Cyber-Security für kleine und mittlere Unternehmen (KMU)

Anforderungen

VdS 3473 : 2015-07 (01)

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
D-50735 Köln
Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

VdS-Richtlinien für die Informationssicherheit

Cyber-Security für kleine und mittlere Unternehmen (KMU)

Anforderungen

Inhalt

1 Allgemeines

1.1 Motivation

Für den Erfolg eines Unternehmens sind nicht nur wettbewerbsfähige Produkte und Dienstleistungen notwendig. Die Nutzung moderner IT zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen sowie der Anschluss an das Internet sind heute ebenso unabdingbare Erfordernisse, um im weltweiten Wettbewerb bestehen zu können. Digitalisierung und Vernetzung bergen jedoch auch neue Gefahren, die Unternehmen in ihrem Risikomanagement berücksichtigen müssen. Eine gut organisierte Informationssicherheit vermindert die Anzahl der Schwachstellen, verringert die verbleibenden Risiken und begrenzt dadurch potentielle Schäden für das Unternehmen.

Für die Abwehr „klassischer" Gefahren stehen etablierte Schutz-Standards, insbesondere die Richtlinien der VdS Schadenverhütung GmbH, zur Verfügung. Nun hat die VdS mit den vorliegenden Richtlinien ein auf kleine und mittlere Unternehmen (KMU) zugeschnittenes Verfahren für die Etablierung und Aufrechterhaltung einer angemessenen Informationssicherheit entwickelt.

1.1 Geltungsbereich

Diese Richtlinien legen Mindestanforderungen an die Informationssicherheit fest und können für kleine und mittlere Unternehmen (KMU), den gehobenen Mittelstand, Verwaltungen, Verbände und sonstige Organisationen angewendet werden.

1.2 Anwendungshinweise

Die vorliegenden Richtlinien sind Grundlage für eine Zertifizierung durch die VdS.

Die Umsetzung der geforderten Maßnahmen bedingt Fachwissen und Erfahrung auf dem Gebiet der Informationssicherheit. Sind diese Kenntnisse nicht in ausreichendem Maß vorhanden, empfiehlt sich die Inanspruchnahme qualifizierter Dienstleister gemäß VdS 3477.

Aus Gründen der leichteren Lesbarkeit wird in diesen Richtlinien auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form verwendet. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten.

1.3 Gültigkeit

Diese Richtlinien gelten ab dem 01.07.2015.

2 Normative Verweise

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils zuletzt veröffentlichte Fassung.

BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise

BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4 Notfallmanagement

DIN EN 50173-Reihe Informationstechnik – Anwendungsneutrale Kommunikationskabelanlagen

DIN EN 50174-Reihe Informationstechnik – Installation von Kommunikationsverkabelung

DIN EN ISO 9001 Qualitätsmanagementsysteme – Anforderungen

DIN EN ISO 22301 Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen

ISO 31000 Risk Management – Principles and guidelines

ISO/IEC 27005 Information technology – Security techniques – Information security risk management

VdS 2007 Anlagen der Informationstechnologie (IT-Anlagen) – Merkblatt zur Schadenverhütung

3 Glossar

Administrativer Zugang: Zugang, der einen Nutzer dazu befähigt, ein IT-System zu verwalten, d. h. der einem Nutzer umfangreiche Rechte in einem IT-System einräumt.

Administrator: Ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems oder Netzwerks.

Aktive Netzwerkkomponente: Netzwerkkomponente, die über eine eigene Logik verfügt, wie z. B. Hub, Switch, Repeater, Bridge, Medienkonverter, Gateway, Firewall usw. Eine aktive Netzwerkkomponente benötigt in aller Regel eine Stromversorgung. Eine aktive Netzwerkkomponente ist ein IT-System.

Aufgabe: Dauerhaft wirksame Aufforderung an Handlungsträger, festgelegte Handlungen wahrzunehmen.

Authentizität: Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.

Authentifizierungsmerkmal: Merkmal, mit dessen Hilfe die anfragende Instanz ihre Identität nachweisen kann. Authentifizierungsmerkmale können Wissen (z. B. Passwort oder PIN), Besitz (z. B. Chipkarte oder Token) oder biometrische Merkmale (z. B. Fingerabdruck oder Iris) sein.

Bedrohung: Potentielle Möglichkeit, dass ein Schaden entsteht.

Business Continuity Management (BCM): Ganzheitlicher Managementprozess für die systematische Vorbereitung auf das Bewältigen von Schadenereignissen mit dem Ziel, zentrale Geschäftsprozesse auch beim Eintreten von Notfällen, Krisen oder Katastrophen weiter zu betreiben, bzw. schnellstmöglich wieder in Gang zu setzen.

Cloud Computing: Technologie, die es erlaubt über ein Netz auf einen geteilten Pool von konfigurierbaren IT-Ressourcen zuzugreifen.

Daten: Gebilde aus Zeichen, die aufgrund bekannter Abmachungen Informationen darstellen.

Datenleitung: Physisches Medium, über das Daten ausgetauscht werden können.

Funktion: Bündel von Aufgaben, durch die ein Teil des Unternehmungsziels erreicht werden soll.

Gefahr: Mögliche Schadwirkung auf ein zu schützendes Objekt.

Gefährdung: Bedrohung plus Schwachstelle.

Information: Sinn und Bedeutung, die der Empfänger aus erhaltenen Daten interpretiert.

Informationssicherheit: Schutz von Informationen hinsichtlich gegebener Sicherheitsanforderungen (bspw. Vertraulichkeit, Verfügbarkeit oder Integrität).

Informationssicherheitsbeauftragter (ISB): Person, die die Aufgaben gem. Abschnitt 4.3 wahrnimmt.

Informationssicherheitsprozess: Organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der Informationssicherheit.

Informationssicherheitsteam (IST): Gremium, das die Aufgaben gem. Abschnitt 4.4 wahrnimmt.

Informationstechnik (IT): Oberbegriff für die Informations- und Datenverarbeitung sowie -übertragung inklusive der dafür benötigten Hard- und Software.

Integrität: Korrektheit (Unversehrtheit) von Informationen bzw. die korrekte Funktionsweise der Datenverarbeitung.

IS-Richtlinie: Richtlinie zur Informationssicherheit; siehe Kapitel 6.

IT-Infrastruktur: Alle langlebigen Einrichtungen materieller und institutioneller Art für den Betrieb von Anwendungssoftware.

IT-Ressource: Betriebsmittel für die elektronische Informationsverarbeitung. Hierzu zählen u. a. IT-Systeme, Personal, Datenträger, Verbindungen sowie Daten und Informationen.

