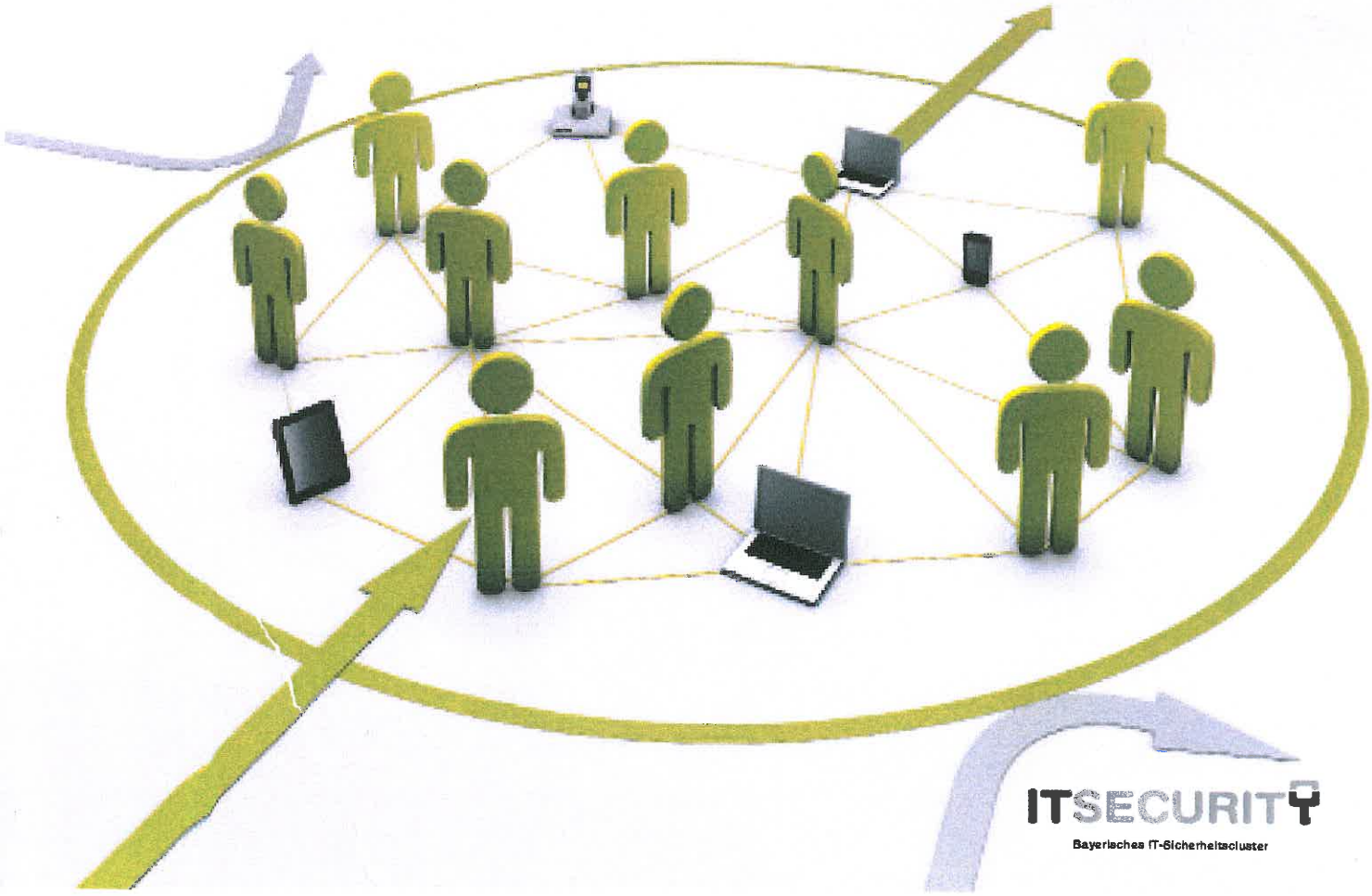
ISIS 12

Informationssicherheit
für den Mittelstand

ISIS12 - Katalog



ITSECURITY

Bayerisches IT-Sicherheitscluster

Impressum

Herausgeber

Bayerischer IT-Sicherheitscluster e.V.
Bruderwöhrdstr. 15 b
93055 Regensburg

Tel: +49 (0) 941-604889-18
Fax: +49 (0) 941-604889-11

Email: sandra.wiesbeck@it-sec-cluster.de
Internet: www.isis12.de
www.it-sicherheit-bayern.de

Redaktion

Sandra Wiesbeck
Katrin Neubauer

Katalog

Version 1.2

Inhaltsverzeichnis

Einleitung

Der ISIS12 Katalog wurde aus den BSI IT-Grundschutzkatalogen (vgl. [1]) und dem de jure Standard ISO/IEC 270001 (vgl. [2]) (Maßnahmenziele A.5 - A.15) bzw. den Konkretisierungen in ISO/IEC 27002 (vgl. [3]) abgeleitet.
Für die ISIS12-Zielgruppe (mittelständische Unternehmen) wurde die Fülle der vorgefundenen Sicherheitsmaßnahmen reduziert. Breitenwirkung, Umsetzbarkeit und trotzdem eine systematische Abdeckung von Gefährdungen standen für die Entwicklung des ISIS12 Katalogs im Mittelpunkt. Auch der Detailierungsgrad, zwischen BSI IT-Grundschutz (extrem) und der ISO/IEC 27001 (minimalistisch und abstrakt), wurde bewusst auf die Zielgruppe der mittelständischen Unternehmen angepasst: Der Anwender bekommt konkret umzusetzende Sicherheitsmaßnahmen für die Entwicklung des Sicherheitskonzepts.

Die im BSI IT-Grundschutzkatalog enthaltenen Bausteine wurden in Verbindung mit den in 2011 zum ersten Mal vom BSI publizierten „Goldenen Regeln" (vgl.[4]) bewusst reduziert, zusammengefasst und vereinfacht; nach dem Grundsatz „So einfach wie möglich - aber nicht einfacher". So wurde etwa aus Gründen der Reduktion von Komplexität bewusst auf betriebssystemspezifische Besonderheiten verzichtet. Nur ein allgemeiner Client-Baustein kommt beim ISIS12 Vorgehensmodell für alle Client-Betriebssysteme zum Einsatz.
Im Gegensatz zur ISO/IEC 27001 stehen mit dem ISIS12-Katalog konkrete Handlungsempfehlungen zur Verfügung, deren Umfang entsprechend der Zielgruppe reduziert wurde.

Abb. 1: Genese des ISIS12 Katalogs

Aufbau des ISIS12-Kataloges

Die Gliederung der BSI IT-Grundschutzkataloge in 5 Schichten (B1 - B5), wurde dazu auf die folgenden vier Schichten reduziert:

- S1: Universale Aspekte
- S2: Infrastruktur
- S3: IT-Systeme und Netze
- S4: Anwendungen

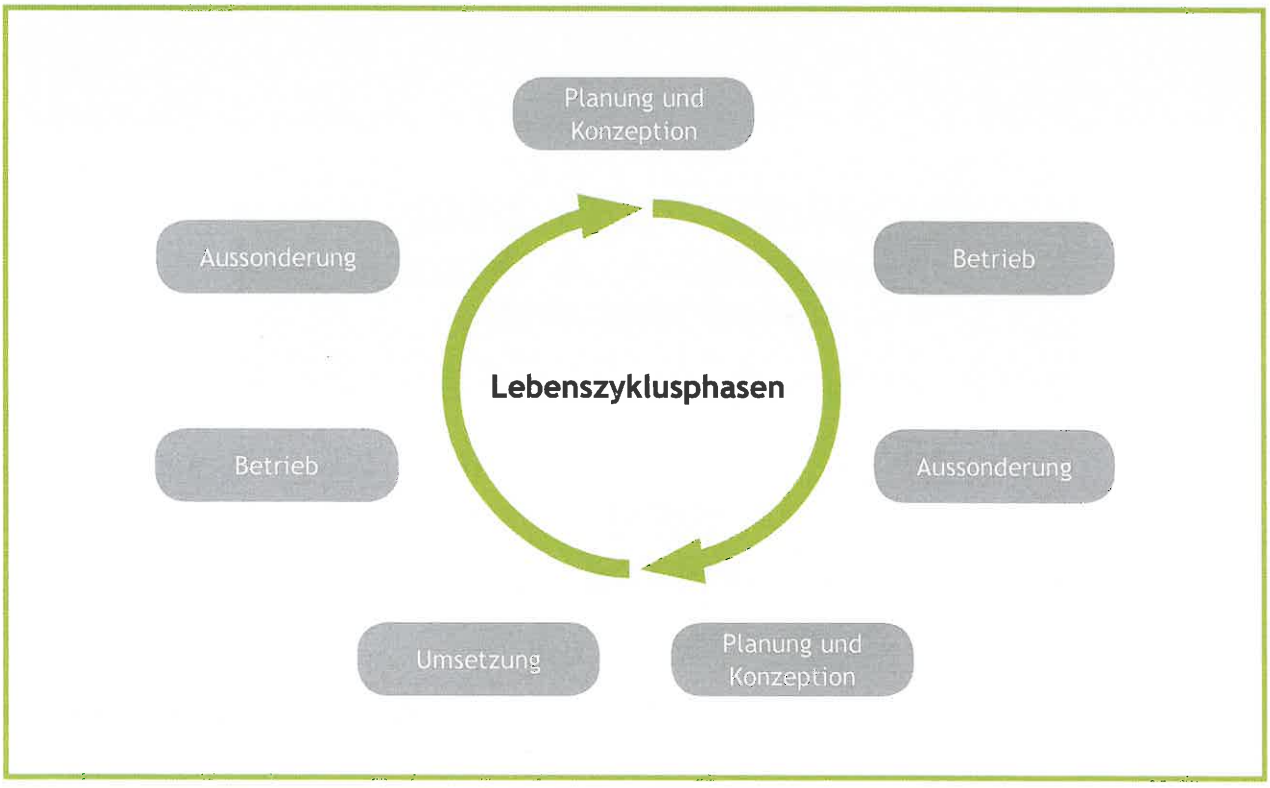
In den Schichten (S1 - S4) finden sich Bausteine mit entsprechenden Sicherheitsmaßnahmen. Die einzelnen Maßnahmen sind in sechs Kategorien unterteilt:

- M1: Infrastruktur
- M2: Organisation
- M3: Personal
- M4: Hardware und Software
- M5: Kommunikation
- M6: Notfallvorsorge

Beispiele:

Infrastruktur:	M 1.15 (A)	Geschlossene Fenster und Türen
Organisation:	M 2.8 (A)	Vergabe von Zugriffsrechten
Personal:	M 3.10 (A)	Auswahl eines vertrauenswürdigen Administrators und Vertreters
Hardware und Software:	M 4.3 (A)	Einsatz von Viren-Schutzprogrammen
Kommunikation:	M 5.33 (B)	Absicherung von Fernwartung
Notfallvorsorge:	M 6.96 (A)	Notfallvorsorge für einen Server

Die Maßnahmen selbst sind in verschiedene Lebenszyklusphasen unterteilt:



Zudem finden sich noch sogenannte Siegelstufen:

- (A) Einstiegstufe
- (B) Aufbaustufe
- (C) Zertifizierung

Diese Kategorisierung aus den BSI IT-Grundschutzkatalogen wurde aus Gründen der Transparenz übernommen, obwohl diese nicht immer nachvollziehbar ist.

Beispiel:

M 6.96 (A) Notfallvorsorge für einen Server

M 6. > Notfallvorsorge
96 > laufende Nummer
(A) > Einstiegsstufe

Anmerkung:

Der ISIS12 Katalog wird jährlich im Turnus der Erscheinung der BSI Ergänzungslieferung des IT-Grundschutzkataloges aktualisiert und angepasst. Die vom BSI jährlich veröffentlichte „Zuordungstabelle ISO 27001 und 27002 und IT-Grundschutz" (vgl. [5]) wird dazu als weiteres Filterkriterium herangezogen.

Arbeit mit dem ISIS12-Katalog

Wird das ISIS12-Tool verwendet, so gestaltet sich die Arbeit mit dem ISIS12-Katalog sehr einfach und komfortabel. Die notwendige Modellierung, also die Zuordnung von Bausteinen, mit den darin enthaltenen Maßnahmen, geschieht beim Eintrag der Anwendungen und den damit verbunden IT-Zielobjekten (IT-Systeme, Netze, Räume und Gebäude) automatisch. Es werden die betreffenden Bausteine aus den Schichten 2-4 den entsprechenden Objekten im definierten Informationsverbund zugeordnet. Die Bausteine aus der Schicht 1 (Universale Aspekte) werden, wie im Kapitel 8 des ISIS12-Vorgehensmodells beschrieben, notwendigerweise komplett dem Informationsverbund zugeordnet. Die entsprechenden Maßnahmen werden somit im ISIS12-Tool zur weiteren Verarbeitung bereit gestellt.
Wird ohne Tool-Unterstützung gearbeitet, so müssen diese soeben beschriebenen Zuordnungen zur weiteren Verarbeitung manuell erfolgen.

S1: Universale Aspekte

In dieser Schicht finden sich Bausteine, mit entsprechenden Sicherheitsmaßnahmen, die unabhängig vom jeweiligen Unternehmen für den gesamten Informationsverbund anzuwenden sind.

B 1.1 ISMS

S1

Mit (Informations-)Sicherheitsmanagement wird die Planungs- und Lenkungsaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden.

- Die Leitungsebene muss die Gesamtverantwortung für Informationssicherheit in der Institution übernehmen.
- Die Leitungsebene muss eine übergeordnete Leitlinie zur Informationssicherheit verabschieden, die den Stellenwert der Informationssicherheit, die Sicherheitsziele und die wichtigsten Aspekte der Sicherheitsstrategie beschreibt.
- Die Sicherheitsleitlinie muss allen Mitarbeitern und sonstigen Mitgliedern der Institution bekannt gegeben werden.
- Die Leitungsebene muss einen IT-Sicherheitsbeauftragten benennen, der die Informationssicherheit in der Institution fördert und den Sicherheitsprozess steuert und koordiniert.
- Der IT-Sicherheitsbeauftragte muss mit angemessenen Ressourcen ausgestattet werden und berichtet bei Bedarf direkt an die Leitungsebene.
- Im Rahmen des Sicherheitsprozesses müssen für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden.
- Alle Sicherheitsmaßnahmen müssen systematisch in Sicherheitskonzepten dokumentiert und regelmäßig aktualisiert werden.
- Alle Mitarbeiter der Institution und sonstige relevante Personen (wie extern Beschäftigte oder Projektmitarbeiter) müssen systematisch und zielgruppengerecht zu Sicherheitsrisiken sensibilisiert und zu Fragen der Informationssicherheit geschult werden.
- Der Sicherheitsprozess, die Sicherheitskonzepte, die Leitlinie zur Informationssicherheit und die Organisationsstruktur für Informationssicherheit müssen regelmäßig auf Wirksamkeit und Angemessenheit überprüft und aktualisiert werden (vgl. [6]).

Planung und Konzeption
M 2.192 (A) Erstellung einer Leitlinie zur Informationssicherheit
M 2.335 (A) Festlegung der Sicherheitsziele und -strategie
M 2.336 (A) Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene

Umsetzung
M 2.193 (A) Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
M 2.195 (A) Erstellung eines Sicherheitskonzepts
M 2.197 (A) Integration der Mitarbeiter in den Sicherheitsprozess
M 2.337 (A) Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
M 2.199 (A) Aufrechterhaltung der Informationssicherheit
M 2.201 (C) Dokumentation des Sicherheitsprozesses

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B1.0.
Die Maßnahmen wurde im Rahmen der bereits durchlaufenen Schritte erfüllt.

B 1.2 Organisation / Personal

S1

Organisation

Viele Sicherheitsmaßnahmen sind auf organisatorischer Ebene zu ergreifen, insbesondere gehören dazu die allgemeinen und übergreifenden Maßnahmen, die als organisatorische Standardmaßnahmen zur Erreichung eines Mindestschutzniveaus erforderlich sind.

- Für alle Aufgaben im Sicherheitsprozess müssen sowohl Verantwortlichkeiten als auch Befugnisse festgelegt sein. Alle Mitarbeiter müssen auf ihre Verantwortung für die Informationssicherheit in ihrem Einflussbereich hingewiesen worden sein.
- Für alle Informationen, Anwendungen und IT-Komponenten sollte festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist. Es muss auch klar geregelt sein, welche Informationen mit wem ausgetauscht werden dürfen und wie diese dabei zu schützen sind.
- Es müssen konkrete Handlungsanweisungen und Verantwortlichkeiten zur Informationssicherheit festgelegt werden. Diese Regelungen sind den betroffenen Mitarbeitern in geeigneter Weise bekannt zu geben.
- Die Aufgabenverteilung und die hierfür erforderlichen Funktionen sind so zu strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu verhindern (Funktionstrennung).
- Auf den verschiedenen Ebenen müssen angemessene und praktikable Berechtigungen vergeben werden (z. B. für den Zutritt zu Räumen, Zugang zu IT-Systemen, Zugriff auf Anwendungen). Es sollten immer nur so viele Rechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Es muss ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben.
- Die Betriebsmittel, die zur Aufgabenerfüllung und zur Einhaltung der Sicherheitsanforderungen erforderlich sind, müssen in ausreichender Menge vorhanden sein. Es muss geeignete Prüfverfahren vor Einsatz der Betriebsmittel geben. Für die Bestandsführung müssen die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Um den Missbrauch von Daten zu verhindern, sollte die zuverlässige Löschung oder Vernichtung von Betriebsmitteln geregelt sein.
- Es sind Regelungen für Ersatzteilbeschaffung, Reparaturen und Wartungsarbeiten festzulegen, um auf Störungen bei einer nicht funktionierenden Infrastruktur adäquat reagieren zu können. Bei bestehenden Wartungsverträgen sind feste Wartungsintervalle und Wartungsdetails einzelner IT-Systeme (oder Gruppen) verbindlich zu regeln.
- Betriebs- und Sachmittel, die besonderen Schutzbedingungen unterliegen, müssen so entsorgt werden, dass keine Rückschlüsse auf ihre Verwendung oder Inhalte gezogen werden können. Den Mitarbeitern sollte bekannt sein, wie mit ausgesonderten Datenträgern vor einer Vernichtung umzugehen ist. Es sollte hierfür ein Handlungsleitfaden zur Verfügung stehen.
- Es muss geregelt sein, welche Reaktionen auf Verletzungen der Sicherheitsvorgaben erfolgen sollen. Nur so ist eine zielgerichtete und zeitnahe Reaktion möglich.
- In allen Geschäftsprozessen muss es funktionierende Vertretungsregelungen geben (vgl. [6]).

S1

Personal

Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen ab. Im Personalbereich sind daher von der Einstellung bis zum Weggang von Mitarbeitern aus der Institution eine Reihe von Sicherheitsmaßnahmen erforderlich.

