierung ist es, das Bewusstsein der Mitarbeiter für Sicherheitsprobleme zu schärfen. Durch Schulungen zur IT-Sicherheit wird den Mitarbeitern die notwendige Kompetenz zur IT-Sicherheit vermittelt, die sie bei der Ausführung ihrer Fachaufgaben benötigen. Es ist sicherzustellen, dass alle Mitarbeiter die Abläufe kennen und wissen, an wen sie sich wenden müssen, falls Sicherheitsfragen auftreten oder Sicherheitsprobleme gelöst werden müssen.

Damit die Durchführung von Schulungs- und Sensibilisierungsmaßnahmen auch nachhaltig unterstützt wird, ist es wichtig, dass das Management auf die Bedeutung der IT-Sicherheit aufmerksam gemacht wird. Dieser Baustein ist also grundsätzlich für alle zu empfehlen, die für die IT-Sicherheit in einer Institution (egal welcher Größe) verantwortlich sind.

In diesem Baustein wird daher beschrieben, wie ein effektives Schulungs- und Sensibilisierungsprogramm zur IT-Sicherheit aufgebaut und aufrechterhalten werden kann.

Gefährdungslage

Für den IT-Grundschutz werden in diesem Baustein die folgenden typische Gefährdungen betrachtet:

Organisatorische Mängel

-	G 2.2	Unzureichende Kenntnis über Regelungen
-	G 2.7	Unerlaubte Ausübung von Rechten
-	G 2.102	Unzureichende Sensibilisierung für IT-Sicherheit
-	G 2.103	Unzureichende Schulung der Mitarbeiter

Menschliche Fehlhandlungen:

-	G 3.1	Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
-	G 3.3	Nichtbeachtung von IT-Sicherheitsmaßnahmen
-	G 3.8	Fehlerhafte Nutzung des IT-Systems
-	G 3.9	Fehlerhafte Administration des IT-Systems
-	G 3.44	Sorglosigkeit im Umgang mit Informationen
-	G 3.77	Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahmen

Vorsätzliche Handlungen:

-	G 5.2	Manipulation an Daten oder Software
-	G 5.9	Unberechtigte IT-Nutzung
-	G 5.19	Missbrauch von Benutzerrechten
-	G 5.20	Missbrauch von Administratorrechten
-	G 5.42	Social Engineering
-	G 5.104	Ausspähen von Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um eine umfassende Sensibilisierung für IT-Sicherheitsfragen in einer Institution zu erreichen, sollte ein Programm aufgebaut werden, das unter anderem Schulungen, Trainingsprogramme, Sicherheitskampagnen und andere Aktivitäten beinhalten kann. Damit dieses wirkungsvoll realisiert wird, sind eine Reihe von Schritten zu durchlaufen.

Planung und Konzeption

Die Unterstützung der Leitung ist für den gesamten IT-Sicherheitsprozess notwendig. Dies setzt voraus, dass diese die Bedeutung der IT-Sicherheit hinreichend bekannt ist. In M 3.44 *Sensibilisierung des Managements für IT-Sicherheit* wird beschrieben, wie dies erreicht werden kann.

Zunächst muss das Schulungs- und Sensibilisierungsprogramm strategisch vorbereitet und geplant werden. Die hierfür notwendigen Schritte sind in der Maßnahme M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit* beschrieben und werden durch die daran anschließenden Maßnahmen erläutert. Daher sollte mit der Umsetzung der Maßnahme M 2.312 begonnen werden.

Die Basis jedes Schulungsprogramms sind die Sicherheitsleitlinie und die Sicherheitsrichtlinien, die sowohl übergreifend als auch themenbezogen innerhalb einer Behörde oder eines Unternehmens existieren sollten (siehe M 2.192 *Erstellung einer IT-Sicherheitsleitlinie*).

Beschaffung

Für die Durchführung von Schulungs- und Sensibilisierungsprogrammen wird internes oder externes Personal benötigt, das die Sensibilisierungs- und Schulungsmaßnahmen vorbereiten und durchführen kann, siehe dazu M 3.48 *Auswahl von Trainern oder Schulungsanbietern* .

Umsetzung

Für die Durchführung von Schulungs- und Sensibilisierungsmaßnahmen werden diverse Ressourcen benötigt, beispielsweise Personal für Konzeption und Durchführung oder Räumlichkeiten für Schulungen. Besondere Sicherheitsaspekte, die bei der Gestaltung von Schulungsräumen zu beachten sind, finden sich in Baustein B 2.11 *Besprechungs-, Veranstaltungs- und Schulungsräume* .

Schulungsinhalte zur IT-Sicherheit müssen je nach Zielgruppe geeignet ausgewählt werden, siehe M 3.45 *Planung von Schulungsinhalten zur IT-Sicherheit* .