IT-Verantwortlicher: Leiter der IT-Abteilung, bzw. das für die Informationstechnik zuständige Management.

IT-Outsourcing: Auslagerung von IT-Aufgaben an rechtlich unabhängige Anbieter.

IT-System: Technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind z. B. Server, Clients, Drucker, Mobiltelefone, Smartphones, Telefonanlagen, Laptops, Tablets und aktive Netzwerkkomponenten.

Katastrophaler Schaden: Schaden, auf den eines der folgenden Kriterien zutrifft:

1. Auswirkungen auf Leib und Leben von Personen:
   Es werden Menschen schwer verletzt oder kommen ums Leben.
2. Auswirkung auf zentrale Geschäftsprozesse:
   Zentrale Geschäftsprozesse werden zum Erliegen gebracht und die Rückkehr zum Regelbetrieb ist (innerhalb eines akzeptablen Zeitraums) nicht möglich.
3. Auswirkung auf zentrale Werte des Unternehmens:
   Zentrale Unternehmenswerte gehen verloren oder werden zerstört und ihre Wiederherstellung ist (mit den Mitteln des Unternehmens) nicht mehr möglich.
4. Auswirkungen auf die Rechtskonformität:
   Gesetze, Verträge oder Normen werden gebrochen und die daraus resultierende Haftung ist für das Unternehmen oder für die Verantwortlichen ruinös.

5. Schadenshöhe:
   Der Schaden kann mit den Mitteln des Unternehmens nicht wieder behoben werden.

Kritisches IT-System: IT-System, das die Bedingungen gem. Abschnitt 9.3 erfüllt.

Kritischer mobiler Datenträger: Mobiler Datenträger, der die Bedingungen gem. Abschnitt 9.3 erfüllt.

Kritische Verbindung: Verbindung, die die Bedingungen gem. Abschnitt 9.3 erfüllt.

Leitlinie: Dokument des Topmanagements, das ein Ziel des Unternehmens und seine Priorität definiert sowie Verantwortlichkeiten zu seiner Erreichung festlegt.

Mitarbeiter: Natürliche Person, die in einem Vertragsverhältnis mit dem Unternehmen steht und eine oder mehrere Positionen im Unternehmen einnimmt.

Mobiler Datenträger: Datenträger, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile Datenträger sind z. B. Speichersticks und -karten sowie externe Festplatten, aber auch Speichermedien wie CD-ROMs, DVDs und Disketten.

Mobiles IT-System: IT-System, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile IT-Systeme sind z. B. Notebooks, Smartphones, Tablets oder Digitalkameras.

Netzwerkkomponente: Technische Anlagen, die der Weiterleitung von Daten dienen. Es werden aktive und passive Netzwerkkomponenten unterschieden.

Netzübergang: Schnittstelle zwischen zwei unterschiedlichen Netzwerken. Dabei können sich die Netzwerke durch die physikalischen Übertragungsmedien, durch die verwendeten Protokolle oder durch eine unterschiedliche administrative Hoheit voneinander unterscheiden.

Notbetriebsniveau: Definition, welche Funktionen von einem IT-System erbracht werden müssen, damit ein Notbetrieb aufrechterhalten werden kann.

Notfall: Situation, in der Prozesse oder Ressourcen eines Unternehmens nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind so hoch, dass sie nicht akzeptabel sind. Die Behandlung eines Notfalls kann nicht im allgemeinen Tagesgeschäft abgewickelt werden.

Passive Netzwerkkomponente: Netzwerkkomponente ohne eigene Logik, z. B. Kabel, Patchfeld, Dose, Stecker usw. Eine passive Netzwerkkomponente benötigt in aller Regel keine Stromversorgung.

Personal: Interne und externe Mitarbeiter.

physischer Zugriff: Umstand, der es ermöglicht, physisch mit einem IT-System oder einem Netzwerk zu interagieren.

Position: Platz, den ein Mitarbeiter in der Hierarchie eines Unternehmens einnimmt.

Projektverantwortlicher: Person, die für die ordnungsgemäße Durchführung eines Projekts des Unternehmens verantwortlich ist.

Prozess: System von Tätigkeiten, das Eingaben mit Hilfe von Mitteln in Ergebnisse umwandelt.

Prozess mit hohem Schadenspotential: Prozess, bei dessen Fehlfunktion oder kurzzeitigem Ausfall ein katastrophaler Schaden entstehen kann.

Prozessverantwortlicher: Person, die inhaltlich für einen oder mehrere Geschäftsprozesse verantwortlich ist. Sie besitzt den Überblick über die für diese Geschäftsprozesse benötigten Ressourcen und über die an sie gestellten Anforderungen.

Ressource: Betriebsmittel, das dem Unternehmen gehört oder ihm zur Verfügung steht.

Risiko: Eine nach Eintrittswahrscheinlichkeit und Schadenshöhe bewertete Gefährdung.

Rolle: Bündel von Verhaltenserwartungen und Verantwortlichkeiten, die an eine Position gerichtet wird.

Schnittstelle: Teil eines IT-Systems, das der Kommunikation dient. Dies sind nicht nur Ethernet- oder Wireless-LAN-Adapter sondern z. B. auch andere Komponenten wie ISDN-Karten, Modems, USB-Ports, NFC- und Infrarot-Schnittstellen, SD-Slots oder Tastaturen.

Schwachstelle: Umstand der es ermöglicht, dass eine Bedrohung mit einem zu schützenden Objekt räumlich und/oder zeitlich zusammentreffen kann.

Server: Zentrales IT-System, über das funktionale und infrastrukturelle Netzdienste realisiert werden.

Sicherheitsvorfall: Unerwünschtes Ereignis, das Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden nach sich ziehen kann. Was genau als Sicherheitsvorfall eingestuft wird, muss von jedem Unternehmen selbst definiert werden.

Störung: Situation, in der Prozesse oder Ressourcen eines Unternehmens nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als gering einzustufen. Die Beseitigung einer Störung kann im allgemeinen Tagesgeschäft vorgenommen werden.

Systemsoftware: Firmware, Betriebssystem und systemnahe Software. Systemsoftware verwaltet die internen und externen Hardwarekomponenten eines IT-Systems.

Topmanagement: Oberste Führungsebene, wie z. B. Vorstände, Geschäftsführer oder Behördenleiter.

Verbindung: Kanal, über den Daten ausgetauscht werden können.

Verfahren: Festgelegte Art und Weise, wie ein Prozess (oder auch eine einzelne Tätigkeit innerhalb eines Prozesses) auszuführen ist.