- Zur geregelten Einarbeitung neuer Mitarbeiter müssen diese auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen werden.
- Alle Mitarbeiter sollten umgehend über Regelungen zur Informationssicherheit, deren Veränderungen und ihre spezifischen Auswirkungen auf einen Geschäftsprozess oder auf das jeweilige Arbeitsumfeld unterrichtet werden.
- Die Mitarbeiter sollten dazu motiviert werden, Regelungen zur Informationssicherheit eigenverantwortlich umzusetzen. Dazu sollten sie durch geeignete Schulungen motiviert und gefördert werden.
- Administrations- und Wartungspersonal muss detailliert über die von ihnen betreuten Systeme und deren Sicherheitseigenschaften ausgebildet werden, da diese aufgrund der weitgehenden Rechte im Umgang mit der IT eine hohe Verantwortung tragen.
- Es muss Vertretungsregelungen in allen Bereichen geben. Um eine kontinuierliche Verfügbarkeit wichtiger Prozesse zu erreichen, muss insbesondere dafür gesorgt werden, dass Schlüsselpositionen immer besetzt sind, sobald dies von den Abläufen her gefordert wird.
- Kommunikationsprobleme innerhalb der Institution, persönliche Probleme von Mitarbeitern, ein schlechtes Betriebsklima und andere Faktoren können zu Unzufriedenheit und damit zu Sicherheitsrisiken führen. Um hier rechtzeitig vorbeugen zu können, sollten geeignete Anlaufstellen (z. B. Mitarbeitervertretungen) eingerichtet werden.
- Bei Mitarbeitern, die die Institution verlassen oder andere Funktionen übernehmen, müssen bestehende Regelungen mit erhöhter Sorgfalt überprüft werden. Nachfolger müssen eingearbeitet werden, Unterlagen sind zurückzugeben und erteilte Berechtigungen sind wieder zu entziehen. Vor der Verabschiedung sollte noch einmal explizit auf Verschwiegenheitsverpflichtungen hingewiesen werden.
- Alle Mitarbeiter sollten explizit darauf verpflichtet werden, einschlägige Gesetze, Vorschriften und interne Regelungen einzuhalten. Außerdem sollten alle Mitarbeiter darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind, solange sie nicht anders gekennzeichnet sind (vgl. [6]).

B 1.2 Organisation / Personal

S1

Planung und Konzeption
M 2.1 (A) Festlegung von Verantwortlichkeiten und Regelungen
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 2.393 (A) Regelung des Informationsaustausches

Betrieb
M 2.6 (A) Vergabe von Zutrittsberechtigungen
M 2.7 (A) Vergabe von Zugangsberechtigungen
M 2.8 (A) Vergabe von Zugriffsrechten
M 2.16 (B) Beaufsichtigung oder Begleitung von Fremdpersonen
M 2.39 (B) Reaktion auf Verletzungen der Sicherheitsvorgaben
M 5.33 (B) Absicherung von Fernwartung

Aussonderung
M 2.13 (A) Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

Planung und Konzeption
M 2.226 (A) Regelungen für den Einsatz von Fremdpersonal

Umsetzung
M 3.1 (A) Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
M 3.10 (A) Auswahl eines vertrauenswürdigen Administrators und Vertreters

Betrieb
M 3.3 (A) Vertretungsregelungen
M 3.4 (A) Schulung vor Programmnutzung
M 3.5 (A) Schulung zu Sicherheitsmaßnahmen
M 3.11 (A) Schulung des Wartungs- und Administrationspersonals

Aussonderung
M 3.6 (A) Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

Anmerkung:
Dieser Baustein entspricht den gekürzten BSI IT-Grundschutzbausteinen B1.1 und B1.2.

B 1.3 Notfallmanagment

S1

Das Notfallmanagement einer Behörde oder eines Unternehmens umfasst sowohl die Notfallvorsorge, als auch Aspekte zur Bewältigung eines Notfalls. Dazu ist der Aufbau geeigneter Organisationsstrukturen und Regelungen für den Umgang mit Notfällen aller Art notwendig.

- Die Leitungsebene muss hinter den Zielen des Notfallmanagements stehen und sich ihrer Verantwortung dafür bewusst sein. Die Leitungsebene muss den Notfallmanagement-Prozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird.
- Es müssen die organisatorischen Voraussetzungen für das Notfallmanagement geschaffen werden, d. h. Rollen und Verantwortlichkeiten müssen definiert und von der Leitungsebene ein ausreichendes Budget zur Verfügung gestellt werden. Es muss ein Notfallbeauftragter benannt werden, der den Notfallmanagement-Prozess steuert und koordiniert.
- Auf Basis einer Schutzbedarfsanalyse oder einer Business Impact Analyse und einer anschließenden Risikoanalyse müssen die Auswirkungen von Geschäftsunterbrechungen untersucht sowie die Verfügbarkeitsanforderungen an die Geschäftsprozesse und deren benötigten Ressourcen ermittelt werden.
- Die kritischen Prozesse müssen definiert und analysiert werden, danach folgt die Auswahl einer angemessenen Strategie, um einerseits Ausfallrisiken zu reduzieren und andererseits nach dem Auftreten von Notfällen Ausfallzeiten verkürzen zu können. Diese werden in einem Notfallvorsorgekonzept dokumentiert.
- Für eine rasche Notfallbewältigung ist ein Notfallhandbuch zu erstellen, in dem beschrieben wird, welche Maßnahmen bei einem Notfall durchgeführt und umgesetzt werden müssen. Das Notfallhandbuch sollte mindestens Alarmierungspläne, Meldewege, Notfall-, Wiederanlauf-, Wiederherstellungs- und Geschäftsfortführungspläne, sowie alle wichtigen Informationen und Aufgabenzuordungen der Mitglieder des Notfallteams enthalten.
- Die entwickelten Maßnahmen und Verfahren zur Notfallbewältigung müssen regelmäßig durch Übungen und Tests auf ihre Wirksamkeit untersucht werden. Notfall-Übungen erleichtern es, sich rechtzeitig im Vorfeld auf eine Notfallsituation einstellen und Fehler in der Notfallkonzeption erkennen zu können.
- Um ein effizientes Notfallmanagement aufrecht zu erhalten, müssen nicht nur die Dokumente regelmäßig aktualisiert werden, sondern auch die Notfallvorsorgemaßnahmen überprüft und angepasst werden.
- Alle Mitarbeiter der Institution müssen systematisch und zielgruppengerecht sensibilisiert und im Umgang mit Notfallsituationen geschult werden. So wird in der Institution eine Notfallmanagement-Kultur etabliert (vgl. [6]).

Planung und Konzeption

M 6.111 (A) Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene

Umsetzung

M 6.112 (A) Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement
M 6.114 (A) Erstellung eines Notfallkonzepts
M 6.115 (C) Integration der Mitarbeiter in den Notfallmanagement-Prozess

Betrieb

M 6.117 (B) Tests und Notfallübungen
M 6.118 (A) Überprüfung und Aufrechterhaltung der Notfallmaßnahmen

Anmerkung:

Dieser Baustein entspricht den gekürzten BSI IT-Grundschutzbausteinen B1.3.

B 1.4 Datensicherung

S1

Computersysteme und Datenträger (z. B. Festplatten) können ausfallen oder manipuliert werden. Durch den Verlust oder die Veränderungen von gespeicherten geschäftsprozessrelevanten Daten können gravierende Schäden verursacht werden. Durch regelmäßige Datensicherungen können Schäden durch Ausfälle von Datenträgern, Schadsoftware oder Manipulationen an Datenbeständen zwar nicht verhindert, deren Auswirkungen aber minimiert werden.

- Es muss festgelegt werden, wer für die Datensicherung der einzelnen IT-Systeme zuständig ist.
- Neben dem Datum müssen Umfang, Art der Durchführung der Sicherung sowie gewählte Parameter und die eingesetzte Hard- und Software der Datensicherungen dokumentiert werden. Ebenso sollten die wichtigsten Informationen für eine spätere Datenrekonstruktion festgehalten werden.
- Die eingesetzten Speichermedien sollten ausreichend Speicherkapazität haben und müssen eindeutig beschriftet sein.
- Auch die Daten mobiler IT-Systeme wie Laptops, PDAs und Handys müssen regelmäßig gesichert werden.
- Backup-Datenträger müssen einerseits im Bedarfsfall schnell verfügbar sein, andererseits sollten sie aber räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden, damit sie bei Notlagen wie z. B. Brand oder Hochwasser verfügbar sind.
- Es sollten nur befugte Personen auf die Datensicherungsmedien zugreifen dürfen. Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden.
- Es muss regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt werden können (vgl. [6]).

Planung und Konzeption
M 6.33 (B) Entwicklung eines Datensicherungskonzeptes
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 6.37 (A) Dokumentation der Datensicherung

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

Notfallvorsorge
M 6.32 (A) Regelmäßige Datensicherung
M 6.41 (A) Übungen zur Datenrekonstruktion

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B1.4.

B 1.5 Datenschutz

S1

Jeder Einzelne muss das Recht haben, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen („informationelles Selbstbestimmungsrecht"). Es ist die Aufgabe des Datenschutzes, dass dieses Recht durch die Verarbeitung und den Umgang mit personenbezogenen Daten nicht beeinträchtigt wird.

- Die Leitungsebene muss einen Datenschutzbeauftragten benennen, der den Datenschutz in der Institution fördert und den ordnungsmäßigen Umgang mit personenbezogenen Daten steuert und kontrolliert.
- Der Datenschutzbeauftragte muss mit angemessenen Ressourcen ausgestattet werden. Er muss bei Bedarf direkt an die Leitungsebene berichten können.
- Es sollte klare Regeln für den Umgang mit personenbezogenen Daten geben, die allen Mitarbeitern und sonstigen Mitgliedern der Institution bekannt gegeben werden. Alle Beschäftigten sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten.
- Der Datenschutzbeauftragte muss bei allen Änderungen in Geschäftsprozessen und neuen Projekten eingebunden werden, so dass er die rechtlichen Rahmenbedingungen für die Datenverarbeitung prüfen und geeignete Vorkehrungen ausarbeiten kann.
- Alle Mitarbeiter der Institution und sonstige relevante Personen (wie extern Beschäftigte oder Projektmitarbeiter) müssen systematisch und zielgruppengerecht zu Datenschutzfragen sensibilisiert und zum Umgang mit personenbezogenen Daten geschult werden.
- Die Leitungsebene muss die Gesamtverantwortung für den Datenschutz in der Institution übernehmen (vgl. [6]).

Planung und Konzeption

M 7.1 (C) Datenschutzmanagement
M 7.3 (A) Aspekte eines Datenschutzkonzeptes
M 7.4 (A) Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten
M 7.5 (A) Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

Umsetzung

M 7.6 (A) Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten
M 7.7 (A) Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten
M 7.8 (A) Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten
M 7.11 (A) Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten
M 7.12 (A) Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten

Betrieb

M 7.14 (A) Aufrechterhaltung des Datenschutzes im laufenden Betrieb
M 7.15 (A) Datenschutzgerechte Löschung/Vernichtung

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B1.5.

B 1.6 Schutz vor Malware

S1

Wenn IT-Systeme mit Schadsoftware (Viren, Würmer, Trojanische Pferde usw.) befallen werden, kann dies die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und der darauf gespeicherten Daten gefährden. Für einen effizienten Computer-Virenschutz ist daher zu sorgen.

- Innerhalb der vernetzten Strukturen einer Institution müssen Viren-Schutzprogramme so auf den IT-Systemen platziert werden, dass alle möglichen Infektionswege abgedeckt sind. Dabei muss sichergestellt werden, dass auch die mobilen Endgeräte ausreichend geschützt sind.
- Die Viren-Schutzprogramme müssen regelmäßig durch zeitnahes Einspielen von Updates und Patches auf den aktuellen Stand gebracht werden.
- Schadprogramm-Signaturen müssen in möglichst kurzen Abständen, mindestens täglich, aktualisiert werden.
- Auf allen IT-Systemen müssen für die Betriebssysteme sowie für alle installierten Treiber und Programme zeitnah die jeweils hierfür veröffentlichten sicherheitsrelevanten Updates und Patches eingespielt werden. Dies gilt besonders für Programme, mit denen auf Fremdnetze zugegriffen wird, beispielsweise Browser.
- Die Mitarbeiter müssen darüber informiert sein, wie sie eine Infektion mit Schadsoftware verhindern können, woran sie sie erkennen und wie sie sich in einem solchen Fall zu verhalten haben.
- Erkannte Infektionen mit Schadprogrammen müssen zeitnah an die zuständigen Fachkräfte gemeldet werden. Die Meldung sollte möglichst automatisch erfolgen.
- Infizierte IT-Systeme müssen unverzüglich von allen Datennetzen getrennt werden und dürfen bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden.
- Entdeckte Schadprogramme müssen zeitnah durch fachkundiges Personal entfernt werden.
- Es müssen zentrale Ansprechpartner mit der notwendigen Fachkunde für das Thema Schadsoftware benannt werden (vgl. [6]).

Planung und Konzeption
M 2.154 (A) Erstellung eines Sicherheitskonzeptes gegen Schadprogramme
M 2.160 (A) Regelungen zum Schutz vor Schadprogrammen

Beschaffung
M 2.157 (A) Auswahl eines geeigneten Viren-Schutzprogramms

Betrieb
M 2.158 (A) Meldung von Schadprogramm-Infektionen
M 2.159 (A) Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen
M 2.224 (A) Vorbeugung gegen Schadprogramme
M 4.3 (A) Einsatz von Viren-Schutzprogrammen

Notfallvorsorge
M 6.23 (A) Verhaltensregeln bei Auftreten von Schadprogrammen

Anmerkung:
Dieser Baustein entspricht den gekürzten BSI IT-Grundschutzbausteinen B1.6.

B 1.7 Hard- und Softwaremanagement

S1

Für den sicheren Einsatz von IT-Systemen und IT-Anwendungen in einer Institution müssen sowohl die einzelnen IT-Komponenten angemessen geschützt, als auch alle Abläufe und Vorgänge, die diese IT-Systeme berühren, so gestaltet werden, dass das angestrebte IT-Sicherheitsniveau erreicht und beibehalten wird. Sicherheit sollte integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein. Hierfür sind klare Regelungen erforderlich, um einen ordnungsgemäßen und sicheren IT-Betrieb sicherstellen zu können.

- Durch eine geeignete Benutzerkonten- und Rechteverwaltung muss sichergestellt werden, dass nur diejenigen Personen Zugang auf IT-Systeme und Zugriff auf Applikationen und Informationen haben, die aufgrund ihrer Aufgaben dazu berechtigt sind.
- Die Verantwortung für die Administration von IT-Systemen und Anwendungen muss klar definiert werden.
- Es müssen Richtlinien für den IT-Betrieb und die IT-Nutzung definiert und den Benutzern bekannt gemacht werden. Dazu gehören auch Richtlinien für die Informationssicherheit.
- Die Mitarbeiter sowie alle, die Zugang zu internen Informationen haben, müssen zum sicheren Umgang mit Informationstechnik und Informationen sensibilisiert und geschult werden. Für Fragen der Benutzer zur Informationssicherheit und zu IT-Themen sollte eine Betreuung sichergestellt sein.
- Aktuelle sicherheitsrelevante Updates und Patches müssen zeitnah auf allen Systemen installiert werden.
- Systemkonfigurationen müssen ausreichend dokumentiert werden. Außerdem müssen Installationshinweise, Benutzerhandbücher und -Anleitungen vorhanden sein, um Probleme zu vermeiden und um den Betrieb nach Ausfällen wieder herzustellen.
- Um sicherzustellen, dass nur Befugte auf Systeme und Informationen zugreifen können, ist es wichtig, dass sich jeder vor Nutzung von IT-Systemen und IT-Anwendungen authentisieren muss. Dazu sind Regelungen, z. B. für den Umgang mit Passwörtern und deren Gestaltung, zu definieren. Die Benutzer müssen über die Regelungen und deren Anwendung, sowie deren Hintergründe informiert werden.
- IT-Systeme sind weniger angreifbar, wenn sie nur minimal nach außen geöffnet sind. Daher muss genau überlegt werden, welche Anwendungen und Dienste auf einem System (Internet, Fernzugriff, ...) sinnvoll sind. Nur diese sollten installiert oder aktiviert werden.
- Der Hard- und Software-Bestand muss regelmäßig kontrolliert werden, nicht freigegebene Hard- oder Software muss entfernt werden, bei Verlust oder Diebstahl von IT-Systemen oder Komponenten müssen sofort geeignete Maßnahmen ergriffen werden (vgl. [6]).

Planung und Konzeption
M 2.9 (A) Nutzungsverbot nicht freigegebener Hard- und Software
M 2.11 (A) Regelung des Passwortgebrauchs
M 2.30 (A) Regelung für die Einrichtung von Benutzern / Benutzergruppen
M 2.214 (A) Konzeption des IT-Betriebs
M 2.220 (A) Richtlinien für die Zugriffs- bzw. Zugangskontrolle
M 2.221 (A) Änderungsmanagement

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

Umsetzung
M 1.32 (B) Geeignete Aufstellung von Druckern und Kopierern
M 2.25 (A) Dokumentation der Systemkonfiguration
M 2.26 (A) Ernennung eines Administrators und eines Vertreters
M 2.204 (A) Verhinderung ungesicherter Netzzugänge
M 4.1 (A) Passwortschutz für IT-Systeme
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

B 1.7 Hard- und Softwaremanagement

S1

Betrieb
M 2.31 (A) Dokumentation der zugelassenen Benutzer und Rechteprofile
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 2.219 (A) Kontinuierliche Dokumentation der Informationsverarbeitung
M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen

Aussonderung
M 2.167 (B) Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten
M 4.234 (B) Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B1.9

B 1.8 Outsourcing

S1

Beim Outsourcing werden Arbeits- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Outsourcing kann sowohl Nutzung und Betrieb von Hardware und Software, aber auch Dienstleistungen betreffen. Dabei ist es unerheblich, ob die Leistung in den Räumlichkeiten des Auftraggebers oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters erbracht wird. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation, einer Webseite oder des Wachdienstes.