Betrieb, Kontinuierliche Pflege und Weiterentwicklung

Ein stets unabdingbarer Bestandteil der Schulungen zur IT-Sicherheit ist dabei der Umgang mit IT (siehe M 3.4 *Schulung vor Programmnutzung* , M 3.11 *Schulung des Wartungs- und Administrationspersonals* , M 3.26 *Einweisung des Personals in den sicheren Umgang mit IT* und weitere themenspezifische Maßnahmen).

Bei der Einführung neuer Techniken sollten die Mitarbeiter frühzeitig über diese informiert sowie für Gefahrenpotentiale und Sicherheitsmaßnahmen sensibilisiert werden, damit die neuen Techniken auch ordnungsgemäß eingesetzt werden.

Wie die Organisation die Bildung eines IT-Sicherheitsbewußtseins bei den Mitarbeitern fördern kann, wird in M 2.198 *Sensibilisierung der Mitarbeiter für IT-Sicherheit* und M 3.47 *Durchführung von Planspielen zur IT-Sicherheit* beschrieben.

Es sollte zu Sicherheitsfragen auch immer geeignete Ansprechpartner geben, siehe M 3.46 *Ansprechpartner zu Sicherheitsfragen* .

Nachfolgend wird das Maßnahmenbündel für den Bereich "IT-Sicherheitssensibilisierung und -schulung" vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier aus Redundanzgründen verzichtet.

Planung und Konzeption

-	M 2.312	(A)	Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit

-	M 3.44	(A)	Sensibilisierung des Managements für IT-Sicherheit

Beschaffung

-	M 3.48	(A)	Auswahl von Trainern oder Schulungsanbietern

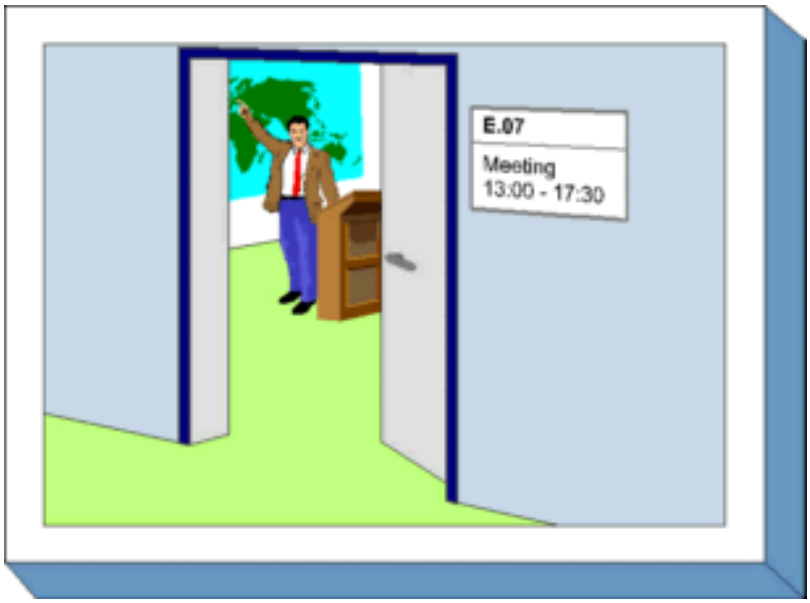
Umsetzung

-	M 3.45	(A)	Planung von Schulungsinhalten zur IT-Sicherheit
-	M 3.5	(A)	Schulung zu IT-Sicherheitsmaßnahmen
-	M 3.46	(A)	Ansprechpartner zu Sicherheitsfragen
-	M 3.49	(B)	Schulung zur Vorgehensweise nach IT-Grundschutz

Betrieb

-	M 2.198	(A)	Sensibilisierung der Mitarbeiter für IT-Sicherheit
-	M 3.4	(A)	Schulung vor Programmnutzung
-	M 3.11	(A)	Schulung des Wartungs- und Administrationspersonals
-	M 3.26	(A)	Einweisung des Personals in den sicheren Umgang mit IT
-	M 3.47	(Z)	Durchführung von Planspielen zur IT-Sicherheit

B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume



Beschreibung

Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im wesentlichen dadurch aus, dass sie

- von wechselnden Personen bzw. Personenkreisen genutzt werden,
- sowohl durch eigenes Personal als auch durch Externe genutzt werden,
- eine in sich geschlossene Nutzung mit dem gleichen Kreis nutzende Personen meist nur kurze Zeit andauert, wenige Stunden bis zu wenigen Tagen,

- mitgebrachte IT-Systeme gemeinsam mit eigener IT betrieben werden (z. B. fremder Laptop am eigenen Beamer),
- die dort genutzten Informationen in der Regel lokal (z. B. auf Laptop oder mobilem Datenträger) vorhanden sind oder aus einem eigens eingerichteten Test- oder Trainingsnetz zur Verfügung gestellt werden. Teilweise ist sogar ein Anschluss an das LAN vorhanden, so dass auf institutionsinterne Daten zugegriffen werden kann.