Verfügbarkeit: Wahrscheinlichkeit, dass ein System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt. Die Verfügbarkeit von Informationen ist vorhanden, wenn diese stets wie vorgesehen genutzt werden können.

Vertraulichkeit: Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein. Die Vertraulichkeit von Informationen ist gegeben, wenn nur der dafür bestimmte Empfängerkreis diese lesen bzw. interpretieren kann.

Zentraler Geschäftsprozess: Geschäftsprozess, der mit entscheidend für die Aufgabenerfüllung des Unternehmens ist. Dies kann z. B. ein Prozess für die Wertschöpfung oder für den Erhalt bzw. die Verbesserung der Wettbewerbsfähigkeit sein.

Zugang: Einrichtung, die es erlaubt, mit der nichtöffentlichen IT des Unternehmens zu kommunizieren.

Zugriff: Datenaustausch zwischen einer zugreifender Instanz und einem IT-System.

4 Organisation der Informationssicherheit

Informationssicherheit ist dynamisch und für jedes Unternehmen individuell. Um mit möglichst geringem Aufwand das vom Unternehmen angestrebte Sicherheitsniveau zu definieren, umzusetzen und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage anzupassen, ist es notwendig, einen entsprechenden Prozess (Informationssicherheitsprozess) zu etablieren.

4.1 Verantwortlichkeiten

Verantwortlichkeiten für den Informationssicherheitsprozess MÜSSEN eindeutig und widerspruchsfrei zugewiesen werden.

4.1.1 Zuweisung und Dokumentation

Es MUSS für jede Verantwortlichkeit im Informationssicherheitsprozess dokumentiert werden:

1. welche Ziele erreicht werden sollen
2. für welche Ressourcen die Verantwortlichkeit besteht
3. welche Aufgaben erfüllt werden müssen, damit die Ziele erreicht werden
4. welche Berechtigungen an die Verantwortlichkeit gebunden sind, um diese wahrnehmen zu können
5. welche Ressourcen für die Wahrnehmung der Verantwortlichkeit zur Verfügung stehen
6. wie und durch welche Position(en) die Erfüllung der Verantwortlichkeit überprüft wird
7. welche Positionen die Verantwortlichkeit wahrnehmen

4.1.2 Funktionstrennungen

Bei der Verteilung der Verantwortlichkeiten im Informationssicherheitsprozess MUSS das Prinzip der Funktionstrennung umgesetzt werden. Widersprüchliche Verantwortlichkeiten DÜRFEN NICHT von ein und derselben Person oder Unternehmenseinheit wahrgenommen werden.

Ist eine Funktionstrennung nicht oder nur mit einem unverhältnismäßig hohen Aufwand durchführbar, MÜSSEN andere Maßnahmen wie Überwachung von Tätigkeiten, Kontrollen oder Leitungsaufsicht umgesetzt werden.

Ist eine Funktionstrennung nicht durchführbar, MUSS dies in der Dokumentation der Funktionsverteilung besonders hervorgehoben und begründet werden.

Um Zuständigkeitslücken oder Überschneidungen von Verantwortlichkeiten im Informationssicherheitsprozess zu vermeiden, MÜSSEN die entsprechenden Regelungen jährlich vom Informationssicherheitsbeauftragten (ISB) überprüft werden.

4.1.3 Ressourcen

Um Verantwortlichkeiten im Informationssicherheitsprozess wahrzunehmen, MUSS das entsprechende Personal im erforderlichen Umfang (siehe Abschnitt 4.1.1) von anderen Tätigkeiten freigestellt werden.

4.1.4 Delegieren von Aufgaben

Verantwortliche für Informationssicherheit DÜRFEN Aufgaben an andere Personen delegieren. Die Verantwortung bleibt jedoch bei ihnen, sodass sie die Erfüllung und das Ergebnis der delegierten Aufgaben überprüfen MÜSSEN.

4.2 Topmanagement

Das Topmanagement MUSS sich zur Wahrnehmung folgender Verantwortlichkeiten verpflichten:

1. übernehmen der Gesamtverantwortung für die Informationssicherheit
2. übernehmen der Verantwortlichkeit für den Informationssicherheitsprozess
3. in Kraft setzen von Richtlinien für die Informationssicherheit (IS-Richtlinien)
4. bereitstellen der notwendigen technischen, finanziellen und personellen Ressourcen für die Informationssicherheit
5. einbetten der Informationssicherheit in die Strukturen, Hierarchien und Arbeitsabläufe des Unternehmens

4.3 Informationssicherheitsbeauftragter (ISB)

Das Topmanagement MUSS die Verantwortlichkeiten eines Informationssicherheitsbeauftragten (ISB) einem Mitarbeiter zuweisen.

Dieser MUSS folgende Verantwortlichkeiten wahrnehmen:

1. initiieren, planen, umsetzen und steuern des Informationssicherheitsprozesses
2. erarbeiten konkreter Verbesserungsvorschläge
3. unterstützen des Topmanagements bei der Erarbeitung und jährlichen Überprüfung sowie bei der Anpassung der IS-Leitlinie (siehe Kapitel 2)
4. unterstützen des Topmanagements in zentralen Fragen der Informationssicherheit
5. erarbeiten und jährliches überprüfen sowie anpassen aller IS-Richtlinien
6. untersuchen von sicherheitsrelevanten Ereignissen
7. einleiten und steuern von Sensibilisierungs- und Schulungsmaßnahmen
8. Ansprechpartner bei Projekten mit Auswirkungen auf die Informationsverarbeitung, sowie bei der Einführung neuer Software und IT-Systeme sein, um sicherzustellen, dass sicherheitsrelevante Aspekte ausreichend beachtet werden
9. jährliches berichten an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit im Unternehmen, insbesondere über Risiken und Sicherheitsvorfälle
10. wahrnehmen der Rolle des zentralen Ansprechpartners für Informationssicherheit

4.4 Informationssicherheitsteam (IST)

Das Topmanagement MUSS ein Informationssicherheitsteam (IST) bestellen.

In diesem MÜSSEN folgende Unternehmenseinheiten bzw. Positionen persönlich oder durch einen Repräsentanten vertreten sein:

1. Topmanagement
2. ISB
3. IT-Verantwortlicher
4. Personal
5. Datenschutzbeauftragter (sofern vorhanden)
6. Das Team MUSS den ISB bei folgenden Tätigkeiten unterstützen:
7. erstellen der IS-Leitlinie und aller IS-Richtlinien
8. jährliches überprüfen der IS-Leitlinie und aller IS-Richtlinien
9. unternehmensweites koordinieren und lenken der Informationssicherheitsmaßnahmen
10. erkennen neuer Gefährdungen

4.5 IT-Verantwortlicher

Die Aufgaben eines IT-Verantwortlichen MÜSSEN vom Topmanagement einem Mitarbeiter zugewiesen werden.