- Vor der Entscheidung Geschäftsprozesse auszulagern, muss überlegt werden, ob und in welcher Form dies möglich ist. Hierbei müssen neben anderen Rahmenbedingungen auch die sicherheitsrelevanten Aspekte einbezogen werden.
- Sobald die Entscheidung zum Outsourcing gefallen ist, müssen die wesentlichen übergeordneten Sicherheitsanforderungen für das Outsourcing-Vorhaben festgelegt werden. Diese sind unter anderem die Basis für die Auswahl eines Outsourcing-Dienstleisters.
- Bei der Vertragsgestaltung mit dem Outsourcing-Dienstleisters müssen möglichst detailliert die IT-Sicherheitsanforderungen und die Kriterien zur Messung von Servicequalität und Sicherheit beschrieben werden. Im Vertrag müssen auch Auskunfts-, Mitwirkungs- und Revisionspflichten geregelt sein.
- Bei der Übertragung der Aufgaben müssen klare Führungsstrukturen geschaffen und auf beiden Seiten eindeutige Ansprechpartner benannt werden. Außerdem müssen ausreichende Tests geplant und durchgeführt werden, damit die Produktionseinführung reibungslos erfolgen kann. - Auch während des laufenden Betriebs eines Outsourcing-Vorhabens muss der Auftraggeber regelmäßige Kontrollen zur Aufrechterhaltung der IT-Sicherheit beim Dienstleister durchführen (lassen).
- Nichts dauert ewig. Daher müssen Eigentumsrechte an Hard- und Software sowie die Rückgabe der Datenbestände vom Dienstleister geklärt sein. Außerdem müssen alle erforderlichen Informationen für die Weiterführung des Betriebs von IT-Systemen und IT-Anwendungen ausreichend dokumentiert sein (vgl. [6]).

Planung und Konzeption
M 2.42 (A) Festlegung der möglichen Kommunikationspartner
M 2.221 (A) Änderungsmanagement
M 2.226 (A) Regelungen für den Einsatz von Fremdpersonal

Beschaffung
M 2.252 (A) Wahl eines geeigneten Outsourcing-Dienstleisters

Umsetzung
M 2.253 (A) Vertragsgestaltung mit dem Outsourcing-Dienstleister
M 2.255 (A) Sichere Migration bei Outsourcing-Vorhaben

Betrieb
M 2.256 (A) Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb

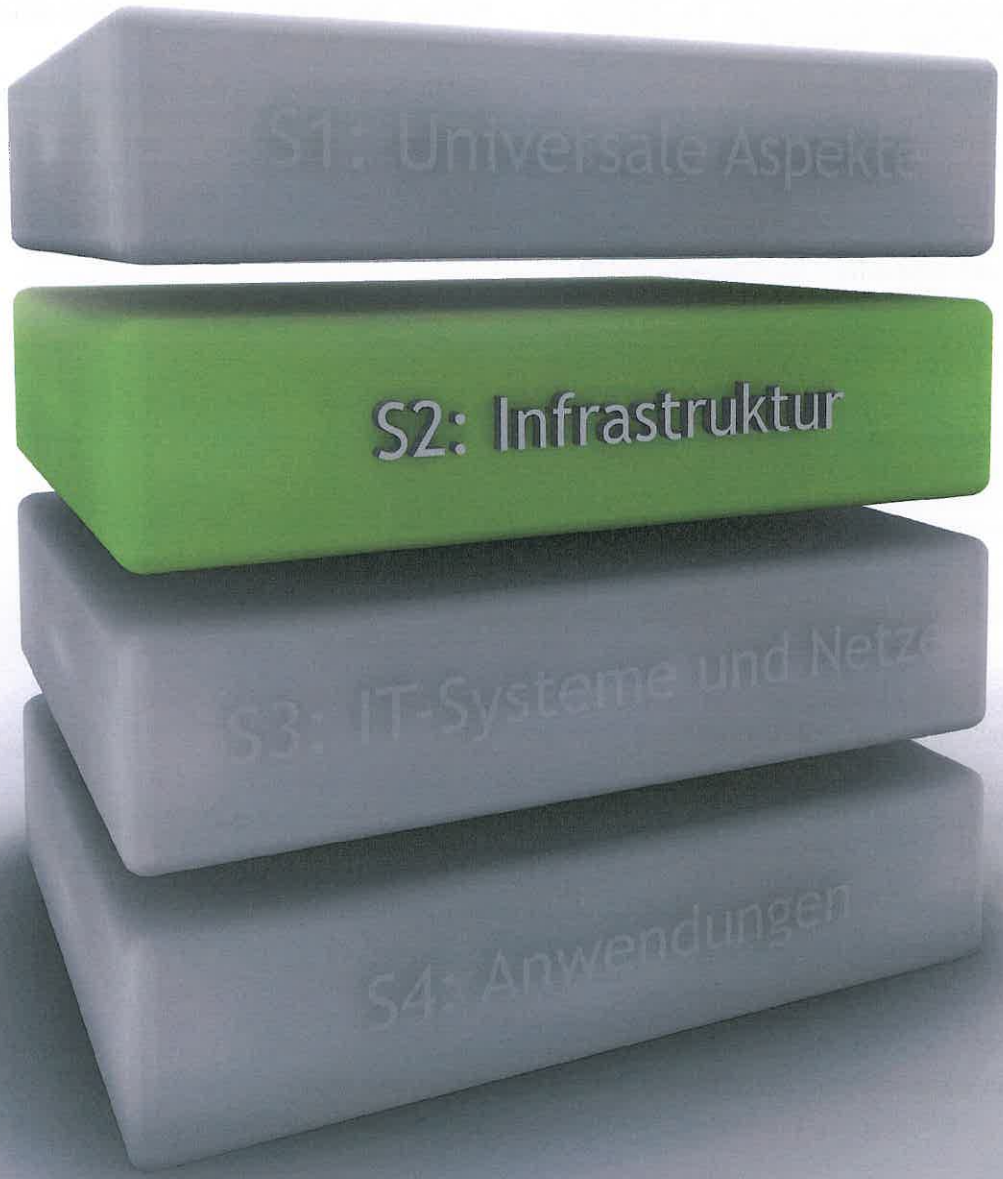
Aussonderung
M 2.307 (A) Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses

Notfallvorsorge
M 6.83 (A) Notfallvorsorge beim Outsourcing

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B1.11.

S2: Infrastruktur

Hierunter fallen speziell die Bausteine für die Bereiche Gebäude, Räume, Verkabelung, mobile Arbeitsplätze und entsprechende verwandte Bausteine.



B 2.1 Gebäude

S2

Ein Gebäude ermöglicht einer Institution durch seine Infrastruktureinrichtungen erst den Betrieb der Geschäftsprozesse und der zugehörigen IT. Es bildet den äußeren Schutz der Informationen und Ressourcen und muss deshalb ausreichend geschützt werden. Dabei muss einerseits das Bauwerk (Wände, Decken, Böden, Dach, Fenster und Türen) betrachtet werden und andererseits alle gebäudeweiten Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung, Rohrpost etc.

- Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein.
- Bei der Raumplanung sind die zu erwartenden elektrischen Anschlusswerte und die abzuführende Wärmemenge zu bestimmen. Bei Änderungen der Raumnutzung oder der IT-Ausstattung sind die Elektroinstallation und die Kühlung zu prüfen und anzupassen, wenn nötig.
- Es muss ein umfassendes Blitz- und Überspannungsschutzkonzept erstellt und realisiert werden
- Die aus der Bauordnung erwachsenden Vorschriften zum Brandschutz sind für die Anforderungen des Brandschutzes der IT nicht ausreichend. Daher ist ein IT-bezogenes Brandschutzkonzept zu erstellen und umzusetzen. Es muss ein Brandschutzbeauftragter benannt werden. Brandschutzbegehungen sollten ein- bis zweimal im Jahr stattfinden.
- Für schutzbedürftige Gebäudeteile, Räume, Verteiler der Versorgungseinrichtungen (Strom, Wasser, Gas, Telefon, etc.) ist eine Zutrittsregelung und -kontrolle festzulegen. Hierbei sollten die betroffenen Bereiche eindeutig bestimmt und die Zahl der zutrittsberechtigten Personen auf ein Mindestmaß reduziert werden. Andere Personen sollten erst nach vorheriger Prüfung der Notwendigkeit Zutritt erhalten. Alle erteilten Zutrittsberechtigungen sollten dokumentiert werden.
- Für alle Schlösser des Gebäudes ist ein Schließplan zu erstellen, dabei ist die Verwaltung der Schlüssel zentral zu regeln. Es müssen Reserveschlüssel vorhanden sein und sicher, aber für Notfälle griffbereit aufbewahrt werden.
- In unbenutzten Räumen sind Fenster und nach außen gehende Türen (Balkone, Terrassen) zu schließen.
- Es sind genaue Lagepläne aller Versorgungsleitungen im Gebäude und auf dem dazugehörenden Grundstück zu führen und alle die Leitungen betreffenden Sachverhalte aufzunehmen.
- Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für einen sicheren IT-Betrieb. Dabei umfasst die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher.
- Die elektrotechnische Verkabelung muss für den Bedarf angemessen sein, eine Überlast ist zu vermeiden.
- Für die elektrotechnische Verkabelung sind geeignete Kabeltypen unter physikalischmechanischer Sicht auszuwählen, die dem jeweiligen Einsatzzweck gerecht werden.
- Brandschutzbestimmungen müssen auf jeden Fall beachtet und elektrische Zündquellen, wie z. B. nicht überprüfte Steckdosenleisten oder ähnliches, vermieden werden. Der Brandschutzbeauftragte ist aus diesen Gründen frühzeitig mit einzubeziehen (vgl. [6]).

B 2.1 Gebäude

S2

- Es muss ein geeigneter Überspannungsschutz vorhanden sein, um mögliche Schäden an IT-Geräten in Netzen durch direkten Blitzeinschlag, Einkopplung und Schalthandlungen zu reduzieren. Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und ersetzt werden, wenn dies erforderlich ist.
- Leitungen und Verteiler sind gegen unbefugte Zugriffe zu sichern. Die Zahl der Stellen, an denen das Kabel oder Verteiler zugänglich sind, sollte auf ein Mindestmaß reduziert werden.
- Die elektrotechnische Verkabelung ist so zu gestalten, dass Fehlerstromfreiheit gewährleistet ist, da solche Fehlerströme zu schädlichen Ausgleichsströmen auf Schirmungen führen können. Die Fehlerstromfreiheit muss im laufenden Betrieb aufrechterhalten werden.
- Insofern Veränderungen an der elektrotechnischen Verkabelung vorgenommen werden oder Gebäude und Räume neu verkabelt werden, ist die elektrotechnische Verkabelung genau zu dokumentieren, beispielsweise auf einem Gebäude- oder Raumplan. Bei der Dokumentation an den Kabeln ist darauf zu achten, dass diese für Befugte nachvollziehbar, aber ansonsten neutral ist.
- Die IT-Verkabelung ist die physikalische Grundlage der internen Kommunikationsnetze einer Institution und reicht von den Übergabepunkten aus einem Fremdnetz bis zu den Anschlusspunkten der Netzteilnehmer. Zu den aktiven Netzkomponenten, wie z. B. Router oder Switches, sowie für die elektrotechnische Verkabelung sind eigene goldene Regeln definiert und bei den entsprechenden Bausteinen zu finden.
- Bei der Dokumentation an den Kabeln ist darauf zu achten, dass diese für Befugte nachvollziehbar, aber ansonsten neutral ist, damit keine Rückschlüsse auf Art der übertragenen Daten und die Wichtigkeit des IT-Kabels gezogen werden können.
- Bevor größere Veränderungen an der IT-Verkabelung oder eine Neuverkabelung von Räumen oder Gebäuden vorgenommen werden soll, muss eine Anforderungsanalyse durchgeführt werden. Diese bildet die Grundlage für die Auswahl geeigneter Kabeltypen die dem jeweiligen Einsatzzweck, wie z. B. Primär-, Sekundär- oder Tertiär-Verkabelung, gerecht werden. Die Kabel sind dabei nicht nur aus physikalisch-mechanischer, sondern auch aus kommunikationstechnischer Sicht auszuwählen.
- Die Installation der IT-Kabel sollte mit besonderer Sorgfalt und nur durch ausreichend geschultes Personal oder durch einen externen Fachbetrieb erfolgen.
- Für die Wartung, Fehlersuche, Instandsetzung und für eine erfolgreiche Überprüfung der Verkabelung ist eine nachvollziehbare und aktuelle Dokumentation und eine eindeutige Kennzeichnung aller zugehörigen Komponenten erforderlich. Die IT-Verkabelung ist daher genau zu dokumentieren und die einzelnen Kabel und Trassen beispielsweise auf Gebäudeplänen einzutragen. Bei einer Installation durch einen Drittanbieter ist bei der Abnahme der IT-Verkabelung auch zu überprüfen, ob die Dokumentation vollständig und nachvollziehbar ist.
- Leitungen und Verteiler sind gegen unbefugte Zugriffe zu sichern. Die Zahl der Stellen, an denen Kabel oder Verteiler zugänglich sind, sollte auf ein Mindestmaß reduziert werden.
- Bestehende Verbindungen sind regelmäßig zu überprüfen, ob diese noch mit den dokumentierten Netzteilnehmern verbunden sind und noch die Aufgabe erfüllen, für die sie installiert wurden. Auch sind die Kabel auf evtl. Beschädigungen etc. zu überprüfen (vgl. [6]).

S2

Planung und Konzeption
M 1.3 (A) Angepasste Aufteilung der Stromkreise
M 1.7 (A) Handfeuerlöscher
M 1.8 (A) Raumbelegung unter Berücksichtigung von Brandlasten
M 1.12 (A) Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Umsetzung
M 1.1 (A) Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
M 1.2 (A) Regelungen für Zutritt zu Verteilern
M 1.6 (A) Einhaltung von Brandschutzvorschriften
M 1.9 (A) Brandabschottung von Trassen
M 1.51 (A) Brandlastreduzierung
M 2.17 (A) Zutrittsregelung und -kontrolle
M 5.4 (A) Dokumentation und Kennzeichnung der Verkabelung

Betrieb
M 1.15 (A) Geschlossene Fenster und Türen
M 2.14 (A) Schlüsselverwaltung
M 2.391 (B) Frühzeitige Information des Brandschutzbeauftragten
M 2.394 (B) Prüfung elektrischer Anlagen

Aussonderung
M 5.1 (A) Entfernen oder Deaktivieren nicht benötigter Leitungen

Notfallvorsorge
M 6.17 (A) Alarmierungsplan und Brandschutzübungen

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbausteinen B2.1, B2.2 und B2.12.

B 2.2 Büroraum

S2

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

- Alle Büroräume sollten gegen unbefugten Zutritt ausreichend geschützt sein. Dafür muss festgelegt werden, wer zu welchen Räumen unter welchen Bedingungen Zutritt erhält.
- Fenster und Türen sind zu verschließen, wenn ein Raum nicht besetzt ist.
- Büroräume müssen so ausgestattet sein, dass schutzbedürftige Datenträger und Dokumente weggeschlossen werden können. Dazu müssen beispielsweise verschließbare Schreibtische, Rollcontainer oder Schränke vorhanden sein.
- In Büros mit Publikumsverkehr sollten Diebstahlsicherungen zum Schutz von IT-Systemen (z. B. Laptops) vorgesehen werden, da andernfalls die Gefahr relativ groß ist, dass solche Geräte in einem unbewachten Augenblick „verschwinden".
- Arbeitsplätze sollten unter ergonomischen Gesichtspunkten eingerichtet werden. Das Arbeitsumfeld sollte gegen Störungen durch Lärm oder Staub so gut wie möglich abgeschirmt sein.
- Alle Mitarbeiter müssen darauf hingewiesen werden, dass auch in Büroräumen die vorhandenen IT-Geräte, Zubehör, Software oder Daten ausreichend gegen Diebstahl, Zerstörung und Veränderungen geschützt werden müssen (vgl. [6]).

Umsetzung
M 2.17 (A) Zutrittsregelung und -kontrolle

Betrieb
M 1.15 (A) Geschlossene Fenster und Türen
M 1.23 (A) Abgeschlossene Türen
M 1.45 (A) Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B2.3.

B 2.3 Serverraum

S2

Server sollten in speziellen Serverräumen untergebracht werden, in dem auch weitere serverspezifische Unterlagen, Datenträger oder Hardware (wie z. B. Router, Switches oder Klimatechnik) vorhanden sein können. Ein Serverraum ist ein geschlossener Sicherheitsbereich. Er ist kein ständiger Arbeitsplatz und sollte lediglich für sporadische und kurzfristige Aufgaben betreten werden.

- Ein Serverraum muss Server und die anderen aufgestellten IT-Geräte angemessen physisch schützen. Er muss vor unbefugtem Zutritt geschützt sein, eine angemessene Stromversorgung und Klimatisierung bieten. Außerdem muss er ausreichenden Brandschutz und Schutz vor Wasser- und anderen Umweltschäden bieten.
- Der Zutritt zum Serverraum muss auf die Personen beschränkt werden, die direkten Zugriff auf Server und sonstige im Serverraum installierte IT-Geräte benötigen. Neben hochwertigen Zutrittskontrollmechanismen sollten Sicherheitstüren und -fenster eingebaut werden. Serverräume sollten grundsätzlich verschlossen werden, wenn sie nicht besetzt sind.
- Serverräume sollten so geplant bzw. ausgewählt werden, dass potentielle Gefährdungen durch Umgebungseinflüsse minimiert werden.
- Es ist für ausreichenden Brandschutz zu sorgen. Es muss ein absolutes Rauchverbot verhängt werden. In jedem Serverraum sollten Handfeuerlöscher, die für elektronische Geräte geeignet sind, und Not-Aus-Schalter griffbereit vorhanden sein.
- Es sollten nach Möglichkeit keine Versorgungsleitungen, z. B. für Wasser oder Gas, durch den Serverraum verlaufen.
- Auf eine ausreichende Klimatisierung des Serverraumes ist zu achten.
- Die im Serverraum verwendeten Stromkreise müssen so ausgelegt sein, dass sie den tatsächlichen Bedürfnissen der vorhandenen Technik genügen.
- Damit es durch Spannungsspitzen im Stromnetz nicht zur Schädigung der elektrischen Geräte im Serverraum kommt, müssen Maßnahmen zum Überspannungsschutz und gegen elektrostatische Aufladung getroffen werden.
- Es sollte eine (oder mehrere) unterbrechungsfreie Stromversorgung im Serverraum vorhanden sein, um einen kurzzeitigen Stromausfall zu überbrücken. Die Stromversorgung sollte zumindest solange aufrechterhalten bleiben, dass ein geordnetes Herunterfahren der angeschlossenen Systeme möglich ist (vgl. [6]).

Planung und Konzeption
M 1.3 (A) Angepasste Aufteilung der Stromkreise
M 1.7 (A) Handfeuerlöscher
M 1.24 (C) Vermeidung von wasserführenden Leitungen
M 1.27 (B) Klimatisierung
M 1.28 (B) Lokale unterbrechungsfreie Stromversorgung
M 1.58 (A) Technische und organisatorische Vorgaben für Serverräume

Umsetzung
M 2.17 (A) Zutrittsregelung und -kontrolle
M 2.21 (A) Rauchverbot

Betrieb
M 1.15 (A) Geschlossene Fenster und Türen
M 1.23 (A) Abgeschlossene Türen

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B2.4. Bei entsprechendem erhöhtem Schutzbedarf kann zudem noch BSI IT-Grundschutzbaustein B2.9 (Rechenzentrum) zusätzlich verwendet werden.