Aus diesen extrem unterschiedlichen Nutzungen heraus ergibt sich eine Gefährdungslage, die kaum mit denen anderer Räume vergleichbar ist. Das Hauptaugenmerk ist dabei, neben den üblichen Gefährdungen für Räume aller Art, auf die Gefährdung durch den "Spieltrieb" anwesender Personen zu legen.

Gefährdungslage

Für den IT-Grundschutz von Besprechungs-, Veranstaltungs- und Schulungsräumen werden folgende Gefährdungen angenommen:

Organisatorische Mängel:

-	G 2.1	Fehlende oder unzureichende Regelungen
-	G 2.2	Unzureichende Kenntnis über Regelungen
-	G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
-	G 2.104	Inkompatibilität zwischen fremder und eigener IT

Menschliche Fehlhandlungen:

-	G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
-	G 3.78	Fliegende Verkabelung

Technisches Versagen:

-	G 4.1	Ausfall der Stromversorgung
-	G 4.2	Ausfall interner Versorgungsnetze

Vorsätzliche Handlungen:

-	G 5.4	Diebstahl

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Planung und Konzeption

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

-	Die Nutzungsmöglichkeiten von Besprechungs-, Veranstaltungs- und Schulungsräumen variieren sehr stark. Da hiervon auch die erforderlichen Sicherheitsmaßnahmen abhängen, sollte zunächst eine Nutzungsübersicht erstellt werden, das die geplanten Einsatzszenarien berücksichtigt (siehe M 2.331 *Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen*).

-	Basierend auf dem Nutzungskonzept sollten geeignete Räumlichkeiten ausgewählt und ausgestattet werden (siehe M 2.332 *Einrichtung von Besprechungs-, Veranstaltungs- und Schulungsräumen*).

-	Wenn auf LANs oder das Internet zugegriffen werden soll, müssen die Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen sorgfältig abgesichert werden (siehe M 5.124 *Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen*).

Umsetzung

Es müssen Sicherheitsregelungen für Besprechungs-, Veranstaltungs- und Schulungsräume festgelegt sowie technisch und organisatorisch umgesetzt werden. Alle Mitarbeiter müssen darüber informiert werden, welche Nutzungsregelungen zu beachten sind (siehe M 2.333 *Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen*).

Betrieb

Auch in Besprechungs-, Veranstaltungs- und Schulungsräumen muss mit den Einrichtungen und der vorhandenen Technik sorgfältig umgegangen werden. Dazu gehören die Einhaltung der von der Institution vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien.

Aussonderung

Gerade in Besprechungs-, Veranstaltungs- und Schulungsräumen mit

häufig wechselnden Benutzern ist es wichtig, Arbeitsmaterialien wie Datenträger und Papiere sorgsam zu entsorgen und nicht einfach liegen zu lassen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Besprechungs-, Veranstaltungs- und Schulungsräume" vorgestellt.

Planung und Konzeption

-	M 3.9	(Z)	Ergonomischer Arbeitsplatz
-	M 5.77	(Z)	Bildung von Teilnetzen
-	M 2.331	(A)	Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
-	M 2.332	(B)	Einrichtung von Besprechungs-, Veranstaltungs- und Schulungsräumen
-	M 5.124	(C)	Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen

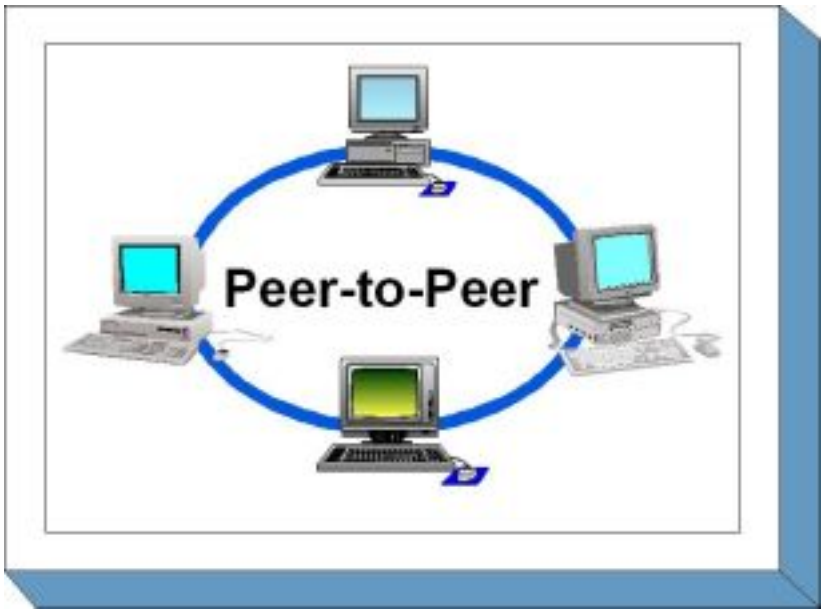
Umsetzung

-	M 1.6	(A)	Einhaltung von Brandschutzvorschriften
-	M 2.69	(B)	Einrichtung von Standardarbeitsplätzen
-	M 2.204	(A)	Verhinderung ungesicherter Netzzugänge
-	M 2.333	(A)	Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen
-	M 4.252	(C)	Sichere Konfiguration von Schulungsrechnern

Betrieb

-	M 1.15	(A)	Geschlossene Fenster und Türen
-	M 2.16	(B)	Beaufsichtigung oder Begleitung von Fremdpersonen
-	M 4.109	(C)	Software-Reinstallation bei Arbeitsplatzrechnern

B 5.1 Peer-to-Peer-Dienste



Beschreibung

Peer-to-Peer-Dienste sind Funktionen auf Arbeitsplatz-Computern, die anderen IT-Systemen im lokalen Netz Ressourcen zur Verfügung stellen, beispielsweise gemeinsamen Zugriff auf die Festplatte oder auf Drucker. Solche Dienste werden von den gängigen Betriebssystemen unterstützt. In diesem Baustein werden die Betriebssysteme Windows für Workgroups (WfW), Windows 95/ NT/2000 und Unix betrachtet, berücksichtigt wird hier aber nur die reine Peer-to-Peer-Funktionalität dieser Betriebssysteme. Auf sicherheitsspezifische Aspekte einzelner Anwendungen bei der Benutzung von Peer-to-Peer-Funktionalitäten, zum Beispiel bezüglich *Mail*, *Exchange*, *Schedule+*, *Direct-Data-Exchange (DDE)* oder *Remote Access Service (RAS)*, wird nur am Rande eingegangen. Weiterhin werden in diesem Kapitel ausschließlich die für Peer-to-Peer-Dienste spezifischen Gefährdungen und Maßnahmen beschrieben, daher sind zusätzlich noch die betriebssystemspezifischen Bausteine zu betrachten. Peer-to-Peer-Kommunikation über das Internet ist nicht Gegenstand dieses Bausteins.

Da Peer-to-Peer-Dienste wesentlich geringere

Sicherheitsfunktionalitäten bieten als durch dedizierte Server bereitgestellte Dienste, sollten Peer-to-Peer-Dienste innerhalb servergestützter Netze nicht verwendet werden.

Gefährdungslage

Für den IT-Grundschutz von Peer-to-Peer-Diensten werden folgende typische Gefährdungen angenommen:

Organisatorische Mängel:

-	G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
-	G 2.65	Komplexität der SAMBA-Konfiguration

Menschliche Fehlhandlungen:

-	G 3.9	Fehlerhafte Administration des IT-Systems
-	G 3.18	Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
-	G 3.19	Speichern von Passwörtern unter WfW und Windows 95
-	G 3.20	Ungewollte Freigabe des Leserechtes bei Schedule+

Vorsätzliche Handlungen:

-	G 5.45	Ausprobieren von Passwörtern unter WfW und Windows 95
-	G 5.46	Maskerade unter WfW
-	G 5.47	Löschen des Post-Office unter WfW

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu

diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Bearbeitung der originären Peer-to-Peer-Maßnahmen sollte zuerst anhand von Maßnahme M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste* eine Sicherheitsstrategie ausgearbeitet werden, da diese die Grundlage für die weiteren Maßnahmen ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Peer-to-Peer-Dienste" vorgestellt:

Planung und Konzeption

-	M 2.67	(A)	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
-	M 5.37	(B)	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz

Umsetzung

-	M 2.94	(B)	Freigabe von Verzeichnissen unter Windows NT
-	M 3.19	(A)	Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten
-	M 4.45	(A)	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
-	M 4.149	(A)	Datei- und Freigabeberechtigungen unter Windows 2000/XP

Betrieb

-	M 2.68	(B)	Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten

-	M 4.46	(A)	Nutzung des Anmeldepasswortes unter WfW und Windows 95
-	M 4.58	(B)	Freigabe von Verzeichnissen unter Windows 95
-	M 5.82	(A)	Sicherer Einsatz von SAMBA