IT-Verantwortliche MÜSSEN folgende Aufgaben wahrnehmen:

1. umsetzen der IS-Richtlinien in ihrem Verantwortungsbereich durch entsprechende technische und organisatorische Maßnahmen
2. abstimmen aller Maßnahmen mit dem ISB, die aus ihrer Sicht zur Verbesserung und Erhaltung der Informationssicherheit in ihrem Verantwortungsbereich ergriffen werden müssen sowie deren Planung, Koordination und Umsetzung

4.6 Administratoren

Die Verantwortlichkeiten eines Administrators MÜSSEN mindestens einem Mitarbeiter zugewiesen werden.

Administratoren MÜSSEN folgende Verantwortlichkeiten wahrnehmen:

1. implementieren technischer Maßnahmen im Informationssicherheitsprozess in Abstimmung mit dem IT-Verantwortlichen
2. erstellen von Vorschlägen für die Verbesserung der Informationssicherheit

4.7 Vorgesetzte mit Personalverantwortung

Vorgesetzte mit Personalverantwortung MÜSSEN sicherstellen, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf das ihnen unterstellte Personal umgesetzt werden.

4.8 Personal

Das Personal MUSS die folgenden Aufgaben wahrnehmen:

1. einhalten und umsetzen aller sie oder ihre Tätigkeit betreffenden Maßnahmen und Regelungen zur Informationssicherheit
2. melden von Störungen, Sicherheitsvorfällen und Notfällen

4.9 Projektverantwortliche

Projektverantwortliche MÜSSEN den ISB bei allen Projekten mit Auswirkung auf die Informationsverarbeitung konsultieren, um sicherzustellen, dass sicherheitsrelevante Aspekte ausreichend beachtet werden.

4.10 Lieferanten und sonstige Auftragnehmer

Das Unternehmen MUSS Lieferanten und sonstigen Auftragnehmer verpflichten, die sie betreffenden Maßnahmen und Regelungen zur Informationssicherheit einzuhalten bzw. umzusetzen, sofern sie Zugriff auf kritische Informationen (siehe Abschnitt 9.2) besitzen oder sie nichtöffentliche Bereiche der Informationstechnologie (IT) des Unternehmens nutzen.

5 Leitlinie zur Informationssicherheit (IS-Leitlinie)

Die Leitlinie zur Informationssicherheit (IS-Leitlinie) ist das zentrale Dokument für den gesamten Informationssicherheitsprozess. In ihr werden die zu erreichenden Ziele durch das Topmanagement vorgegeben und Verantwortlichkeiten sowie Befugnisse definiert.

5.1 Allgemeine Anforderungen

Die IS-Leitlinie MUSS vom Topmanagement beschlossen und bekannt geben werden.

Das Topmanagement MUSS die IS-Leitlinie jährlich auf Aktualität prüfen und ggf. eine Aktualisierung veranlassen.

Die IS-Leitlinie MUSS nach jeder Aktualisierung zeitnah bekannt gegeben werden und in der jeweils aktuellen Form dem Personal zur Verfügung stehen.

5.2 Inhalte

Die IS-Leitlinie MUSS folgende Anforderungen erfüllen:

1. Sie definiert die Ziele und den Stellenwert der Informationssicherheit im Unternehmen.
2. Sie definiert sämtliche Positionen für den Informationssicherheitsprozess und weist auf deren Aufgaben hin.
3. Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin.

6 Richtlinien zur Informationssicherheit (IS-Richtlinien)

Zur Unterstützung und Konkretisierung der IS-Leitlinie ist es notwendig, weitere Vorgaben für die Informationssicherheit zu verabschieden und in einzelnen Dokumenten, den IS-Richtlinien, zu sammeln.

6.1 Allgemeine Anforderungen

Jede IS-Richtlinie MUSS vom ISB unter Mitarbeit des IST erstellt und vom Topmanagement in Kraft gesetzt werden.

Der ISB MUSS jede IS-Richtlinie jährlich auf Aktualität prüfen und ggf. eine Aktualisierung veranlassen.

Bei der Erstellung und Anpassung von IS-Richtlinien SOLLTEN alle gesetzlichen, behördlichen und vertraglichen Anforderungen ermittelt und entsprechend umgesetzt werden.

Die IS-Richtlinien MÜSSEN nach jeder Aktualisierung den Zielgruppen zeitnah bekannt gegeben werden.

Dies MUSS in einer für die Zielgruppe zugänglichen und verständlichen Form geschehen, bspw. im Zuge einer Schulung.

IS-Richtlinien MÜSSEN im Unternehmen umgesetzt oder vom Topmanagement aufgehoben werden.

6.2 Inhalte

Jede IS-Richtlinie MUSS folgende Anforderungen erfüllen:

1. Sie enthält, für wen sie verbindlich ist.
2. Sie begründet, warum sie erstellt wurde und legt fest, was mit ihr erreicht werden soll.
3. Sie verstößt nicht gegen die IS-Leitlinie oder andere Richtlinien.
4. Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin.

6.3 Regelungen für Nutzer

Es MÜSSEN Regelungen für die Nutzung der IT getroffen werden, die für alle Nutzer (inkl. aller Führungsebenen) sowie für die gesamte IT verbindlich sind.

Folgende Regelungen MÜSSEN getroffen werden:

1. Generelle Nutzungsbedingungen
    a. Das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt sind, wird untersagt.
    b. Das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten wird untersagt.
2. Privatnutzung
    a. Es wird definiert, ob die private Nutzung der IT erlaubt ist.
    b. Wenn die private Nutzung der IT erlaubt ist, so wird sie im Sinne des Unternehmens ausgestaltet.
3. Grundlegende Verhaltensregeln
    a. Es wird nur freigegebene Hard- und Software in der IT-Infrastruktur installiert, genutzt oder betrieben.
    b. Es wird untersagt, eigene Netzübergänge zu installieren; es werden ausschließlich die vom Unternehmen bereitgestellten Netzübergänge zur Nutzung freigegeben.
    c. Die in der IT-Infrastruktur installierten Sicherheitseinrichtungen werden nicht deinstalliert, deaktiviert, mutwillig umgangen oder in ihrer Konfiguration verändert.
    d. Zugangskennungen werden nicht weitergegeben.
    e. Informationen werden nicht eigenmächtig verschlüsselt oder vor lesendem Zugriff geschützt; hierfür werden die vom Unternehmen explizit freigegebenen technischen Verfahren genutzt.