B 2.4 Raum Technik

S2

In Räumen für technische Infrastruktur werden Geräte und Einrichtungen untergebracht, die selten oder nie direkt von Menschen bedient werden müssen. Im Allgemeinen finden sich hier Verteiler für die internen Versorgungsnetze, Sicherungen der Elektroversorgung oder auch Netzkoppel-Elemente. Es können hier auch Netzserver untergebracht werden, wenn kein separater Serverraum vorhanden ist.

- Ein Raum für technische Infrastruktur muss eine hinreichende physische Sicherheit bieten. Er muss vor unbefugtem Zutritt geschützt sein, eine angemessene Stromversorgung und Klimatisierung bieten. Außerdem muss er ausreichenden Brandschutz und Schutz vor Wasser und anderen Umweltschäden bieten.
- Der Zutritt zu Räumen für technische Infrastruktur muss auf die Personen beschränkt werden, die mit den entsprechenden technischen Wartungsaufgaben betraut sind.
- Räume für technische Infrastruktur sollten grundsätzlich immer verschlossen sein, wenn die dort aufgestellten Geräte nicht so in Schränken verschlossen sind, dass keine unbefugte Nutzung möglich ist.
- Es ist für ausreichenden Brandschutz zu sorgen. Es muss ein absolutes Rauchverbot verhängt werden. Es sollten Handfeuerlöscher, die für elektronische Geräte geeignet sind, und Not-Aus-Schalter griffbereit vorhanden sein.
- Es sollten nach Möglichkeit keine Versorgungsleitungen, z. B. für Wasser oder Gas, durch Räume für technische Infrastruktur verlaufen.
- Die Stromkreise müssen so ausgelegt sein, dass sie den tatsächlichen Bedürfnissen der vorhandenen Technik genügen. Damit es durch Spannungsspitzen im Stromnetz nicht zur Schädigung der elektrischen Geräte kommt, müssen Maßnahmen zum Überspannungsschutz getroffen werden.
- Bei erhöhten Sicherheitsanforderungen sollten Infrastrukturräume darüber hinaus durch besonders gesicherte Türen und Fenster auch gegen gewaltsames Eindringen geschützt werden, da sie oft bevorzugte Angriffsziele darstellen (vgl. [6]).

Planung und Konzeption
M 1.3 (A) Angepasste Aufteilung der Stromkreise
M 1.7 (A) Handfeuerlöscher
M 1.24 (C) Vermeidung von wasserführenden Leitungen
M 1.27 (B) Klimatisierung

Umsetzung
M 2.17 (A) Zutrittsregelung und -kontrolle
M 2.21 (A) Rauchverbot

Betrieb
M 1.15 (A) Geschlossene Fenster und Türen
M 1.23 (A) Abgeschlossene Türen

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B2.6.

B 2.5 Häuslicher / Mobiler Arbeitsplatz

S2

Ein häuslicher Arbeitsplatz kann zum Beispiel von Telearbeitern, freien Mitarbeitern oder Selbständigen genutzt werden. Bei einem häuslichen Arbeitsplatz kann nicht die infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in einer Büroumgebung innerhalb der Räumlichkeiten einer Institution anzutreffen ist. Sobald dienstliche Aufgaben daher nicht in den Räumen des Unternehmens bzw. der Behörde, sondern in der häuslichen Umgebung wahrgenommen werden, sind Sicherheitsmaßnahmen zu ergreifen, die eine mit einem Büroraum vergleichbare Sicherheitssituation erreichen lassen.

- Ein häuslicher Arbeitsplatz sollte von der übrigen Wohnung durch eine Tür abgetrennt sein. Es ist sinnvoll, für einen häuslichen Arbeitsplatz ein getrenntes Arbeitszimmer einzurichten.
- Der häusliche Arbeitsplatz muss über eine geeignete Einrichtung verfügen. Dazu gehören neben ausreichend Platz geeignete Büromöbel, Beheizungs- und Belüftungsmöglichkeiten, eine ausreichende Beleuchtung sowie Strom- und Telefonanschlüsse.
- Vertrauliche Informationen (z. B. Notizen, alte Datensicherungen) müssen sicher entsorgt werden. Sie dürfen nicht einfach in den Hausmüll geworfen werden.
- Dienstliche Unterlagen und Datenträger müssen am häuslichen Arbeitsplatz so aufbewahrt werden, dass kein Unbefugter darauf zugreifen kann. Daher müssen ausreichende verschließbare Behältnisse (Schreibtisch, Rollcontainer, Schrank, etc.) vorhanden sein.
- Es ist zu regeln, welche Informationen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind.
- Fenster und Türen sind zu verschließen, wenn der häusliche Arbeitsplatz nicht besetzt ist (vgl. [6]).

B 2.5 Häuslicher / Mobiler Arbeitsplatz

S2

Dienstliche Aufgaben werden häufig nicht mehr nur in den Räumen der Institution selbst wahrgenommen, sondern an wechselnden Arbeitsplätzen und in unterschiedlichen Umgebungen. Die dabei verarbeitenden Informationen müssen angemessen geschützt werden, in Wort, Schrift und IT. Die Leistungsfähigkeit von mobilen IT-Systemen wie beispielsweise Laptops, Handys und PDAs wächst ständig und lässt es zu, große Mengen geschäftsrelevanter Informationen außerhalb der Räume der jeweiligen Institution zu bearbeiten. Dabei ist zu beachten, dass die infrastrukturelle Sicherheit nicht der einer Büroumgebung entspricht.

- Für die Verarbeitung von Informationen außerhalb der Institutionsgrenzen sind klare Regelungen zu treffen. Für alle Arbeiten unterwegs ist zu regeln, welche Informationen außerhalb des Unternehmens bzw. der Behörde transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind.
- Die Art und der Umfang der Mitnahme von Datenträgern und IT-Komponenten ist klar zu regeln. So muss festgelegt werden, welche mobilen Datenträger verwendet und welche Informationen darauf transportiert werden dürfen. Vor allem die Nutzung von mobilen Endgeräten muss klar geregelt sein.
- Die Nutzer von mobilen Endgeräten sind für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen zu sensibilisieren. Sie sollten über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten Geräte aufgeklärt werden.
- Bei der mobilen Arbeit ist sicherzustellen, dass Dritte beispielsweise durch Mithören im Zug oder Mitlesen auf einem Laptop-Bildschirm keine wichtigen Informationen erfahren. Sensible Informationen sollten daher außerhalb der geschützten Büroumgebung nicht bearbeitet werden.
- An mobilen Arbeitsplätzen sollten weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt bleiben. Sie sollten zumindest gegen einfache Wegnahme gesichert werden, also beispielsweise mit Diebstahlsicherungen versehen, in Schränke geschlossen oder andere, einfache Maßnahmen ergriffen werden.
- Es ist sicherzustellen, dass Datenträger auch beim mobilen Einsatz sicher entsorgt werden. Vor der Entsorgung ausgedienter oder defekter Datenträger und Dokumente ist genau zu überlegen, ob diese sensible Informationen enthalten. In diesem Fall müssen die Datenträger und Dokumente wieder mit zurück transportiert werden und auf institutseigenem Wege entsorgt bzw. vernichtet werden.
- Wenn eine Verarbeitung von Informationen auf fremden IT-Systemen, beispielsweise in einem Internet-Cafe oder bei einem Kunden, notwendig ist, ist sicherzustellen, dass keine vertraulichen Informationen verarbeitet werden. Vor allem ist darauf zu achten, dass gewährleistet ist, dass die Informationen sicher vernichtet werden und beispielsweise der Browser Cache nach dem Besuch des Firmenintranets gelöscht wird (vgl. [6]).

Planung und Konzeption
M 1.44 (A) Geeignete Einrichtung eines häuslichen Arbeitsplatzes
M 1.61 (A) Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
M 2.218 (C) Regelung der Mitnahme von Datenträgern und IT-Komponenten
M 2.309 (A) Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung

Umsetzung
M 2.112 (A) Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution

Betrieb
M 1.15 (A) Geschlossene Fenster und Türen
M 1.23 (A) Abgeschlossene Türen
M 4.251 (A) Arbeiten mit fremden IT-Systemen

Aussonderung
M 2.13 (A) Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

Anmerkung:
Dieser Baustein entspricht den gekürzten BSI IT-Grundschutzbausteinen B2.8 und B2.10.

B 2.6 Besprechungs- und Schulungsräume

S2

Besprechungs-, Veranstaltungs- und Schulungsräume werden von wechselnden Personen bzw. Personenkreisen (sowohl von eigenem Personal als auch durch Externe) genutzt. Dabei kann die Nutzungsdauer stark variieren. In diesen Räumen werden Informationen mit unterschiedlichem Schutzbedarf bearbeitet und ausgetauscht.

- Es müssen Sicherheitsregeln für die Nutzung der Besprechungs-, Veranstaltungs- und Schulungsräume erstellt, sowie technisch und organisatorisch umgesetzt werden. Dies umfasst Verhaltenshinweise genereller Art für die Benutzer, aber auch Vorgaben zur Benutzung sowohl fest installierter, als auch mitgebrachter IT-Geräte.
- Die in Besprechungs-, Veranstaltungs- und Schulungsräume besprochenen und ausgetauschten Informationen müssen entsprechend ihres Schutzbedarfs gegen unbefugte Kenntnisnahme geschützt werden. Beim Austausch und der Verarbeitung von elektronischen Informationen muss sichergestellt sein, dass diese nicht die internen IT-Systeme gefährden können
- Externe Teilnehmer von Besprechungen oder Schulungen sollten außerhalb der Besprechungs- und Schulungsräume nicht unbeaufsichtigt sicherheitsrelevante Bereiche der Institution betreten können.
- Die in Besprechungs-, Veranstaltungs- und Schulungsräumen vorhandene IT muss entsprechend den Erfordernissen konfiguriert und administriert werden. Dabei müssen auch Zuständigkeiten für Administration und Problembehandlung festgelegt werden.
- IT-Systeme, die dauerhaft in Besprechungs-, Veranstaltungs- und Schulungsräumen betrieben werden, müssen sicher konfiguriert sein, so dass sie vor Manipulationen und vor Schadsoftware geschützt sind. Hierfür sollten Standardkonfigurationen vordefiniert sein, damit sie schnell neu installiert werden können und ein Mindestniveau an Sicherheit gewährleistet ist.
- IT-Systeme in Besprechungs- und Schulungsräumen sollten restriktiv konfiguriert und gehärtet sein. Es sollten Sicherheitsprogramme installiert sein, wie z. B. Virenschutz-Programm, Personal Firewall und Integritätsprüfprogramm.
- Es dürfen weder durch eigene, noch durch fremde IT externe Verbindungen unter Umgehung der internen Sicherheitsmaßnahmen, z. B. der Firewall, geschaffen werden. Daher sind alle Benutzer auf die Gefahren hinzuweisen, die mit der Schaffung „wilder" Zugänge verbunden sind. Es muss auch klare Regelungen für Zugriffe auf LAN- und TK-Schnittstellen aus Besprechungs- und Schulungsräumen geben (vgl. [6]).

Planung und Konzeption
M 2.331 (A) Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
M 2.332 (B) Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen
M 5.124 (C) Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen

Umsetzung
M 2.204 (A) Verhinderung ungesicherter Netzzugänge
M 2.333 (A) Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen

Betrieb
M 1.15 (A) Geschlossene Fenster und Türen
M 2.16 (B) Beaufsichtigung oder Begleitung von Fremdpersonen

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B2.11.

S3: IT-Systeme und Netze

In dieser Schicht werden klassische IT-Systeme und Netzwerke als Bausteine zusammengefasst. Es handelt sich hier um die wichtigsten IT-Systeme und Netzwerke, die in mittelständischen Unternehmen zum Einsatz kommen. Es wurde an dieser Stelle bewusst eine zu tiefe Detaillierung vermieden, um diesen Schritt leichter umsetzen zu können.

B 3.1 Server

S3

Server müssen an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Server sollten daher grundsätzlich in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden. Dabei ist zu regeln, wer Zutritt zu den Räumen bzw. Zugriff auf die Server selbst erhält. Server sollten nicht als Arbeitsplatzrechner genutzt werden.

- Alle Server müssen an unterbrechungsfreie Stromversorgungen (USV) angeschlossen werden, damit Stromausfälle solange überbrückt werden können, bis entweder die (Ersatz-) Energieversorgung wieder sichergestellt ist oder die Server geordnet heruntergefahren sind.
- Zugriffsrechte auf Dateien, die auf Servern gespeichert sind, müssen restriktiv vergeben werden. Jeder Benutzer darf nur auf die Dateien Zugriffsrechte erhalten, die er für seine Aufgabenerfüllung benötigt.
- Das gesamte Netz einer Organisation sollte durch ein entsprechendes Sicherheitsgateway geschützt sein. Server, die Dienste nach außen hin anbieten, sollten in einer Demilitarisierten Zone (DMZ) aufgestellt werden. Server sollten möglichst nicht im selben IP-Subnetz wie die Clients platziert werden. Wenn Server zumindest durch einen Router von den Clients getrennt sind, bestehen wesentlich bessere Möglichkeiten zur Steuerung des Zugriffs und zur Erkennung von Anomalien im Netzverkehr, die auf mögliche Probleme hindeuten.
- Server können beispielsweise lokal über eine Konsole, über das Netz oder über ein zentrales netzbasiertes Tool administriert werden. Abhängig von der genutzten Zugriffsart müssen geeignete Sicherheitsvorkehrungen getroffen werden.
- Es ist zu entscheiden, welche Informationen durch die Server mindestens protokolliert werden sollen, wie lange die Protokolldaten aufbewahrt werden sollen und wer unter welchen Voraussetzungen die Protokolldaten einsehen darf.
- Nicht benötigte Netzdienste von Servern müssen deaktiviert oder deinstalliert werden (vgl. [6]).

B 3.1 Server

S3

Planung und Konzeption
M 1.28 (B) Lokale unterbrechungsfreie Stromversorgung
M 2.315 (A) Planung des Servereinsatzes
M 2.316 (A) Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
M 5.10 (A) Restriktive Rechtevergabe

Beschaffung
M 2.317 (C) Beschaffungskriterien für einen Server

Umsetzung
M 2.204 (A) Verhinderung ungesicherter Netzzugänge
M 2.318 (A) Sichere Installation eines Servers
M 4.7 (A) Änderung voreingestellter Passwörter
M 4.15 (A) Gesichertes Login
M 4.16 (A) Zugangsbeschränkungen für Accounts und / oder Terminals
M 4.17 (A) Sperren und Löschen nicht benötigter Accounts und Terminals
M 4.237 (A) Sichere Grundkonfiguration eines IT-Systems

Betrieb
M 2.22 (Z) Hinterlegen des Passwortes
M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
M 4.24 (A) Sicherstellung einer konsistenten Systemverwaltung
M 4.238 (A) Einsatz eines lokalen Paketfilters
M 4.239 (A) Sicherer Betrieb eines Servers
M 5.8 (B) Regelmäßiger Sicherheitscheck des Netzes
M 5.9 (B) Protokollierung am Server

Aussonderung
M 2.320 (A) Geregelte Außerbetriebnahme eines Servers

Notfallvorsorge
M 6.24 (A) Erstellen eines Notfall-Bootmediums
M 6.96 (A) Notfallvorsorge für einen Server

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.101.

B 3.2 Client

Als Client wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt. 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 aufgebaut 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. Unabhängig vom eingesetzten Betriebssystem sollten folgende Sicherheitsaspekte berücksichtig werden:

- Vor der Installation muss festgelegt werden, welche Komponenten des Betriebssystems und welche Anwendungsprogramme und Tools installiert werden sollen. Vor allem die Installation des Betriebssystems sollte möglichst erfolgen, ohne dass das System an das Netz angeschlossen ist (Offline-Installation).
- Für die Installation sollten nur Medien und Dateien benutzt werden, die aus einer sicheren Quelle stammen.
- Es sollte mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können. „Normales Arbeiten" in der Administrator-Umgebung muss vermieden werden.
- Falls eine größere Anzahl von Clients ähnlich installiert und konfiguriert werden sollen, so bietet es sich an, eine „generische" Installation vorzunehmen, die anschließend auf die einzelnen Clients übertragen wird und die nur noch minimale Änderungen vor der Inbetriebnahme erforderlich macht.
- Nach der Installation sollte überprüft werden, welche Programme und Netzdienste auf dem System installiert und aktiviert sind. Nicht benötigte Programme und Netzdienste sollten deaktiviert oder ganz deinstalliert werden.
- Es muss überprüft werden, ob die Berechtigungen für Systemverzeichnisse und -dateien den Vorgaben der Sicherheitsrichtlinie entsprechen.
- Es sollte geprüft werden, welche Benutzerkonten wirklich gebraucht werden. Nicht benötigte Benutzerkonten sollten entweder gelöscht oder zumindest deaktiviert werden, damit unter dem betreffenden Konto keine Anmeldung am System möglich ist.
- Server und Clients mit hohem Schutzbedarf sollten, zusätzlich zum Schutz durch die organisationsweiten Sicherheitsgateways oder Paketfilter, die das interne Netz segmentieren, mit einem lokalen Paketfilter abgesichert werden.
- Eine Bildschirmsperre sollte eingerichtet werden, die sich sowohl manuell vom Benutzer aktivieren lässt, als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch gestartet wird.
- Es sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden (vgl. [6]).

B 3.2 Client

S3

Planung und Konzeption
M 2.321 (A) Planung des Einsatzes von Client-Server-Netzen
M 2.322 (A) Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz

Umsetzung
M 4.237 (A) Sichere Grundkonfiguration eines IT-Systems

Betrieb
M 3.18 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
M 4.2 (A) Bildschirmsperre
M 4.3 (A) Einsatz von Viren-Schutzprogrammen
M 4.4 (C) Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
M 4.238 (A) Einsatz eines lokalen Paketfilters
M 4.241 (A) Sicherer Betrieb von Clients
M 5.45 (B) Sichere Nutzung von Browsern

Aussonderung
M 2.323 (A) Geregelte Außerbetriebnahme eines Clients

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

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.201.

B 3.3 Notebook

S3

Ein Laptop oder Notebook ist ein PC in einer transportfreundlichen, kompakten Bauform, der daher mobil genutzt werden kann. Ein Laptop ist ein vollwertiger Arbeitsplatz-Rechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden.

- Alle Betriebssystem- und Software-Komponenten müssen sorgfältig ausgewählt, sowie sicher installiert werden, um die Risiken zu minimieren. Es muss regelmäßig kontrolliert werden, dass die Konfiguration nicht verändert wurde und keine ungenehmigte Software installiert wurde. Die Änderung der voreingestellten Optionen durch den Benutzer sollte administrativ unterbunden werden.
- Die Software des Laptops und die Datenbestände müssen auf dem aktuellen Stand gehalten und notwendige Sicherheitspatches zeitnah eingespielt werden. Nach einem externen Einsatz muss ein Laptop zunächst gründlich auf Viren und andere Schadsoftware überprüft werden, bevor er wieder ans LAN angeschlossen werden darf. Im mobilen Einsatz, aber auch im Büro sollten grundsätzlich Diebstahl-Sicherungen verwendet werden. Im Umgang mit externen Speichermedien wie USB-Sticks sollten die Benutzer Vorsicht walten lassen, durch unbedachte Weitergabe können vertrauliche Daten offen gelegt oder Schadprogramme aufgelesen werden.
- Alle Daten, die auf mobilen IT-Systemen lokal gespeichert werden, müssen regelmäßig gesichert werden. Hierfür müssen geeignete Verfahren zur Datensicherung in Abhängigkeit vom Volumen des Datenbestands ausgewählt werden. Die Datensicherung sollte möglichst weitgehend automatisiert werden, so dass die Benutzer möglichst wenig Aktionen selbst durchführen müssen.
- Bei Laptops besteht ein relativ hohes Verlust- und Diebstahlsrisiko. Damit die Daten nicht in falsche Hände fallen, müssen die Dateien oder besser die gesamte Festplatte und alle mobilen Datenträger verschlüsselt sein.
- Zugriffe von einem Laptop von außerhalb auf das interne Netz sollten ausschließlich verschlüsselt erfolgen (über VPN gesichert). E-Mails sollten ausschließlich verschlüsselt von Mail-Servern auf den Laptop übertragen werden (z. B. mittels SSL).
- 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.
- Es ist unabdingbar, dass sich jeder Laptop nur nach einer erfolgreichen Authentisierung starten lässt. Das Gleiche gilt für den Zugriff auf das interne LAN.
- Sowohl bei der Authentisierung als auch bei Verschlüsselung von Datenträger und Kommunikation müssen starke Passwörter gewählt werden, die nicht zu erraten sind. Diese sollte aus einer Kombination von Zahlen, Buchstaben und Sonderzeichen bestehen und mindestens 8 Zeichen lang sein. Die Passwörter dürfen auf keinen Fall zusammen mit dem Laptop aufbewahrt werden.
- 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 (vgl. [6]).

B 3.3 Notebook

S3

Planung und Konzeption
M 2.36 (B) Geregelte Übergabe und Rücknahme eines tragbaren PCs
M 2.309 (A) Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung

Umsetzung
M 5.91 (A) Einsatz von Personal Firewalls für Internet-PCs
M 5.121 (B) Sichere Kommunikation von unterwegs
M 5.122 (A) Sicherer Anschluss von Laptops an lokale Netze

Betrieb
M 1.33 (A) Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
M 4.3 (A) Einsatz von Viren-Schutzprogrammen
M 4.27 (A) Zugriffsschutz am Laptop

Aussonderung
M 2.306 (A) Verlustmeldung

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

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.203.

B 3.4 Security Gateway (Firewall)

Mit Sicherheitsgateways können unterschiedliche Netze gekoppelt werden. Am häufigsten werden sie am Übergang zwischen Internet und internem Netz eingesetzt, aber sie können auch unterschiedlich vertrauenswürdige Netzbereiche des internen Netzes miteinander verbinden. Ein Sicherheitsgateway besteht in der Regel aus mehreren Hard- und Softwarekomponenten, die den Kommunikationsfluss zwischen den angeschlossenen Netzen nach den Vorgaben einer Sicherheitsrichtline durchsetzen. Aus diesen Vorgaben werden konkrete Regeln erstellt, mit denen der Netzwerkverkehr gesteuert und so unerlaubter Datentransfer unterbunden wird.

- Interne Netze müssen beim Anschluss an externe Netze (z. B. das Internet) durch ein Sicherheitsgateway geschützt werden.
- Es muss sichergestellt sein, dass es keinen unbefugten, von außen initiierten Verbindungsaufbau in das geschützte Netz geben kann.
- Sicherheitsgateways sollten aus mehreren Komponenten mit einer PAP Struktur (Paketfilter Applikation Level Gateway) bestehen.
- Für das Sicherheitsgateway müssen eindeutige Regeln definiert sein, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen müssen durch das Sicherheitsgateway unterbunden werden (Whitelist-Ansatz).
- Dient das Sicherheitsgateway zur Ankopplung eines internen Netzes an das Internet, sollten alle Dienste, die aus dem Internet erreichbar sein sollen (z. B. E-Mail, Webauftritt) an das Sicherheitsgateway angeschlossen sein. Die entsprechenden Server sollten in einer DMZ (Demilitarisierten Zone) des Sicherheitsgateways platziert werden.
- Alle Verbindungen zwischen den gekoppelten Netzen sollten im Sicherheitsgateway terminiert und von dort zum gewünschten Verbindungspartner neu aufgebaut werden (Proxy-Funktionalität).
- Zur Überwachung des Betriebs und zur Analyse von Angriffen bzw. Fehlern sollten Protokolle von allen, dem Sicherheitsgateway zugehörigen Komponenten erstellt werden (also insbesondere Paketfilter und Application Level Gateway). Hierbei sind die rechtlichen Rahmenbestimmungen unbedingt einzuhalten.
- Das Sicherheitsgateway sollte für Unbefugte unzugänglich aufgestellt sein, beispielsweise in einem Serverraum oder in einem Serverschrank (vgl. [6]).

B 3.4 Security Gateway (Firewall)

S3

Planung und Konzeption
M 2.70 (A) Entwicklung eines Konzepts für Sicherheitsgateways
M 2.71 (A) Festlegung einer Policy für ein Sicherheitsgateway
M 2.299 (A) Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway
M 2.476 (A) Konzeption für die sichere Internet-Anbindung

Beschaffung
M 2.74 (A) Geeignete Auswahl eines Paketfilters
M 2.75 (A) Geeignete Auswahl eines Application-Level-Gateways

Umsetzung
M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln
M 2.77 (A) Integration von Servern in das Sicherheitsgateway

Betrieb
M 2.78 (A) Sicherer Betrieb eines Sicherheitsgateways
M 4.47 (A) Protokollierung der Sicherheitsgateway-Aktivitäten
M 5.39 (A) Sicherer Einsatz der Protokolle und Dienste
M 5.59 (A) Schutz vor DNS-Spoofing bei Authentisierungsmechanismen
M 5.70 (A) Adressumsetzung - NAT (Network Address Translation)

Aussonderung
M 2.300 (C) Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways

Notfallvorsorge
M 6.94 (C) Notfallvorsorge bei Sicherheitsgateways

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.301

B 3.5 Router / Switch

S3

Für eine Kommunikation in Netzen werden neben einer Verkabelung auch Netzkoppelelemente, wie Router und Switches, benötigt. Ein Ausfall einer oder mehrerer dieser Komponenten der Netztechnik kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Daher müssen Router und Switches vor unerlaubten Zugriffen und Manipulationen geschützt werden.

- Vor der Beschaffung der Netzkomponenten (Router und Switches) muss eine Sicherheitsstrategie für den sicheren Betrieb der Geräte festgelegt und dokumentiert werden.
- Um Unbefugten den Zugriff auf Router und Switches zu erschweren, sollten diese Geräte so aufgestellt werden, dass nur Berechtigte Zugriff haben.
- Das eingesetzte Betriebssystem auf Routern und Switches sollte stabil und immer auf dem aktuellen Stand gehalten werden, indem Patches und Updates systematisch und zeitnah eingespielt werden (nach Test und vorheriger Datensicherung).
- Nicht benötigte Dienste auf Routern und Switches könnten zur Durchführung von Angriffen oder zur Informationsgewinnung missbraucht werden. Entsprechend dem Minimalprinzip sollten daher unnötige Dienste auf Routern und Switches abgeschaltet werden.
- Router und Switches können lokal über eine Konsole oder entfernt über eine Netzverbindung administriert werden. Abhängig von der Zugriffsart müssen geeignete Sicherheitsvorkehrungen getroffen werden. Bei der Remote-Administration von Routern und Switches muss in jedem Fall eine Absicherung der Kommunikation erfolgen. Dies kann beispielsweise durch die Nutzung des Dienstes SSH anstatt Telnet oder durch die Schaffung eigener LAN-Segmente, die ausschließlich für Administrationszwecke genutzt werden, erreicht werden.
- Voreingestellte Passwörter auf Routern und Switches müssen nach der Installation geändert werden. Darüber hinaus sollten die Geräte so konfiguriert werden, dass die Passwörter nicht im Klartext, sondern verschlüsselt in der Konfigurationsdatei gespeichert werden.
- Die Zugriffsrechte für die Nutzung und die Administration von Routern und Switches sollten möglichst restriktiv vergeben werden und mit Hilfe von Access Control Lists (ACLs) kontrolliert werden.
- Die Protokollierung sollte immer genutzt und sorgfältig eingerichtet werden. Darüber hinaus müssen die protokollierten Daten zur Beurteilung der korrekten Funktion des Geräts und zur Erkennung von Angriffen oder Angriffsversuchen zeitnah ausgewertet werden.
- Ein regelmäßiges Backup der Router-Konfigurationen sollte durchgeführt werden und Sicherungskopien der laufenden Konfiguration müssen so angelegt werden, dass auch bei einem Ausfall des Management-Systems ein Zugriff jederzeit möglich ist (vgl. [6]).

B 3.5 Router / Switch

S3

Planung und Konzeption
M 2.279 (A) Erstellung einer Sicherheitsrichtlinie für Router und Switches

Beschaffung
M 2.280 (C) Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches

Umsetzung
M 1.43 (A) Gesicherte Aufstellung aktiver Netzkomponenten
M 4.201 (A) Sichere lokale Grundkonfiguration von Routern und Switches
M 4.202 (A) Sichere Netz-Grundkonfiguration von Routern und Switches
M 4.203 (A) Konfigurations-Checkliste für Router und Switches

Betrieb
M 2.281 (A) Dokumentation der Systemkonfiguration von Routern und Switches
M 2.282 (A) Regelmäßige Kontrolle von Routern und Switches
M 2.283 (B) Software-Pflege auf Routern und Switches
M 4.206 (C) Sicherung von Switch-Ports

Aussonderung
M 2.284 (C) Sichere Außerbetriebnahme von Routern und Switches

Notfallvorsorge
M 6.91 (C) Datensicherung und Recovery bei Routern und Switches

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.302.

B 3.6 Speichersysteme(SAN, NAS)

S3

Über ein Speichernetz können gleichzeitig mehrere Server oder gegebenenfalls auch direkt Endgeräte diesen Speicher nutzen. Speichersysteme, die aus mehreren vernetzten Einheiten bestehen, nutzen üblicherweise ein dediziertes Netzwerk von Speichern und werden daher auch als „Speichernetze" bezeichnet. Ein Speichersystem gilt als die zentrale Instanz, die für andere Systeme Speicherplatz zur Verfügung stellt.

- Speichersysteme und Speichernetze erfordern spezielle Kenntnisse der Administratoren. Diese müssen daher immer ausreichend zu diesem Thema und deren Sicherheitsaspekten geschult sein.
- Die grundsätzliche Entscheidung, welche Art von Speichersystem angemessen für die Institution ist, muss durch eine Anforderungsanalyse festgestellt werden. Maßgebliche Kenngrößen sind die Anforderungen an die Verfügbarkeit, Performance und Kapazität. Wenn die Kapazität eines Speichersystems oder Speichernetzes ausgereizt ist, muss in der Regel erneut geplant und investiert werden. Es ist daher wichtig, die Speichersysteme in Bezug auf die Kapazitätsanforderungen regelmäßig zu überprüfen, um die Größe rechtzeitig anpassen zu können.
- Bevor ein Speichersystem in den Produktivbetrieb integriert wird, muss es sicher konfiguriert werden. Viele Geräte werden vom Hersteller mit einer Default-Konfiguration ausgeliefert, in der so gut wie keine Sicherheitsmechanismen aktiv sind. Daher muss die Überprüfung der Default-Einstellungen und die Grundkonfiguration offline erfolgen, in einem eigens dafür eingerichteten und besonders gesicherten Testnetz oder über das Administrationsnetz. Die Dokumentation der Konfiguration muss aktuell und vollständig sein, um bei Notfällen schnell reagieren zu können und Fehler bei Änderungen im System zu vermeiden.
- Änderungen und Aktualisierungen an Speichersystemen und Speichernetzen müssen gut geplant und vor dem Einsatz im Produktivbetrieb ausführlich getestet werden.
- Bei Speichersystemen und Speichernetzen mit hohen Verfügbarkeitsanforderungen sollten Single Points of failure, d. h. Komponenten, die bei einem Ausfall den Komplettausfall des Systems mit sich ziehen können, durch ausreichender Redundanzen vermieden werden.
- Soll ein Speichersystem außer Betrieb genommen werden, muss ein Vorgehen zur Migration der Daten entworfen werden. Es muss sichergestellt sein, dass alle Daten auf dem Speichersystem so auf andere Speichersysteme überführt werden, dass alle Anforderungen, die sich aus der Tätigkeit der Institution ergeben, aber auch gesetzliche Anforderungen zu Aufbewahrungsfristen und dergleichen, erfüllt werden (vgl, [6]).

B 3.6 Speichersysteme(SAN, NAS)

S3

Planung und Konzeption
M 2.351 (A) Planung von Speichersystemen
M 2.352 (A) Erstellung einer Sicherheitsrichtlinie für NAS-Systeme
M 2.353 (A) Erstellung einer Sicherheitsrichtlinie für SAN-Systeme
M 2.362 (A) Auswahl eines geeigneten Speichersystems

Umsetzung
M 1.59 (A) Geeignete Aufstellung von Speicher- und Archivsystemen
M 2.357 (B) Aufbau eines Administrationsnetzes für Speichersysteme
M 2.358 (A) Dokumentation der Systemeinstellungen von Speichersystemen
M 3.54 (A) Schulung der Administratoren des Speichersystems
M 4.80 (B) Sichere Zugriffsmechanismen bei Fernadministration
M 4.274 (A) Sichere Grundkonfiguration von Speichersystemen

Betrieb
M 2.359 (B) Überwachung und Verwaltung von Speichersystemen
M 2.360 (B) Sicherheits-Audits und Berichtswesen bei Speichersystemen
M 4.275 (A) Sicherer Betrieb eines Speichersystems

Aussonderung
M 2.361 (C) Deinstallation von Speichersystemen

Notfallvorsorge
M 6.1 (A) Erstellung einer Übersicht über Verfügbarkeitsanforderungen
M 6.98 (A) Notfallvorsorge für Speichersysteme

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.303.

B 3.7 Virtualisierung

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Je nach Produkt können mehrere Virtualisierungsserver zu einer virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden. Betrachtet werden dabei die Sicherheitsaspekte der Virtualisierung.

- Aufgrund der hohen Komplexität ist eine detaillierte Planung beim Aufbau einer virtuellen Infrastruktur unerlässlich. Daher sollte schon bei einer konzeptionellen Betrachtung und im Vorfeld einer Projektierung eine genaue Analyse der notwendigen Rahmenbedingungen durchgeführt werden.
- Es ist zu prüfen, ob alle Anwendungen, die auf virtuellen IT-Systemen betrieben werden sollen, durch ihre Hersteller auf der gewählten Virtualisierungsplattform unterstützt werden.
- Bei der Entscheidung, welche virtuellen IT-Systeme gemeinsam auf einem Virtualisierungsserver ausgeführt werden dürfen, muss der Schutzbedarf der einzelnen virtuellen IT-Systeme berücksichtigt werden.
- Die einzusetzende Virtualisierungssoftware muss eine ausreichende Isolation und Kapselung der virtuellen IT-Systeme gewährleisten. Dies bedeutet insbesondere, dass die einzelnen virtuellen IT-Systeme nur über festgelegte Wege miteinander kommunizieren und nur über definierte Kanäle auf die Hard-/Software des Virtualisierungsservers zugreifen können.
- Auf den eigentlichen Virtualisierungsservern, das heißt außerhalb der virtuellen IT-Systeme, sollten möglichst nur solche Dienste betrieben werden, die zur Virtualisierungstechnik gehören.
- Bei der Auswahl der Hardware für Virtualisierungsserver ist darauf zu achten, dass Systeme beschafft werden, die für die gewählte Virtualisierungslösung geeignet sind. Jeder Virtualisierungsserver muss so leistungsfähig sein, dass für alle virtuellen IT-Systeme, die auf diesem Virtualisierungsserver ablaufen sollen, genügend Leistung bereitsteht.
- Die Verwaltungsschnittstellen der Virtualisierungsserver sollten in einem eigenen Netz angeschlossen werden. Dieses ist physisch oder logisch von dem Netz zu trennen, in dem die virtuellen IT-Systeme betrieben werden.
- Beim Einsatz von Virtualisierung kann es Probleme mit der Systemzeit geben. Es muss sichergestellt werden, dass die Systemzeit in den virtuellen IT-Systemen stets korrekt ist.
- Viele Hersteller stellen für die virtuellen IT-Systeme so genannte Gastwerkzeuge zur Verfügung, mit denen die virtuellen IT-Systeme auf einfache Weise durch die Virtualisierungssoftware gesteuert werden können. Es sind verbindliche Regelungen zur Konfiguration und zum Einsatz dieser Gastwerkzeuge in virtuellen IT-Systemen zu erstellen (vgl, [6]).

B 3.7 Virtualisierung

S3

Planung und Konzeption
M 2.392 (A) Modellierung von Virtualisierungsservern und virtuellen IT-Systemen
M 2.444 (A) Einsatzplanung für virtuelle IT-Systeme
M 2.477 (A) Planung einer virtuellen Infrastruktur
M 3.71 (B) Schulung der Administratoren virtueller Umgebungen

Beschaffung
M 2.445 (A) Auswahl geeigneter Hardware für Virtualisierungsumgebungen

Umsetzung
M 2.83 (B) Testen von Standardsoftware
M 2.447 (A) Sicherer Einsatz virtueller IT-Systeme
M 4.346 (A) Sichere Konfiguration virtueller IT-Systeme
M 5.154 (B) Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen

Betrieb
M 4.349 (A) Sicherer Betrieb von virtuellen Infrastrukturen

Notfallvorsorge
M 6.138 (C) Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.304.

B 3.8 Terminalserver

Terminalserver stellen ein besonders zentralisiertes Szenario einer Client-Server Architektur dar. Anwendungen werden auf den leistungsstarken Terminalservern installiert, von den Clients werden diese gestartet, gesteuert und dargestellt. Diese Ein- und Ausgaben können auf verhältnismäßig einfach ausgestatteten Arbeitsplatz-Rechnern (Fat-Clients) mit der entsprechenden Client-Software verarbeitet werden. Zudem existieren Lösungen, die mit dedizierten Terminals (Thin-Clients) funktionieren. Betrachtet werden Sicherheitsaspekte zu Terminalservern.