4. Informationsfluss bei Abwesenheit
    a. Es wird geregelt, ob neu eintreffende Nachrichten für einen abwesenden Nutzer weitergeleitet werden.
    b. Es wird geregelt, ob und wann auf den Datenbestand eines Abwesenden zugegriffen werden darf.
5. Missbrauchskontrolle
    a. Es werden Mechanismen zur Missbrauchskontrolle definiert und den Betroffenen mitgeteilt.

Das Unternehmen SOLLTE Ausnahmen von den obigen Regelungen in besonders begründeten Fällen ermöglichen.

Ausnahmen MÜSSEN vom ISB im Vorfeld genehmigt und zusammen mit ihrer Begründung dokumentiert werden.

6.4 Regelungen für Lieferanten und sonstige Auftragnehmer

Es MÜSSEN Regelungen für die Nutzung der IT getroffen werden, die für alle Lieferanten und sonstige Auftragnehmer verbindlich sind, die nichtöffentliche Bereiche der IT oder der IT-Infrastruktur des Unternehmens nutzen.

Folgende Regelungen MÜSSEN getroffen werden:

1. Generelle Nutzungsbedingungen
    a. Das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich geschützt sind, wird untersagt.
    b. Das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten wird untersagt.
2. Privatnutzung
    a. Die Privatnutzung der IT wird untersagt.
3. Grundlegende Verhaltensregeln
    a. Änderungen an Sicherheitseinrichtungen sowie die Installation von Netzübergängen (wie z. B. Fernwartungszugänge oder VPN-Verbindungen) werden im Vorfeld mit dem ISB abgestimmt.
    b. Es wird untersagt, Zugangskennungen weiterzugeben.
    c. Es wird untersagt, Informationen eigenmächtig zu verschlüsseln oder vor lesendem Zugriff zu schützen; hierfür werden die vom Unternehmen explizit freigegebenen technischen Verfahren genutzt.
4. Zugriff auf die nichtöffentliche IT
    a. Zugriffe auf die nichtöffentliche IT werden im Vorfeld mit dem ISB abgestimmt.
    b. Wenn IT-Systeme des Dienstleisters auf die nichtöffentliche IT zugreifen, sind diese über grundlegende Sicherheitsmaßnahmen abgesichert; hierfür definiert das Unternehmen Mindestanforderungen.
5. Integrieren von IT-Systemen
    a. Bevor ein IT-System in die IT-Infrastruktur des Unternehmens integriert wird, wird es von einem Administrator freigegeben.

6. Umgang mit den Daten des Unternehmens
    a. Grundsätzlich verbleiben die Daten des Unternehmens in seiner IT-Infrastruktur und dürfen nicht auf fremde IT-Systeme oder Datenträger übertragen werden.
    b. Der Einsatz von mobilen Datenträgern wird von einem zuständigen Administrator im Vorfeld genehmigt.
    c. Mobile Datenträger werden zeitnah auf Schadsoftware getestet, bevor sie in der IT verwendet werden.
    d. Mobile Datenträger auf denen Daten des Unternehmens gespeichert sind, werden grundsätzlich vertraulich behandelt; sie werden nicht weitergegeben oder für andere Personen zugänglich aufbewahrt.
7. Missbrauchskontrolle
    e. Es werden Mechanismen zur Missbrauchskontrolle definiert und den Betroffenen mitgeteilt.

Das Unternehmen SOLLTE Ausnahmen von den obigen Regelungen in besonders begründeten Fällen ermöglichen.

Ausnahmen MÜSSEN vom ISB im Vorfeld genehmigt und zusammen mit ihrer Begründung dokumentiert werden.

6.5 Weitere Regelungen

Im Rahmen dieser VdS-Richtlinien MÜSSEN weitere themenspezifische IS-Richtlinien erarbeitet werden:

1. Mobile IT-Systeme (siehe Abschnitt 10.4)
2. Mobile Datenträger (siehe Abschnitt 12.1)
3. Datensicherung (siehe Abschnitt 16.1)
4. Störungen und Ausfälle (siehe Abschnitt 17.1)
5. Sicherheitsvorfälle (siehe Abschnitt 18.1)

Der Bedarf für weitere IS-Richtlinien MUSS jährlich vom ISB ermittelt werden.

7 Personal

Das Personal ist ein zentraler Faktor für die Implementierung und Aufrechterhaltung der Informationssicherheit. Es ist deshalb notwendig, auch im Personalmanagement die Anforderungen der Informationssicherheit zu berücksichtigen.

7.1 Vor der Einstellung

Wenn eine für die Informationssicherheit des Unternehmens relevante Position besetzt wird, MUSS das Unternehmen sicherstellen, dass der Bewerber über die notwendige Eignung und die erforderliche Vertrauenswürdigkeit verfügt.

7.2 Einstellung und Einarbeitung

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das im Zuge der Einstellung bzw. des Einarbeitens von neuem Personal folgende Punkte sicherstellt:

1. Es wird eine Vertraulichkeitserklärung unterzeichnet, die auch jene Pflichten in Bezug auf Informationssicherheit definiert, die nach Beendigung oder Veränderung des Arbeitsverhältnisses andauern.
2. Neues Personal wird in die IS-Leitlinie, in sämtliche für es verbindliche IS-Richtlinien und sonstige verbindliche Regelungen zur Informationssicherheit eingewiesen.
3. Neues Personal wird im Umgang mit den für sie relevanten Sicherheitsmechanismen geschult (siehe Abschnitt 8.2).
4. Es erhält die benötigten Zugänge und Zugriffsrechte (siehe Kapitel 15) und wird in deren Nutzung geschult.

7.3 Beendigung oder Wechsel der Anstellung

1. Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das bei Beendigung oder Wechsel einer Anstellung folgende Punkte sicherstellt:
2. Soweit erforderlich, werden Personal, Kunden sowie Lieferanten und sonstige Auftragnehmer über Änderungen im Personal- und betrieblichen Bereich informiert.
3. Die Zugänge und Zugriffsrechte (siehe Kapitel 15) des Mitarbeiters werden umgehend überprüft und bei Bedarf angepasst.

8 Wissen

Viele Gefährdungen entstehen aus Unkenntnis oder mangelndem Problembewusstsein oder werden zumindest durch diese Faktoren verstärkt. Deshalb ist es notwendig, dass das Unternehmen über aktuelles Wissen in Bezug auf Informationssicherheit verfügt, das Personal seine Verantwortlichkeiten versteht und es für seine Aufgaben geeignet und qualifiziert ist.

8.1 Aktualität des Wissens

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, mit dem alle relevanten Stellen des Unternehmens sowie ggf. relevante externe Stellen in geeigneter Weise über geänderte rechtliche und technische Bedingungen im Bereich der Informationssicherheit informiert werden.

Das Verfahren MUSS folgende Punkte sicherstellen:

1. Es werden regelmäßig aus verlässlichen Quellen Informationen über die aktuellen technischen und rechtlichen Entwicklungen im Bereich der Informationssicherheit, insbesondere über neue Gefährdungen und mögliche Gegenmaßnahmen, bezogen.
2. Die Informationen werden im Hinblick auf die Bedeutung für die Informationssicherheit zeitnah ausgewertet, um geänderte Gefahrenlagen zu erkennen.
3. Die jeweils Verantwortlichen werden über die relevanten Entwicklungen zeitnah informiert.

Es SOLLTEN Kontakte und Verbindungen zu Interessengruppen und Sicherheitsforen gepflegt werden, damit die Verantwortlichen auf dem aktuellen Wissensstand sind und auf Fachinformationen und -beratung zugreifen können.

8.2 Sensibilisierung, Aus- und Weiterbildung

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das folgende Punkte sicherstellt:

1. Das betroffene Personal wird zielgruppenorientiert über Gefährdungen aufgeklärt und im Umgang mit den vorhandenen Sicherheitsmaßnahmen geschult.
2. Die Inhalte der IS-Leitlinie und sämtlicher relevanter IS-Richtlinien werden vermittelt.
3. Es informiert über Konsequenzen bei Zuwiderhandlung gegen verbindliche Vorgaben.

Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN mit einem Wissenstest abschließen, um das Verständnis des Personals zu ermitteln.

9 Identifizieren kritischer IT-Ressourcen

Der ISB MUSS die kritischen IT-Ressourcen des Unternehmens ermitteln, jährlich prüfen, ob die Aufstellung der kritischen IT-Ressourcen aktuell ist und sie bei Bedarf anpassen.

Das Unternehmen SOLLTE deshalb im Rahmen eines Business Continuity Management (BCM, siehe Kapitel 17) jährlich eine Business Impact Analyse auf Basis eines anerkannten Standards wie BSI-Standard 100-4 oder DIN EN ISO 22301 oder eine Schutzbedarfsanalyse gemäß BSI-Standard 100-2 durchführen.

Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.

9.1 Prozesse

Das Unternehmen MUSS seine zentralen Geschäftsprozesse und seine Prozesse mit hohem Schadenspotential identifizieren und dokumentieren.

Die Dokumentation MUSS folgende Anforderungen erfüllen:

1. Sie enthält eine kurze Beschreibung des Prozesses.
2. Sie begründet, warum der Prozess ein zentraler Prozess bzw. ein Prozess mit hohem Schadenspotential ist.
3. Sie enthält, wer für den Prozess verantwortlich ist (Prozessverantwortlicher).
4. Sie enthält, wie lange ein Ausfall des Prozesses toleriert werden kann (Maximal tolerierbare Ausfallzeit – MTA).

Die Aufstellung der Prozesse und deren Dokumentation MUSS vom Topmanagement freigegeben werden.

9.2 Informationen

Das Unternehmen MUSS jene Informationen ermitteln, die besonders geschützt werden müssen.

Besonders zu schützen sind alle Informationen, bei denen folgende Faktoren zu katastrophalen Schäden führen können:

1. unberechtigte Einsicht, Kenntnisnahme oder Weitergabe (Kriterium „Vertraulichkeit“)
2. Verfälschung (Kriterium „Integrität“)
3. dauerhafter Verlust (Kriterium „Langzeitverfügbarkeit“)
4. kurzzeitige Nichtverfügbarkeit (Kriterium „Unmittelbare Verfügbarkeit“)

Um die kritischen Informationen zu ermitteln MÜSSEN die zentralen Geschäftsprozesse und die Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1) untersucht und sowohl Art als auch Umfang der Informationen berücksichtigt werden.

9.3 IT-Systeme, mobile Datenträger und Verbindungen

Das Unternehmen MUSS seine kritischen IT-Systeme, mobile Datenträger und Verbindungen identifizieren.

IT-Systeme, mobile Datenträger und Verbindungen sind kritisch, wenn sie kritische Informationen (siehe Abschnitt 9.2) verarbeiten, speichern oder übertragen.

Für jedes kritische IT-System, für jeden kritischen mobilen Datenträger und für jede kritische Verbindung MUSS die MTA bestimmt werden. Die MTA MUSS genauso kurz oder kürzer sein wie die kürzeste MTA aller kritischen Prozesse (siehe Abschnitt 9.1), die von dem IT-System, dem mobilen Datenträger oder der Verbindung abhängig sind.

Um die kritischen IT-Systeme, mobilen Datenträger und Verbindungen zu ermitteln KANN ein Top-Down-Ansatz (prozessorientierte Sicht), ein Bottom-Up-Ansatz (systemorientierte Sicht) oder eine Mischung aus beiden verwendet werden. Bei Top-Down wird ermittelt, wo die kritischen Informationen (siehe Abschnitt 9.2) verarbeitet, gespeichert und übertragen werden. Bei Bottom-Up hingegen werden die IT-Systeme, mobilen Datenträger und Verbindungen des Unternehmens untersucht, ob sie kritische Informationen verarbeiten, speichern und übertragen. Eine Mischung aus beiden Ansätzen bietet die Möglichkeit, kritische IT-Systeme, Datenträger und Verbindungen zuverlässiger zu identifizieren.

Nach der Identifizierung der kritischen IT-Systeme, mobilen Datenträger und Verbindungen MUSS ermittelt werden, welche Teile der IT-Infrastruktur für deren Betrieb unbedingt benötigt werden. Auch diese Teile der IT-Infrastruktur sind kritisch.

9.4 Individualsoftware

Das Unternehmen MUSS seine kritische Individualsoftware identifizieren.

Kritische Individualsoftware ist Software, die für den Betrieb von kritischen IT-Systemen (siehe Abschnitt 9.3) zwingend benötigt wird und individuell für das Unternehmen erstellt oder angepasst wurde.

10 IT-Systeme

Die Informationsverarbeitung eines Unternehmens geschieht zum größten Teil elektronisch. Es ist deshalb notwendig, IT-Systeme strukturiert zu verwalten und abzusichern.

10.1 Inventarisierung

Es MUSS eine Inventarisierung vorhanden sein, in der alle IT-Systeme des Unternehmens verzeichnet sind.