- Beim Einsatz von Terminalservern sind von der Institution geeignete Sicherheitsrichtlinien aufzustellen. Die hierin schriftlich festgehaltenen Maßgaben sowie Zielsetzungen müssen die individuellen Bedingungen und Anforderungen einer sicheren Terminalserver-Umgebung widerspiegeln.
- Bei der Migration einer klassischen Client-Server-Architektur auf eine Terminalserver-gestützte Umgebung muss vor der Umsetzung eingehend überprüft werden, ob die zu migrierenden Anwendungen überhaupt dafür geeignet sind.
- Die Verwaltung der Terminalserver-Infrastruktur ist für Administratoren komplex, die Benutzung ist ohne Vorerfahrung in einigen Punkten erklärungsbedürftig. Alle Personen, die mit Terminalservern arbeiten, sollten daher ausreichend in den sie betreffenden Aspekten geschult werden.
- Innerhalb von Mehrbenutzerumgebungen, wie sie Terminalserver-Systeme darstellen, ist die Abschottung der Anwender voneinander sowie gegenüber riskanten Systemfunktionen von erheblicher Bedeutung. Um einen störungsfreien Betrieb zu gewährleisten und die verarbeiteten Daten zu schützen, müssen die Zugangs- und Zugriffsrechte restriktiv vergeben werden.
- Um die Verfügbarkeit von Terminalservern gewährleisten zu können, müssen die Systemressourcen, wie Prozessorleistung, Datendurchsatz zu Speichersystemen und deren Größe, ausreichend dimensioniert werden.
- Es muss verhindert werden, dass die Anwender sicherheitsrelevante Änderungen an der Benutzerumgebung auf den Terminalservern vornehmen können. Es ist sicherzustellen, dass die Anwender nur auf die Ressourcen zugreifen können, die sie für ihre Arbeit tatsächlich benötigen.
- Die Verbindungen zwischen den Terminalservern und deren Clients sollten verschlüsselt werden, wenn diese Kommunikation über ein unsicheres Netz läuft.
- Der Ausfall einer Terminalserver-Umgebung betrifft meist mehrere Anwender. Abhängig von den Verfügbarkeitsanforderungen sollten daher Redundanzmaßnahmen für die Terminalserver ergriffen werden, damit bei einem Ausfall der Schaden in Grenzen gehalten wird.
- Bei allen Komponenten der Terminalserver-Infrastruktur muss regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und wirksam sind (vgl. [6]).

B 3.8 Terminalserver

S3

Planung und Konzeption
M 2.464 (A) Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung
M 2.465 (A) Analyse der erforderlichen Systemressourcen von Terminalservern
M 2.466 (A) Migration auf eine Terminalserver-Architektur
M 5.162 (A) Planung der Leitungskapazitäten beim Einsatz von Terminalservern
M 5.163 (A) Restriktive Rechtevergabe auf Terminalservern

Beschaffung
M 2.468 (B) Lizenzierung von Software in Terminalserver-Umgebungen

Umsetzung
M 4.106 (A) Aktivieren der Systemprotokollierung
M 5.72 (A) Deaktivieren nicht benötigter Netzdienste

Betrieb
M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
M 4.3 (A) Einsatz von Viren-Schutzprogrammen
M 5.164 (B) Sichere Nutzung eines Terminalservers aus einem entfernten Netz

Aussonderung
M 2.469 (A) Geregelte Außerbetriebnahme von Komponenten einer Terminalserver-Umgebung

Notfallvorsorge
M 6.143 (C) Bereitstellung von Terminalserver-Clients aus Depot-Wartung

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.305.

B 3.9 TK-Anlage

S3

Mit einer TK-Anlage können die Telefone einer Institution intern verbunden und extern an ein öffentliches Telefonnetz angeschlossen werden. Neben der Sprachtelefonie können, abhängig von den angeschlossenen Endgeräten, weitere Dienste genutzt werden. So ist es möglich, Daten, Texte, Grafiken und Bewegtbilder über TK-Anlagen zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien übermittelt werden. Betrachtet werden Sicherheitsaspekte von TK-Anlagen.

- Es muss entschieden werden, für welche unterschiedlichen Kommunikationsdienste die TK-Anlage genutzt werden soll. Entsprechend der Einsatzszenarien sind die Anforderungen an die zu beschaffenden Produkte zu formulieren und basierend darauf sind geeignete Produkte auszuwählen.
- Die Benutzer sind im richtigen Umgang mit den jeweiligen Diensten zu schulen. Auf die mit einer TK-Anlage verbundenen Gefährdungen und auf Sicherheitsrisiken durch bestimmte Dienste, wie Konferenzschaltungen und Rufumleitungen, sind die Benutzer hinzuweisen.
- Voreingestellte (Standard-)Passwörter sind direkt nach der Installation, spätestens bei erstmaliger Inbetriebnahme der Komponenten der TK-Anlage zu ändern. Für alle zentralen Komponenten ist eine angemessene Zugangskontrolle zu realisieren.
- Die Schnittstellen einer TK-Anlage, über die Administrationstätigkeiten ausgeführt werden können, müssen vor unautorisiertem Zugriff geschützt werden.
- Bei der Speicherung von personenbezogenen Daten muss auf eine geeignete Absicherung geachtet werden. Dies beinhaltet die Kontrolle (und Einschränkung) des Zugangs zu diesen Daten sowie die Verschlüsselung dieser Daten beim Transport über das Datennetz und auf den jeweiligen Datenträgern.
- Sollen Komponenten der TK-Anlage außer Betrieb genommen oder ersetzt werden, so müssen die sicherheitsrelevanten Informationen, die auf diesen Komponenten gespeichert sind, sicher gelöscht werden.
- Es muss festgelegt werden, wer welche Kommunikationsdienste nutzen darf, welche Regelungen dabei zu beachten und wie interne IT-Systeme zu schützen sind (vgl. [6]).

Planung und Konzeption
M 2.471 (A) Planung des Einsatzes von TK-Anlagen
M 2.472 (A) Erstellung einer Sicherheitsrichtlinie für TK-Anlagen

Beschaffung
M 2.105 (A) Beschaffung von TK-Anlagen

Umsetzung
M 4.7 (A) Änderung voreingestellter Passwörter
M 4.11 (B) Absicherung der TK-Anlagen-Schnittstellen
M 5.15 (A) Absicherung externer Remote-Zugänge von TK-Anlagen

Betrieb
M 4.5 (B) Protokollierung bei TK-Anlagen

Aussonderung
M 2.474 (B) Sichere Außerbetriebnahme von TK-Komponenten

Notfallvorsorge
M 6.26 (B) Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.401.

B 3.10 Mobiltelefon / Smartphone

S3

Mobiltelefone sind inzwischen alltäglicher Bestandteil der Kommunikationsinfrastruktur geworden. Neben herkömmlichen Telefongesprächen bieten die Geräte meist noch eine Vielzahl an zusätzlichen Funktionen, wie das Verschicken von SMS, MMS, E-Mail, die Nutzung von WLAN oder eine Termin und Adressverwaltung. Aktuelle Mobiltelefone nutzen nicht nur die Mobilkommunikationsnetze, sondern verfügen auch über weitere Kommunikationsschnittstellen wie Bluetooth oder Infrarot.

- Für die sichere Nutzung von Mobiltelefonen in einer Institution muss zunächst geregelt werden, unter welchen Ramenbedingungen diese eingesetzt werden dürfen und welche Sicherheitsanforderungen dabei zu beachten sind. Dabei ist auch festzulegen, welche Regelungen für private oder von Besuchern mitgebrachte Mobiltelefone gelten, also beispielsweise, ob diese in Räumen der Institution genutzt werden dürfen.
- Mitarbeiter müssen über die Regelungen zur Nutzung von Mobiltelefonen aufgeklärt werden und für potentielle Gefährdungen sensibilisiert werden.
- Zum Schutz vor Missbrauch und Diebstahl sollten Mobiltelefone nicht an unsicheren Orten unbeaufsichtigt zurückgelassen werden. Verlorene oder gestohlene Geräte müssen sofort gesperrt werden.
- Es muss sichergestellt werden, dass die Sicherheitsmechanismen von Mobiltelefonen genutzt werden. Dazu gehört die Eingabe einer PIN oder eines Passworts sowohl beim Einschalten des Geräts als auch nach längerer Abwesenheit oder beim Wechsel der SIM-Karte. PINs und Passwörter dürfen nicht zu einfach gewählt werden.
- Das Mobiltelefon sollte so konfiguriert werden, dass vor der Verbindung ins Internet und vor dem Herunterladen von MMS eine explizite Bestätigung des Nutzers eingefordert wird. So wird sichergestellt, dass der Verbindungsaufbau gewollt initiiert wurde. Generell sollte die Vertrauenswürdigkeit des Absenders, Anrufers oder Internetquelle bzw. die Plausibilität des Inhalts geprüft werden, um der Verbreitung von Schadsoftware vorzubeugen.
- Kommunikationsschnittstellen wie USB, Bluetooth oder Infrarot sollten nur bei Bedarf aktiviert und die übertragenen Daten (z. B. Datensicherung oder Synchronisation von Datenbeständen) nach Möglichkeit verschlüsselt werden.
- Es muss geregelt werden, wie Daten und Programme sicher gespeichert werden. Vertrauliche Daten, wie personenbezogene Daten oder Zugangsdaten zum Netz der Institution, sollten gar nicht oder nur verschlüsselt auf den Geräten oder zusätzlichen Speicherkarten abgelegt werden. Sensible Informationen sollten nicht über das Mobiltelefon weitergegeben werden.
- Bei der Weitergabe oder Entsorgung der Geräte müssen sämtliche sensiblen Daten aus allen Speicherbereichen des Mobiltelefons entfernt werden (vgl. [6]).

S3

Ein Personal Digital Assistant (PDA) bietet die Möglichkeit persönliche Informationen wie beispielsweise Kontakte, Termine und Nachrichten unterwegs nutzbar zu machen. Je nach PDA können auch verschiedene Dateiformate angezeigt und bearbeitet werden.

- Für den Einsatz von PDAs in einer Institution sind im Vorfeld eine Vielzahl von Regelungen zu treffen. Hierbei ist zu entscheiden, welche Daten auf den PDAs gespeichert und verarbeitet werden dürfen, wie mit privaten Daten auf den PDAs umzugehen ist, welchen Kriterien die PDAs an Betriebssystemen, Schnittstellen, zentrale Administration, Sicherheit usw. entsprechen müssen und welche eingebauten und zusätzlichen Sicherheitsmechanismen des PDAs verwendet werden sollen.
- Es ist zu regeln, unter welchen Rahmenbedingungen PDAs extern genutzt werden dürfen und wie sie unterwegs zu schützen sind. Weiterhin ist zu definieren, welche Schritte beim Verlust eines PDAs durchzuführen sind.
- Wenn sich vertrauliche Daten auf den PDAs befinden, müssen diese durch geeignete Maßnahmen zur Authentisierung und Verschlüsselung vor unbefugtem Zugriff geschützt werden.
- Bei Online-Nutzung von PDAs muss eine sichere Kommunikation mit dem Netz der Institution gewährleistet werden. Hierbei sind Verfahren zu definieren, wie Verbindungen über die unterschiedlichen Schnittstellen von PDAs beispielsweise über VPN-Techniken aufgebaut werden.
- Während des mobilen Einsatzes von PDAs ist eine ausreichende Energieversorgung sicherzustellen. Es ist vor allem darauf zu achten, dass die gespeicherten Daten auch nach dem vollständigen Entladen der Hauptbatterie weiterhin vorhanden sind. Zur Ausfallvorsorge ist eine regelmäßige Datensicherung durchzuführen. Sollte es zu einem Datenverlust kommen, so ist zu definieren, über welche Mechanismen die letzte Datensicherung wieder eingespielt werden kann. Hier ist auch zu definieren, ob und wie diese Wiederherstellung beim mobilen Einsatz vollzogen werden kann (vgl. [6]).

Planung und Konzeption
M 2.188 (A) Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

Umsetzung
M 4.114 (A) Nutzung der Sicherheitsmechanismen von Mobiltelefonen
M 5.121 (B) Sichere Kommunikation von unterwegs

Betrieb
M 2.189 (A) Sperrung des Mobiltelefons bei Verlust
M 5.81 (B) Sichere Datenübertragung über Mobiltelefone
M 1.33 (A) Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
M 4.3 (A) Einsatz von Viren-Schutzprogrammen
M 4.228 (A) Nutzung der Sicherheitsmechanismen von PDAs

Aussonderung
M 2.306 (A) Verlustmeldung

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbausteinen B3.404 und B3.405.

B 3.11 Drucker und Multifunktionsgeräte

S3

Zur Grundausstattung in Büroumgebungen gehören typischerweise Kopierer, sowie bei IT-Arbeitsplätzen Drucker. Arbeitsergebnisse müssen oft auf Papier ausgegeben, bearbeitet und archiviert werden. Häufig wird jedoch nicht jeder einzelne Arbeitsplatz mit einem Drucker ausgestattet. Zum Einsatz kommen dann zentrale Netzdrucker, Kopierer oder Multifunktionsgeräte, auf denen die Benutzer ihre Dokumente ausdrucken oder vervielfältigen können. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste.

- Es muss entschieden werden, ob lokale Drucker, eingesetzt werden sollen, die nur einzelnen IT-Systemen zur Verfügung stehen oder netzfähige Drucker, die von mehreren Benutzern genutzt werden können. Benutzer, die häufiger sensible Informationen ausdrucken müssen, sollten einen lokalen Drucker erhalten. Für die Ausdrucke der restlichen Benutzer oder für Ausdrucke von Informationen mit einem geringeren Schutzbedarf können zentrale Drucker zur Verfügung gestellt werden.
- Es müssen Richtlinien für die Administratoren und Benutzer von Druckern, Kopierern und Multifunktionsgeräten erstellt werden, da technische Maßnahmen alleine nicht den sicheren Einsatz bzw. die sichere Nutzung gewährleisten.
- Um Unbefugten den Zugriff auf Drucker, Kopierer und Multifunktionsgeräte zu erschweren, sollten diese Geräte so aufgestellt werden, dass nur Berechtigte Zutritt haben. Zumindest sollten Drucker nicht in Bereichen aufgestellt werden, in denen sich häufig Externe aufhalten, also nicht in der Nähe von Besprechungs-, Veranstaltungs- oder Schulungsräumen. Generell sollten nur berechtigte Personen Zugriff auf die ausgedruckten oder kopierten Dokumente erhalten.
- Um Drucker, Faxgeräte, Scanner oder Multifunktionsgeräte mehreren Benutzern zur Verfügung zu stellen, werden sie ans LAN angeschlossen. Damit auf diesem Wege keine Angreifer auf das Gerät zugreifen können, müssen die Netz-Verbindungen geschützt und der Zugriff durch eine Authentisierung reguliert werden.
- Da Drucker, Kopierer und Multifunktionsgeräte im Allgemeinen mehr Funktionen bieten, als im normalen Betrieb benötigt werden, können sich unnötige Risiken ergeben. Daher sollten alle nicht benötigten Funktionen deaktiviert bzw. deren Nutzung so weit wie möglich eingeschränkt werden.
- Bei einem Druckserver handelt es sich oft um ein IT-System mit einem handelsüblichen Betriebssystem. Dieser Server muss genau wie ein Mail-, Datei- oder Web-Server durch entsprechende Sicherheitsmaßnahmen geschützt werden.
- Sollen Drucker, Kopierer, Multifunktionsgeräte oder einzelne Komponenten solcher Geräte außer Betrieb genommen oder ersetzt werden, müssen alle sicherheitsrelevanten Informationen von den Geräten gelöscht werden (vgl. [6]).

Planung und Konzeption
M 2.397 (A) Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten
M 2.398 (A) Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten

Beschaffung
M 2.399 (A) Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten

Umsetzung
M 1.32 (B) Geeignete Aufstellung von Druckern und Kopierern

Aussonderung
M 2.13 (A) Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
M 2.400 (A) Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B3.406

B 3.12 LAN

S3

Ein lokales Netz (LAN) setzt sich aus der Verkabelung sowie den aktiven Netzkomponenten zur Netzkopplung zusammen. Generell können dabei unterschiedliche Verkabelungstypen, wie auch unterschiedliche aktive Netzkomponenten in ein LAN integriert werden. Als aktive Netzkomponenten werden alle Netzkomponenten bezeichnet, die eine eigene (Netz-)Stromversorgung benötigen. Dazu gehören unter anderem Router, Switches, Gateways. Als passive Netzkomponenten werden alle Netzkomponenten betrachtet, die keine eigene Netzstrom-Versorgung benötigen wie z. B. Kabel, Verteilerschränke, Patchfelder, Steckverbinder.

- Es sollte eine Topologie gewählt werden, die Erweiterungen bzw. Wachstum unterstützt. Ad-Hoc-Erweiterungen sollten vermieden werden.
- Flache Topologien sollten nach Möglichkeit vermieden werden, insbesondere bei mittelgroßen bis sehr großen Netzen. Stattdessen sollte die Topologie in Schichten unterteilt werden, wobei jeder Schicht, ähnlich wie beim OSI-Modell, konkrete Aufgaben zugewiesen werden. Bewährt hat sich in diesem Zusammenhang eine hierarchische Topologie, bestehend aus Zugangsschicht, Verteilungsschicht und Kernschicht.
- Bei der Bildung von Teilnetzen sollte darauf geachtet werden, dass alle IT-Systeme und Kommunikationsverbindungen in einem Teilnetz in Bezug auf den Grundwert „Vertraulichkeit" den gleichen Schutzbedarf haben. Darüber hinaus sollten Teilnetze mit unterschiedlichem Schutzbedarf durch granulare Zugriffsberechtigungen (z. B. ACL), Paketfilter oder Sicherheitsgateways getrennt werden.
- Bei der Implementierung von VLANs (Virtual Local Area Network) sollte darauf geachtet werden, dass Teilnetze mit unterschiedlichem Schutzbedarf bezüglich der Vertraulichkeit oder der Integrität der übertragenen Daten nicht ohne weiteres als VLANs auf demselben Switch realisiert werden.
- Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden. Dies betrifft beispielsweise die Betriebssoftware von aktiven Netzkomponenten wie z. B. Switches oder Router, aber auch eine Netzmanagement-Software. Bevor jedoch ein Upgrade oder ein Update vorgenommen wird, muss die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau geprüft werden. Dies geschieht am sinnvollsten in einem physikalisch separaten Testnetz, bevor das Update oder Upgrade in den produktiven Einsatz übernommen wird.
- Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, ist in Abhängigkeit von den entsprechenden Verfügbarkeitsanforderungen die notwendige Redundanz vorzusehen, um einem Teil- oder Totalausfall der relevanten Netzkomponenten mit akzeptablem Aufwand vorzubeugen (vgl. [6]).