Die Inventarisierung MUSS durch entsprechende Verfahren (siehe Abschnitt 10.2.1 und 10.2.2) vollständig und aktuell gehalten werden.

In ihr MÜSSEN folgende Informationen für jedes IT-System dokumentiert werden:

1. eindeutiges Identifizierungsmerkmal
2. Informationen, die eine schnelle Lokalisierung erlauben
3. Einsatzzweck

Darüber hinaus SOLLTEN Besonderheiten der Installation und Konfiguration in der Dokumentation verzeichnet werden.

10.2 Lebenszyklus

10.2.1 Inbetriebnahme und Änderung

Es MUSS ein Verfahren (siehe Anhang A 1) für die Inbetriebnahme und Änderung der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:

1. Es wird ermittelt, ob das IT-System kritisch ist (siehe Abschnitt 9.3).
2. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und die Dokumentation der Netzwerke (siehe Abschnitt 11.1) wird aktualisiert.
3. Der Basisschutz (siehe Abschnitt 10.3) wird umgesetzt.
4. Bei Inbetriebnahme werden voreingestellte Authentifizierungsmerkmale (z. B. Standard-Passwörter) geändert oder die dazugehörigen Zugänge deaktiviert.
5. Bei Inbetriebnahme werden die Arbeitsschritte vom jeweils Verantwortlichen schriftlich bestätigt.

10.2.2 Ausmusterung und Weiterverwendung

Es MUSS ein Verfahren (siehe Anhang A 1) für das Ausmustern und Wiederverwenden der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:

1. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und die Dokumentation der Netzwerke (siehe Abschnitt 11.1) werden aktualisiert.
2. Das IT-System wird auf gespeicherte Informationen untersucht.
3. Es wird überprüft, ob und wie diese Informationen gesichert bzw. archiviert werden müssen.
4. Es wird sichergestellt, dass die auf dem IT-System gespeicherten Informationen archiviert sind, wenn sie dauerhaft verfügbar sein müssen (siehe Abschnitt 9.2).
5. Alle Informationen werden vor unrechtmäßigem Zugriff geschützt, indem sie z. B. zuverlässig gelöscht, überschrieben, aus dem IT-System entfernt werden oder indem das IT-System insgesamt zerstört wird.
6. Sämtliche Arbeitsschritte werden vom jeweils Verantwortlichen schriftlich bestätigt.

10.3 Basisschutz

Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für alle IT-Systeme implementiert werden.

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

10.3.1 Updates

Vom Hersteller verfügbare Sicherheitsupdates für die System- und Anwendungssoftware MÜSSEN nach einem implementierten Verfahren (siehe Anhang A 1) getestet, bei Eignung freigegeben und nach ihrer Freigabe umgehend installiert werden.

10.3.2 Beschränkung des Netzwerkverkehrs

Der Netzwerkverkehr von und zu IT-Systemen MUSS auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden, wenn eines der folgenden Kriterien zutrifft:

1. Es existieren über das Netzwerk ausnutzbare Schwachstellen, die nicht behoben werden (z. B. wenn keine Sicherheitsupdates installiert werden können, Passwörter nicht geändert werden können oder unsichere technische Verfahren eingesetzt werden).
2. Es handelt sich um besonders exponierte IT-Systeme (z. B. um IT-Systeme, die aus dem Internet erreichbar oder die in öffentlich zugänglichen Räumen platziert sind).

10.3.3 Protokollierung

Jedes IT-System MUSS das An- und Abmelden von Nutzern, Fehler und Informationssicherheitsereignisse protokollieren.

Protokolldaten SOLLTEN zentral gespeichert werden.

Protokolldaten MÜSSEN 6 Monate lang aufbewahrt werden, sofern keine gesetzlichen Lösch- oder Aufbewahrungspflichten entgegenstehen.

Die Uhren aller IT-Systeme MÜSSEN auf eine gemeinsame Zeit synchronisiert sein, um Auswertungen von Logeinträgen zu ermöglichen.

10.3.4 Externe Schnittstellen und Laufwerke

Externe Schnittstellen und Laufwerke, die nicht für Geschäftsprozesse benötigt werden, SOLLTEN ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden.

10.3.5 Schadsoftware

Alle IT-Systeme MÜSSEN über einen Schutz vor Schadsoftware verfügen.

Jedes IT-System MUSS mit Hilfe geeigneter Software täglich vollständig auf Anwesenheit von Schadsoftware untersucht werden.

Darüber hinaus SOLLTEN alle IT-Systeme über einen Echtzeitschutz verfügen, der alle Dateien auf die zugegriffen wird auf Schadsoftware untersucht.

Bei IT-Systemen mit einem Echtzeitschutz KANN die vollständige Untersuchung auf Schadsoftware auf einen wöchentlichen Rhythmus reduziert werden.

Das Ausführen erkannter Schadsoftware MUSS verhindert werden.

Die Software zum Schutz gegen Schadsoftware MUSS automatisch täglich nach den neuesten Suchmustern der Hersteller suchen und diese verwenden.

10.3.6 Starten von fremden Medien

Es MUSS sichergestellt werden, dass IT-Systeme nur von autorisierten Medien gestartet werden können.

Dies KANN z. B. über BIOS-Passwörter oder über einen physikalischen Schutz der IT-Systeme umgesetzt werden.

10.3.7 Authentifizierung

Der Zugriff auf alle nichtöffentliche Bereiche der IT-Systeme MUSS durch geeignete Anmeldeverfahren abgesichert werden, die eine Authentifizierung verlangen.

Die Anmeldeverfahren MÜSSEN folgende Punkte sicherstellen:

1. Das systematische Ausprobieren von Anmeldeinformationen wird erschwert.
2. Erfolgreiche und erfolglose Anmeldeversuche werden protokolliert.
3. Interaktive Sitzungen werden beendet oder gesperrt, wenn der Nutzer innerhalb einer vorgegebenen Zeitspanne keine Eingaben tätigt.
4. Erfolgt die Anmeldung über ein Netzwerk, so wird die Vertraulichkeit und Integrität der Anmeldeinformationen (z. B. mit Hilfe entsprechender Authentifizierungsprotokolle) sichergestellt.

Damit die Anmeldeverfahren zuverlässig arbeiten können, MÜSSEN folgende Punkte sichergestellt werden:

1. Zugänge werden strukturiert verwaltet (siehe Kapitel 15).
2. Es werden zuverlässige Authentifizierungsmechanismen verwendet.
3. Es werden keine trivialen Authentifizierungsmerkmale (z. B. einfach zu erratende Passwörter) verwendet.