Planung und Konzeption
M 2.139 (A) Ist-Aufnahme der aktuellen Netzsituation
M 2.141 (B) Entwicklung eines Netzkonzeptes
M 4.79 (A) Sichere Zugriffsmechanismen bei lokaler Administration
M 5.13 (A) Geeigneter Einsatz von Elementen zur Netzkopplung

Umsetzung
M 4.7 (A) Änderung voreingestellter Passwörter
M 4.80 (B) Sichere Zugriffsmechanismen bei Fernadministration
M 4.82 (A) Sichere Konfiguration der aktiven Netzkomponenten
M 5.7 (A) Netzverwaltung

Betrieb
M 4.81 (B) Audit und Protokollierung der Aktivitäten im Netz

Notfallvorsorge
M 6.52 (A) Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B4.1.

B 3.13 VPN

S3

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes, wie beispielsweise dem Internet, betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. Die sichere Authentisierung der Kommunikationspartner ist auch dann möglich, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

- Es gibt viele unterschiedliche Nutzungsszenarien für VPNs, wie die Durchführung von Fernwartungstätigkeiten, die Anbindung einzelner Mitarbeiter oder ganzer Standorte. Daher muss geklärt werden, welche Einsatzzwecke unterstützt werden sollen und welche VPN-Typen dafür eingesetzt werden (z. B. Site-to-Site-, End-to-End- und End-to-Site-VPNs).
- Ist die Entscheidung gefallen, für bestimmte Verbindungen ein VPN einzusetzen, so muss dessen Aufbau geplant und konzipiert werden.
- Besondere Aufmerksamkeit ist der Definition einer eigenen VPN-Sicherheitsrichtlinie zu widmen, welche auf die allgemeine Sicherheitsleitlinie abgestimmt werden muss.
- Es ist festzulegen, welche Informationen über VPNs übertragen werden dürfen, wo die VPN-Komponenten benutzt werden dürfen und auf welche anderen internen oder externen Netze oder IT-Systeme über ein VPN zugegriffen werden darf.
- Es muss ein Notfallplan für den VPN-Betrieb erstellt werden.
- Es muss festgelegt werden, wie und von wem die Benutzerkonten und die Zugriffsberechtigungen verwaltet und administriert werden (Berechtigungskonzept).
- Alle Dienste und Protokolle, die über den VPN-Zugang zugelassen werden, sowie die darüber zugreifbaren Ressourcen, sind festzulegen.
- Die Anforderungen an die VPN-Sicherheitsmechanismen (z. B. Authentisierung und Integritätssicherung) müssen definiert werden. Es müssen geeignete Verschlüsselungsverfahren zum Schutz der Daten festgelegt werden.
- Nicht mehr verwendete VPN-Zugänge oder Zugänge von Partnern, mit denen die Kooperation bereits beendet wurde, stellen unnötige Sicherheitslücken dar und sind schnellstmöglich zu sperren.
- Die Aktualität der Dienste eines VPNs sollte laufend gemessen und die Protokolldaten müssen regelmäßig ausgewertet werden (vgl. [6]).

Planung und Konzeption
M 2.416 (A) Planung des VPN-Einsatzes
M 2.418 (A) Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung

Beschaffung
M 2.419 (C) Geeignete Auswahl von VPN-Produkten

Umsetzung
M 4.319 (A) Sichere Installation von VPN-Endgeräten
M 4.320 (A) Sichere Konfiguration eines VPNs
M 5.122 (A) Sicherer Anschluss von Laptops an lokale Netze

Betrieb
M 4.321 (A) Sicherer Betrieb eines VPNs

Aussonderung
M 4.322 (B) Sperrung nicht mehr benötigter VPN-Zugänge

Notfallvorsorge
M 6.109 (A) Notfallplan für den Ausfall eines VPNs

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B4.4.

B 3.14 WLAN

S3

Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netze aufzubauen oder bestehende drahtgebundene Netze zu erweitern. WLANs können aufgrund der einfachen Installation nicht nur dauerhaft, sondern auch für temporär zu installierende Netze, wie z. B. für Veranstaltungen, verwendet werden.

- Ein WLAN muss generell gesichert betrieben werden. Es ist genau zu prüfen, welche Daten darüber übermittelt werden sollen. Je nach Sensibilität der Daten sollte dann ein höherer Absicherungsmechanismus, beispielsweise IEEE 802.11i mit einer EAP-Methode, verwendet werden.
- Die Kommunikation im WLAN muss verschlüsselt werden. Das Verschlüsselungsverfahren WEP gilt als unsicher und sollte nicht mehr für eine Absicherung für das WLAN verwendet werden. WPA bzw. WPA2 sind die bessere Wahl.
- Die kryptographischen Schlüssel für den Zugriff auf ein WLAN sind zufällig zu wählen und regelmäßig zu wechseln. Bei WEP täglich, ansonsten spätestens alle 90 Tage.
- Bevor WLAN-Komponenten in Betrieb genommen werden, müssen alle Standardeinstellungen wie SSID, Passwörter für administrative Zugänge, IP-Adresse der Komponente usw. verändert werden.
- Die Verbindung zwischen einem WLAN und einem LAN sollte zusätzlich abgesichert werden, um die benutzten WLAN-Komponenten vor Missbrauch bei der Nutzung fremder Netze und die internen LANs gegen Missbrauch von außen zu schützen.
- Benutzer und Administratoren des WLANs müssen ausreichend geschult werden, um Sicherheitsvorfälle zu minimieren und auf mögliche Gefahren bei einer unsachgemäßen Verwendung des WLANs hingewiesen und sensibilisiert zu werden.
- Bei der Aussonderung von WLAN-Komponenten müssen die Authentifikationsinformationen für den Zugang zum WLAN und anderer erreichbarer Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden (vgl. [6]).

B 3.14 WLAN

S3

Planung und Konzeption
M 2.381 (A) Festlegung einer Strategie für die WLAN-Nutzung
M 2.382 (A) Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung
M 2.383 (A) Auswahl eines geeigneten WLAN-Standards

Beschaffung
M 2.385 (A) Geeignete Auswahl von WLAN-Komponenten

Umsetzung
M 1.63 (B) Geeignete Aufstellung von Access Points
M 4.294 (A) Sichere Konfiguration der Access Points
M 4.295 (A) Sichere Konfiguration der WLAN-Clients
M 5.139 (A) Sichere Anbindung eines WLANs an ein LAN

Betrieb
M 2.388 (B) Geeignetes WLAN-Schlüsselmanagement
M 4.297 (A) Sicherer Betrieb der WLAN-Komponenten

Aussonderung
M 2.390 (C) Außerbetriebnahme von WLAN-Komponenten

Notfallvorsorge
M 6.102 (A) Verhaltensregeln bei WLAN-Sicherheitsvorfällen

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B4.6.

B 3.15 VoIP

S3

Als Voice over Internet Protokoll, kurz VoIP, wird das Telefonieren über Datennetze bezeichnet. Im Gegensatz zu klassischen Telefonlösungen wird kein separates Netz für den Anschluss von Telefonen benötigt, sondern Soft- und Hardphones werden wie Arbeitsplatz-PCs ans LAN angeschlossen.

- Vor dem Einsatz von VoIP muss die Institution die Sicherheitsregeln für VoIP festlegen.
- Es kann performanter, aber dafür aufwändiger sein, das Telefonnetz vom Datennetz zu trennen. Daher sollte entschieden werden, ob eine Trennung erforderlich ist.
- Bei VoIP gibt es zahlreiche, untereinander nicht kompatible Signalisierungsprotokolle, die den Verbindungaufbau und -abbau steuern. Daher muss die Auswahl eines Signalisierungsprotokolls sorgfältig geplant werden, da die verschiedenen Hersteller von VoIP-Geräten oft nur ein Protokoll unterstützen.
- Aufbauend auf den Einsatzszenarien sind die Sicherheitsanforderungen an die zu beschaffenden Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen.
- Bestehen höhere Anforderungen an die Verfügbarkeit der Sprachkommunikation, sollten alternative Kommunikationsmöglichkeiten, wie Mobiltelefone, bereitgestellt werden oder wichtige VoIP-Komponenten redundant ausgelegt werden.
- Viele VoIP-Endgeräte bieten die Möglichkeit zum automatischen Update ihrer Firmware. Es muss sichergestellt werden, dass neue Firmware nur nach erfolgreicher Überprüfung der Authentizität und Integrität des Codes auf die Endgeräte aufgespielt wird.
- Wird VoIP eingesetzt, sind trotzdem in der Regel in einer Institution auch öffentlich zugängliche Telefone, z. B. in einer Tiefgarage oder in Besprechungsräumen, installiert. Unberechtigte können eventuell über die Netzdosen diesen Telefonen auf das LAN zugreifen. Durch eine entsprechende Netzstrukturierung oder andere Verfahren sollte diese Gefahr verringert werden.
- Sollen VoIP-Komponenten, beispielsweise Endgeräte oder Middleware, außer Betrieb genommen oder ersetzt werden, so müssen von den Geräten alle sicherheitsrelevanten Informationen sicher gelöscht werden (vgl. [6]).

B 3.15 VoIP

S3

Planung und Konzeption
M 2.372 (A) Planung des VoIP-Einsatzes
M 2.373 (A) Erstellung einer Sicherheitsrichtlinie für VoIP

Beschaffung
M 2.375 (A) Geeignete Auswahl von VoIP-Systemen

Umsetzung
M 1.30 (A) Absicherung der Datenträger mit TK-Gebührendaten
M 2.29 (B) Bedienungsanleitung der TK-Anlage für die Benutzer
M 4.7 (A) Änderung voreingestellter Passwörter
M 4.287 (A) Sichere Administration der VoIP-Middleware
M 4.288 (A) Sichere Administration von VoIP-Endgeräten

Betrieb
M 3.13 (B) Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
M 4.291 (A) Sichere Konfiguration der VoIP-Middleware
M 4.292 (A) Protokollierung bei VoIP

Aussonderung
M 2.377 (B) Sichere Außerbetriebnahme von VoIP-Komponenten

Notfallvorsorge
M 6.100 (A) Erstellung eines Notfallplans für den Ausfall von VoIP

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B4.7.

B 3.16 Netz- und Systemmanagement

S3

Ein Managementsystem für Netze und die darin verbunden IT-Systeme dient dazu, möglichst alle im lokalen Netz angesiedelten Hard- und Software-Komponenten zentral zu verwalten. Das Netzmanagement umfasst die Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung des effektiven Einsatzes eines Netzes, während sich das Systemmanagement in erster Linie mit dem Management verteilter IT-Systeme befasst. Ohne funktionierendes Netz kommt es zu erheblichen Störungen im Betriebsablauf einer Institution und nicht sachgerecht gewartete IT-Komponenten stellen ein hohes Sicherheitsrisiko dar. Deshalb ist ein funktionierendes Netz- und Systemmanagement für einen reibungslosen IT-Betrieb notwendig.

- Für ein effizientes und sicheres Netz- und Systemmanagement muss eine Strategie bzw. ein Konzept erstellt werden, aus dem klar hervorgeht, welche Komponenten vom Managementsystem verwaltet werden sollen.
- Geltende Sicherheitsrichtlinien müssen durch das Netz- und Systemmanagement eingehalten und unterstützt werden. Es muss ein Berechtigungsmanagement für die Netz- und System-Administration geben.
- Ein zentrales Werkzeug zur Verwaltung der Komponenten sollte genutzt werden. Bei dessen Auswahl muss berücksichtigt werden, dass alle zu verwaltenden Komponenten vom Werkzeug erfasst werden können, dass, wenn nötig, verschiedene Management-Domänen angelegt werden können und dass möglichst ein Rollen- und Rechtekonzept unterstützt wird.
- Die Kommunikation zwischen Netzmanagement-Tool und Netzkomponenten muss ausreichend abgesichert sein. Dies kann entweder durch ein separates Managementnetz oder durch Verwendung von Protokollen, die Authentisierung und Vertraulichkeit gewährleisten, realisiert werden.
- Neu dem Netz hinzugefügte Netzkomponenten und IT-Systeme sollten automatisch erkannt werden und unberechtigt mit dem Netz verbundenen IT-Systemen muss eine Nutzung des Netzes technisch untersagt werden.
- Die Protokollierung der Netznutzung muss Datenschutzgesetzen genügen, sollte einen ausreichenden Umfang haben und durch entsprechende Analysewerkzeuge unterstützt werden.
- Warnungen beim Erreichen von im Netzplan definierten Schwellwerten, Fehler (z. B. Ausfall einer Komponente), Vorfälle (z. B. unerlaubter Portscan) und andere sicherheitsrelevante Ereignisse sollten vom Managementsystem sofort bekannt gemacht werden.
- Es muss einen Notfallplan für den Ausfall eines Managementsystems geben, in dem Wiederanlaufszenarien beschrieben sind. Hierbei ist auf das sichere Wiederanlaufen der Komponenten zu achten. Alle zum Netz- und Systemmanagement gehörenden Dokumente müssen in das Datensicherungskonzept einbezogen werden.
- Die für das Netz- und Systemmanagement zuständigen Administratoren müssen ausreichend gut geschult sein (vgl. [6]).

Planung und Konzeption
M 2.143 (A) Entwicklung eines Netzmanagementkonzeptes
M 2.144 (A) Geeignete Auswahl eines Netzmanagement-Protokolls
M 2.168 (A) IT-System-Analyse vor Einführung eines Systemmanagementsystems
M 2.169 (A) Entwickeln einer Systemmanagementstrategie

Beschaffung
M 2.170 (A) Anforderungen an ein Systemmanagementsystem
M 2.171 (A) Geeignete Auswahl eines Systemmanagement-Produktes

Umsetzung
M 4.91 (A) Sichere Installation eines Systemmanagementsystems

Betrieb
M 2.146 (A) Sicherer Betrieb eines Netzmanagementsystems
M 4.92 (A) Sicherer Betrieb eines Systemmanagementsystems

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B4.2.

S4: Anwendungen

In der letzten Schicht finden sich Bausteine zu elementaren Anwendungen eines Unternehmens. Speziell datenbankbasierte Anwendungen machen den Großteil der in Unternehmen vorgefunden Applikationen aus.

B 4.1 Webserver

S4

Webserver stellen den Clients Informationen zur Verfügung, wie Texte, Bilder, Videos und ähnliches. Zur Kommunikation wird HTTP verwendet, beziehungsweise in verschlüsselter Form HTTPS. Webserver können Informationen sowohl im Internet als auch im Intranet bereitstellen.

- Die zuständigen Administratoren müssen für den sicheren Betrieb des Webservers und der zugehörigen IT-Systeme und Anwendungen geschult werden. Diese Schulungsmaßnahme sollte nach Möglichkeit bereits vor der Beschaffung des Webservers erfolgen, damit die Administratoren frühzeitig effizient in die Konzeption und den Aufbau einbezogen werden können.
- Es sollte eine Redaktion für das Webangebot eingerichtet werden, vor allem ist festzulegen, wer welche Informationen einstellen darf. Es muss festgelegt werden, wie die Inhalte vor einer Veröffentlichung freigegeben werden.
- Da in der Regel Webserver aus dem Internet erreichbar sind, müssen bekannte Softwareschwachstellen so schnell wie möglich beseitigt werden, indem beispielsweise die betroffene Applikation aktualisiert wird.
- Webangebote müssen in kurzen Abständen auf bekannte Sicherheitsprobleme, wie beispielsweise Cross-Site-Scripting, Injection- und Denial-of-Service-Angriffe überprüft werden. Werden Schwachstellen entdeckt, müssen diese so schnell wie möglich beseitigt werden.
- Die Webinhalte müssen regelmäßig auf Schadsoftware untersucht werden. Vorhandene Schadsoftware muss sofort entfernt werden.
- Die Integrität und Vertraulichkeit der übertragenen Informationen sollten zwischen Webserver und Client geschützt werden, beispielsweise durch Einsatz von Verschlüsselungsprotokollen wie Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).
- Wenn sich das Web-Angebot nicht an anonyme Leser, sondern an einen eingeschränkten Benutzerkreis richten soll, müssen Verfahren für die Authentisierung und das Sessionmanagement etabliert werden.
- Die Webinhalte müssen regelmäßig auf Veränderungen überwacht werden. Es muss einen Notfallplan geben, der z. B. beschreibt, was beim Verdacht auf einen Angriff auf den Webserver zu unternehmen ist (vgl. [6]).

Planung und Konzeption
M 2.173 (A) Festlegung einer Webserver-Sicherheitsstrategie

Umsetzung
M 2.175 (A) Aufbau eines Webservers
M 4.94 (A) Schutz der Webserver-Dateien
M 4.95 (A) Minimales Betriebssystem
M 4.98 (A) Kommunikation durch Paketfilter auf Minimum beschränken
M 4.360 (B) Sichere Konfiguration eines Webservers

Betrieb
M 2.174 (A) Sicherer Betrieb eines Webservers
M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen

Notfallvorsorge
M 6.88 (B) Erstellen eines Notfallplans für den Webserver

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B5.4.

B 4.2 Datenbankbasierende Anwendungen

S4

Datenbanksysteme sind Hilfsmittel zur rechnergestützten Organisation, Erzeugung, Veränderung und Verwaltung großer Datensammlungen. Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadaten), die dauerhaft im Datenbanksystem abgelegt werden. Ein Datenbanksystem besteht aus dem so genannten Datenbankmanagement-System und einer oder mehrerer Datenbanken.

- Die zuständigen Administratoren müssen für den sicheren Betrieb des Datenbanksystems geschult werden. Diese Schulungsmaßnahme sollte nach Möglichkeit bereits vor der Beschaffung des Datenbanksystems erfolgen, damit die entsprechenden Administratoren frühzeitig effektiv in die Konzeption und den Aufbau einbezogen werden können.
- Es sind geeignete Mechanismen zur Identifikation und Authentisierung der Datenbankbenutzer einzusetzen, um eine wirkungsvolle Zugangskontrolle zu gewährleisten. Jedem Benutzer muss eine eigene Datenbankkennung zugeordnet sein.
- Zur konsistenten Datenbankverwaltung müssen Rollen mit entsprechenden Rechten und Pflichten festgelegt werden. Hierbei ist zu definieren, welche Aufgaben, Zugriffsrechte und Befugnisse, die zur Durchführung bestimmter Funktionen notwendig sind, einer Rolle zugewiesen werden sollen. Im Anschluss müssen diese dann realen Personen zugeordnet werden. Die Rollen können im Datenbankmanagement-System durch Benutzergruppen abgebildet werden.
- Um Gefährdungen der Datenbankintegrität und Inkonsistenzen einzelner Datensätze zu vermeiden, sind alle Datenbankobjekte einer Anwendung unter die Verwaltung einer für die spezielle Anwendung eingerichteten Benutzergruppe zu stellen. Dieser Benutzergruppe sind dann die Benutzer zuzuordnen, die die Zugriffsrechte zu ihrer Aufgabenerfüllung benötigen. Außerdem sollte der für die jeweilige Anwendung zuständige Datenbankadministrator Mitglied dieser Benutzergruppe sein.
- Wenn in einer Datenbank Informationen mit hohem Schutzbedarf an Vertraulichkeit gespeichert sind, müssen diese Daten verschlüsselt werden.
- Für Problemfälle sollte ein Konzept (Wiederherstellungskonzept) erstellt werden, das Prüfungen, Entscheidungen und Aktionen beschreibt, um eine korrupte Datenbank auf schnellem und sicherem Wege wieder zur Verfügung stellen zu können.
- Regelmäßige Datensicherungen sind durchzuführen. Für die Datensicherung eines Datenbanksystems muss ein eigenes Datensicherungskonzept erstellt werden (vgl. [6]).

S4

Planung und Konzeption
M 2.132 (A) Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen

Beschaffung
M 2.124 (A) Geeignete Auswahl einer Datenbank-Software

Umsetzung
M 2.125 (A) Installation und Konfiguration einer Datenbank
M 4.7 (A) Änderung voreingestellter Passwörter

Betrieb
M 2.31 (A) Dokumentation der zugelassenen Benutzer und Rechteprofile
M 2.34 (A) Dokumentation der Veränderungen an einem bestehenden System
M 2.128 (A) Zugangskontrolle einer Datenbank
M 2.129 (A) Zugriffskontrolle einer Datenbank
M 2.130 (A) Gewährleistung der Datenbankintegrität
M 2.133 (A) Kontrolle der Protokolldateien eines Datenbanksystems
M 3.18 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
M 4.67 (B) Sperren und Löschen nicht benötigter Datenbank-Accounts

Notfallvorsorge
M 6.49 (A) Datensicherung einer Datenbank

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B5.7.

B 4.3 E-Mail (Server und Client)

S4

Exchange 2000 Server ist ein Managementsystem für Nachrichten, das typischerweise in mittleren bis großen Institutionen eingesetzt werden kann, um E-Mails zu verteilen und zuzustellen. Zusätzlich können von Exchange 2000 Server Groupware-Funktionen, wie Kalender und Aufgabenlisten, verwaltet und Newsgroups den Benutzern zur Verfügung gestellt werden. Outlook 2000 ist ein E-Mail-Client, der Bestandteil des Office 2000 Paketes von Microsoft ist. Neben der reinen E-Mail-Nutzung bietet er eine Reihe von Zusatzfunktionen, die den Arbeitsprozess in Unternehmen und Behörden erleichtern sollen.

- Für den Einsatz des Exchange/Outlook-Systems müssen spezifische Sicherheitsvorgaben erstellt werden, die die vorhandenen Sicherheitsrichtlinien berücksichtigen. Die Benutzer und die Administratoren müssen die sie betreffenden Vorgaben kennen.
- Exchange 2000 Server wird in einer Microsoft Server-Infrastruktur installiert. Bei der Installation von Exchange 2000 wird eine Schema-Erweiterung des Active Directory durchgeführt. Damit beeinflusst eine Exchange-Installation das Active Directory nachhaltig, so dass der Schema-Administrator des Windows 2000 Systems beteiligt werden muss.
- Der Exchange Server darf unter keinen Umständen auf einem Domänen-Controller installiert werden, da dies negative Auswirkungen auf die Sicherheit des gesamten Windows-Systems hätte.
- Es dürfen nur die für den Betrieb von Exchange 2000 unbedingt notwendigen Komponenten installiert und in Betrieb genommen werden.
- Für das Exchange-System muss ein Backup- und ein Notfallvorsorge-Konzept erstellt werden. Zumindest der Mailbox Store, der Public Store sowie die Transaction Logs sollten regelmäßig gesichert werden. Da Exchange und Outlook das Windows 2000 Active Directory benötigen, sollte diese Datenbank ebenso gesichert werden.
- Bei der Datensicherung sind auch Outlook-Clients zu berücksichtigen. Besonderes Augenmerk erfordert das Backup von Daten (z. B. lokal gespeicherte Postfächer), die durch Verschlüsselung, Zugangskennwörter oder andere Mechanismen geschützt sind.
- Der Betrieb eines Exchange-Systems muss protokolliert werden: Zum einen hilft die aktivierte Überwachung, potentielle Schwachstellen möglichst frühzeitig zu erkennen und zu beseitigen. Zum anderen dient die Protokollierung dazu, Verstöße gegen die Sicherheitsrichtlinie zu erkennen oder Nachforschungen über einen Sicherheitsvorfall anzustellen. Es muss ein Konzept für ein Audit und die Protokollierung entworfen werden. Dazu ist festzulegen, wie die Audit- und Protokollierungsfunktion des Exchange-Systems genutzt werden.
- Der teilweise oder komplette Ausfall eines Exchange-Systems hat in vielen Fällen gravierende Auswirkungen auf die Arbeitsmöglichkeiten der E-Mail-Benutzer, da alle Server-basierten Aktionen nicht mehr ausgeführt werden können. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten bei einem Ausfall durchzuführen sind (vgl. [6]).

S4

Planung und Konzeption
M 2.247 (A) Planung des Einsatzes von Exchange/Outlook 2000
M 2.248 (A) Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000

Umsetzung
M 3.31 (A) Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren
M 3.32 (A) Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer
M 4.161 (A) Sichere Installation von Exchange/Outlook 2000
M 4.162 (A) Sichere Konfiguration von Exchange 2000 Servern
M 4.163 (A) Zugriffsrechte auf Exchange 2000 Objekte
M 4.164 (A) Browser-Zugriff auf Exchange 2000
M 4.165 (A) Sichere Konfiguration von Outlook 2000

Betrieb
M 4.166 (A) Sicherer Betrieb von Exchange/Outlook 2000

Notfallvorsorge
M 6.82 (C) Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen

Anmerkung:
a) Ein allgemeiner E-Mail Baustein wäre wünschenswert, liegt jedoch aktuell nicht vor. Die Ausführungen aus dem BSI IT-Grundschutzkatalog beziehen sich auf die „veralteten" MS E-Mailsysteme Exchange und Outlook 2000. Die Maßnahmen sind auf andere E-Mail Systeme entsprechend zu adaptieren.
b) Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B5.12.

B 4.4 Mobile Datenträger

S4

Mobile Datenträger werden für eine Vielzahl von Zwecken eingesetzt, beispielsweise für den Datentransport, die Speicherung von Daten oder die Datennutzung unterwegs. Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern, hierzu gehören unter anderem Disketten, externe Festplatten, CD-ROMs, DVDs, Magnetbänder und USB-Sticks. Bei allen mobilen Datenträgern müssen sowohl die gespeicherten Informationen sicher genutzt, als auch gegen eine unbefugte Weitergabe von Informationen über mobile Datenträger vorgebeugt werden.

- Es sollte klare, schriftliche Regeln für den sicheren Umgang mit mobilen Datenträgern geben. Es sollte insbesondere geregelt sein, an wen über mobile Datenträger welche Daten weitergegeben werden dürfen und dass Datenträger von Externen mit Vorsicht behandelt werden müssen, da sie Schadsoftware enthalten könnten.
- Die Mitarbeiter sollten über die Risiken von mobilen Datenträgern und über die daher erforderlichen Sicherheitsmaßnahmen informiert sein. Im Umgang mit externen Speichermedien wie USB-Sticks sollten die Benutzer Vorsicht walten lassen, durch unbedachte Weitergabe können vertrauliche Daten offen gelegt oder Schadprogramme aufgelesen werden.
- Die Nutzung nicht zugelassener mobiler Datenträger sollte möglichst technisch unterbunden werden, z. B. indem auf USB-Schnittstellen nur die intern freigegebenen USB-Datenträger zugreifen können.
- Die Laufwerke und die Schnittstellen der IT-Systeme zur Nutzung von mobilen Datenträgern sollten gemäß den Sicherheitsvorgaben abgesichert werden. Von mobilen Datenträgern sollte nicht gebootet werden können.
- Bei mobilen Datenträgern besteht ein relativ hohes Verlust- und Diebstahlrisiko. Damit die Daten nicht in falsche Hände fallen, sollten die Dateien oder besser die gesamten mobilen Datenträger verschlüsselt sein.
- Bevor wiederbeschreibbare Datenträger weitergegeben werden, sollten sie vor ihrer erneuten Verwendung oder Aussonderung physikalisch gelöscht werden.
- Jeder Verlust oder Diebstahl eines mobilen Datenträgers sollte umgehend gemeldet werden. Dafür sollte es in jeder Institution klare Meldewege und Ansprechpartner geben.
- Die Vielzahl und Varianten von Datenträgern werden weiter zunehmen. Datenträger werden zunehmend „unsichtbar", da sie in anderen Geräten integriert werden. Daher muss regelmäßig untersucht werden, ob die Sicherheitsvorgaben für den Umgang mit mobilen Datenträgern und Geräten noch aktuell sind (vgl. [6]).

Planung und Konzeption
M 2.3 (B) Datenträgerverwaltung
M 2.401 (C) Umgang mit mobilen Datenträgern und Geräten

Umsetzung
M 4.32 (B) Physikalisches Löschen der Datenträger vor und nach Verwendung

Betrieb
M 3.60 (C) Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten
M 4.4 (C) Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern

Aussonderung
M 2.306 (A) Verlustmeldung

Notfallvorsorge
M 6.38 (A) Sicherungskopie der übermittelten Daten

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B5.14.

B 4.5 Verzeichnisdienst

S4

Ein Verzeichnisdienst stellt in einem Computernetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. Diese Daten können gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten brauchen aber nur einmal zentral verwaltet werden. Software für Verzeichnisdienste wird von vielen Herstellen angeboten. Beispiele hierfür sind Active Directory von Microsoft, Novell eDirectory und OpenLDAP.

- Bevor ein Verzeichnisdienst in einer Institution eingesetzt werden kann, muss der Einsatz des Verzeichnisdienstes geplant werden, vor allem die Struktur des Verzeichnisdienstes und die Verteilung der administrativen Aufgaben.
- Als Grundlage für einen sicheren Betrieb eines Verzeichnisdienstes muss ein Sicherheitskonzept und eine Sicherheitsrichtlinie für den Einsatz des Verzeichnisdienstes erstellt werden. Darin muss geregelt werden, wie der Verzeichnisdienst-Server physikalisch abgesichert, welche Komponenten verwendet und welche Benutzer mit welchen Rechten auf den Verzeichnisdienst zugreifen dürfen.
- Beim erstmaligen Aufbau eines Verzeichnisdienstes ist dieser sicher zu installieren. Hierbei ist darauf zu achten, dass restriktive Verzeichnisdienst-Zugriffsberechtigungen und ein mit SSL verschlüsselter LDAP-Zugriff eingerichtet werden. Werden bei der Installation Einstellungen aus anderen Verzeichnisdiensten oder Vorgängerversionen übernommen, so müssen diese aktualisiert und deren Wirksamkeit und Gültigkeit überprüft werden.
- Ein Verzeichnisdienst darf nur durch berechtigte Administratoren konfiguriert werden.
- Verzeichnisdienste sind naturgemäß kontinuierlichen Veränderungen unterworfen. Entsprechend müssen die sicherheitsrelevanten Konfigurationsparameter ständig angepasst werden. Änderungen an Konfigurationseinstellungen müssen bei einem Verzeichnisdienst mit äußerster Vorsicht durchgeführt werden und die Auswirkung jeder Einstellung sind ausgiebig zu testen.
- Benutzer und Administratoren sind hinsichtlich der Verwendung und Administration des Verzeichnisdienstes ausreichend zu schulen.
- Der Sicherheitszustand eines Verzeichnisdienstes muss kontinuierlich überwacht werden. Dafür sollten unter anderem die Sicherheitseinstellungen und die Protokolldateien regelmäßig überprüft werden. Es empfiehlt sich, eine automatisierte Überwachung einzusetzen.
- Für einen Verzeichnisdienst sind verschiedene präventive Maßnahmen zu treffen, um diesen bei Ausfall schnell wieder betriebsbereit machen zu können. Hierzu gehört neben einem Notfallplan für den Ausfall eines Verzeichnisdienstes in jedem Fall eine regelmäßige Datensicherung des kompletten Verzeichnisdienstes, aber auch der Partitionen bei einem verteilten Verzeichnisdienst.
- Wird entschieden, einen Verzeichnisdienst nicht weiter zu betreiben, sind insbesondere die gespeicherten Daten und Rechte sicher zu löschen. Soll bei einem verteilt aufgebauten Verzeichnisdienst eine Partition ausgesondert werden, muss diese Partition gesichert werden, damit bei auftretenden Problemen diese Partition wieder hergestellt werden kann. Ebenso ist sicherzustellen, dass durch die Aussonderung dieser Partition andere Teile des Verzeichnisdienstes nicht beeinträchtigt werden (vgl. [6]).

B 4.5 Verzeichnisdienst

S4

Planung und Konzeption
M 2.403 (A) Planung des Einsatzes von Verzeichnisdiensten
M 2.404 (A) Erstellung eines Sicherheitskonzeptes für Verzeichnisdienste
M 2.405 (A) Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten
M 2.407 (A) Planung der Administration von Verzeichnisdiensten

Beschaffung
M 2.406 (A) Geeignete Auswahl von Komponenten für Verzeichnisdienste

Umsetzung
M 3.62 (A) Schulung zur Administration von Verzeichnisdiensten
M 3.63 (A) Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten
M 4.307 (A) Sichere Konfiguration von Verzeichnisdiensten
M 4.308 (A) Sichere Installation von Verzeichnisdiensten
M 4.309 (A) Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste

Betrieb
M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen
M 4.311 (A) Sicherer Betrieb von Verzeichnisdiensten

Aussonderung
M 2.410 (B) Geregelte Außerbetriebnahme eines Verzeichnisdienstes

Notfallvorsorge
M 6.107 (C) Erstellung von Datensicherungen für Verzeichnisdienste

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B5.15.

B 4.6 Internet-Nutzung

S4

Da das Internet heutzutage zu den wichtigsten Informations- und Kommunikationsmedien gehört, ist es aus dem Arbeitsalltag nicht mehr wegzudenken. In den meisten Institutionen ist die Nutzung von E-Mail, Informationsangeboten, Internet-Dienstleistungen, Online-Banking, E-Commerce- und E-Government-Anwendungen selbstverständlich. Gleichzeitig muss verhindert werden, dass durch die Anbindung an das Internet für die Institution und deren interne IT-Netze unakzeptable Risiken entstehen.

- Es muss ein Konzept festgelegt werden, in dem grundsätzliche Fragen der Internet-Nutzung geklärt sind, beispielsweise welche Internet-Dienste in der Institution genutzt werden sollen, welche Internet-Dienste im internen Netz genutzt werden dürfen, welche Regeln dabei zu beachten sind und wie die internen IT-Systeme, die das Internet nutzen dürfen, zu schützen sind.
- Für die sichere Internet-Nutzung müssen verbindliche Richtlinien festgelegt werden. Dies umfasst beispielsweise, wer welche Internet-Dienste wann und wofür nutzen darf.
- Alle Mitarbeiter sollten über das Potential, aber auch die Risiken der Internet-Nutzung informiert sein. Sie müssen wissen, welche Rahmenbedingungen sie bei der Nutzung von Internet-Diensten beachten müssen. Dazu gehört insbesondere, dass sie die Regeln kennen, um Dienste sicher zu nutzen und sich korrekt im Internet zu verhalten, beispielsweise in Blogs oder Sozialen Netzwerken.
- Alle internen Anwendungen, IT-Systeme und Netzkomponenten sind so zu installieren und konfigurieren, dass Risiken der Internet-Nutzung, insbesondere durch Schadprogramme, minimiert werden.
- Bei allen Internet-Clients sollten die Sicherheitseinstellungen an die Erfordernisse der Institution angepasst werden. Dies gilt vor allem für die Browser. Die Benutzer sollten die von den Administratoren eingestellten Sicherheitsvorgaben nicht ändern können.
- Um ein internes Netz vor Missbrauch durch aktive Inhalte aus dem Internet zu schützen, sollte soweit wie möglich auf deren Ausführung verzichtet werden.
- Alle Kommunikationsverbindungen müssen angemessen abgesichert werden. Vertrauliche Daten dürfen nur verschlüsselt übertragen werden. Bei der Nutzung von Internet-Diensten sollte daher zumindest TLS/SSL eingesetzt werden.
- Sicherheitsrelevante Patches und Updates für alle Komponenten und die genutzte Software müssen systematisch und zeitnah eingespielt werden.
- Da in vielen Geschäftsprozessen eine Internet-Anbindung als selbstverständlich angesehen wird, müssen je nach den Verfügbarkeitsanforderungen geeignete Ausweichverfahren für den Fall von Störungen bei Internet-Anwendungen oder Netzanbindungen festgelegt werden (vgl. [6]).

Planung und Konzeption
M 2.457 (A) Konzeption für die sichere Internet-Nutzung
M 2.458 (A) Richtlinie für die Internet-Nutzung
M 5.66 (B) Verwendung von TLS/SSL
M 5.69 (A) Schutz vor aktiven Inhalten

Umsetzung
M 3.77 (A) Sensibilisierung zur sicheren Internet-Nutzung

Betrieb
M 2.313 (A) Sichere Anmeldung bei Internet-Diensten
M 5.45 (B) Sichere Nutzung von Browsern
M 5.157 (Z) Sichere Nutzung von sozialen Netzwerken
M 5.158 (Z) Nutzung von Web-Speicherplatz

Anmerkung:
Dieser Baustein entspricht dem gekürzten BSI IT-Grundschutzbaustein B5.19.

Literaturverzeichnis

[1] BSI: 2011a
IT-Grundschutz-Kataloge - 11. Ergänzungslieferung - September 2011
https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html

[2] ISO: 2008 a
ISO/IEC 27001
Information technology - Security techniques - Information security management systems - Requirements
http://www.iso.org/iso/catalogue_detail?csnumber=42103

[3] ISO: 2008 b
ISO/IEC 27002
Information technology -- Security techniques -- Code of practice for information security management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[4] BSI: 2011b
IT-Grundschutz-Kataloge - Goldene Regeln
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/GoldeneRegeln.pdf?__blob=publicationFile

[5] BSI: 2011c
Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Vergleich_ISO27001_GS.pdf?__blob=publicationFile

[6] BSI: 2011:5
IT-Grundschutz-Kataloge

Bayerischer IT-Sicherheitscluster e.V.
Bruderwöhrdstr. 15 b
93055 Regensburg

Tel: +49 (0) 941-604889-18
Fax: +49 (0) 941-604889-11

Email: sandra.wiesbeck@it-sec-cluster.de
Internet: www.isis12.de