10.3.8 Zugriffsbeschränkungen

Mit Hilfe geeigneter Zugriffsbeschränkungen MUSS sichergestellt werden, dass Nutzer keine administrativen Arbeiten durchführen können.

Darüber hinaus SOLLTEN durch geeignete Zugriffsbeschränkungen folgende Anforderungen erfüllt werden:

1. *Nutzer können nur auf Informationen zugreifen, die sie zur Erfüllung ihrer Aufgaben benötigen.*
2. *Nutzer können nur auf Informationen schreibend zugreifen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist.*

10.4 Zusätzliche Maßnahmen für mobile IT-Systeme

Mobile IT-Systeme sind in besonderer Weise Gefährdungen durch Diebstahl, unautori-sierte Zugriffe oder unsichere Netze ausgesetzt, die zusätzliche Maßnahmen erforderlich machen.

Folgende Maßnahmen MÜSSEN in Ergänzung zu Abschnitt 10.3 für alle mobilen IT-Systeme umgesetzt werden.

10.4.1 IS-Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 MUSS der Umgang mit mobilen IT-Systemen in einer IS-Richtlinie festgelegt werden.

Die IS-Richtlinie MUSS folgende Punkte sicherstellen:

1. Es wird festgelegt, welche Informationen des Unternehmens auf den mobilen IT-Systemen erhoben, verarbeitet, gespeichert und übertragen werden dürfen.
2. Die Verantwortung für die Datensicherung wird definiert.
3. Die Nutzer werden über die spezifischen Risiken mobiler IT-Systeme (z. B. Gefahren durch Ausspähung bei der Nutzung in der Öffentlichkeit, Verlust oder Diebstahl) informiert und zur Ergreifung entsprechender Gegenmaßnahmen verpflichtet.

4. Es wird untersagt, mobile IT-Systeme an unberechtigte Dritte weiterzugeben.
5. Es wird definiert, ob und welche Software auf den mobilen IT-Systemen von den Nutzern installiert werden darf.
6. Es wird definiert, ob und unter welchen Bedingungen ein Administrator das mobile IT-System orten darf.
7. Es wird definiert, ob und unter welchen Bedingungen ein Administrator die auf einem mobilen IT-System gespeicherten Informationen aus der Ferne löschen darf.

10.4.2 Schutz der Informationen

Die auf dem mobilen IT-System gespeicherten Informationen des Unternehmens MÜSSEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Datenträger erreicht werden.

10.4.3 Verlust

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das festlegt, wie Nutzer und Administratoren beim Verlust eines mobilen IT-Systems vorzugehen haben.

Das Verfahren MUSS insbesondere festlegen, wie und an wen der Verlust zu melden ist und welche Sofortreaktion erfolgt.

Das Verfahren MUSS sicherstellen, dass die auf dem Gerät hinterlegten Zugänge des Unternehmens nach der Verlustmeldung nicht unberechtigt genutzt werden können (z. B. indem die entsprechenden Authentifizierungsmerkmale umgehend zurückgesetzt oder indem Anrufweiterleitungen modifiziert sowie Sprachnachrichten gelöscht werden).

Der Verlust eines mobilen IT-Systems MUSS als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.

10.5 Zusätzliche Maßnahmen für kritische IT-Systeme

Folgende Maßnahmen MÜSSEN in Ergänzung des Abschnitts 10.3 für alle kritischen IT-Systeme umgesetzt werden.

Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

10.5.1 Risikoanalyse und -behandlung

Für kritische IT-Systeme MUSS eine Risikoanalyse und -behandlung etabliert werden (siehe Anhang A 2).

10.5.2 Notbetriebsniveau

Für jedes kritische IT-System SOLLTE ein Notbetriebsniveau definiert werden.

10.5.3 Robustheit

Auf kritischen IT-Systemen DÜRFEN KEINE Entwicklungen oder Tests durchgeführt werden.

Auf kritischen IT-Systemen MÜSSEN alle Netzwerkdienste, die nicht zur Aufgabenerfüllung benötigt werden, deinstalliert, abgeschaltet oder durch geeignete Filtermechanismen unzugänglich gemacht werden.

Auf kritischen IT-Systemen SOLLTE alle Anwendungssoftware deinstalliert werden, die nicht zur Aufgabenerfüllung benötigt wird.

Sämtliche Zugriffsrechte und Privilegien der Anwendungssoftware auf kritischen IT-Systemen SOLLTEN auf ein Mindestmaß reduziert werden.

10.5.4 Externe Schnittstellen und Laufwerke

Externe Schnittstellen und Laufwerke, die nicht für Geschäftsprozesse benötigt werden, MÜSSEN ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden.

10.5.5 Änderungsmanagement

Änderungen, die auf kritischen IT-Systemen umgesetzt werden sollen, MÜSSEN zuvor in einer Testumgebung getestet und freigegeben worden sein.

Für kritische IT-Systeme MUSS ein Mechanismus vorhanden sein, der sicherstellt, dass bei einer Fehlfunktion oder einem Ausfall des IT-Systems aufgrund einer Änderung sein ursprünglicher Zustand innerhalb der MTA wieder hergestellt werden kann.

10.5.6 Dokumentation

Für jedes kritische IT-System MUSS eine Dokumentation vorhanden sein.

Anhand der Dokumentation MUSS es fachlich versierten Personen möglich sein, folgende Punkte nachzuvollziehen:

1. wer für das IT-System verantwortlich ist
2. wie und mit welchen Zugängen und Authentifizierungsmerkmalen der administrative Zugriff auf das IT-System möglich ist
3. welche grundlegenden Designentscheidungen bei der Installation getroffen wurden
4. welche Änderungen vorgenommen wurden
5. wann sie vorgenommen wurden
6. wer sie vorgenommen hat
7. warum sie vorgenommen wurden

10.5.7 Datensicherung

Alle kritischen IT-Systeme MÜSSEN über eine Datensicherung (siehe Kapitel 16) verfügen.

10.5.8 Überwachung

Es MUSS überwacht werden, ob sich kritische IT-Systeme im Regelbetrieb befinden.

Dabei MUSS sichergestellt werden, dass der Ausfall eines kritischen IT-Systems erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.

Darüber hinaus SOLLTEN die Ressourcen kritischer IT-Systeme überwacht werden, um Engpässe zu erkennen, bevor sie akut werden.

10.5.9 Ersatzsysteme und -verfahren

Wenn ein kritisches IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, MUSS das Unternehmen über ein Ersatzsystem oder -verfahren verfügen, das es ermöglicht, die vom kritischen IT-System abhängigen kritischen Prozesse weiter zu betreiben.

Das Ersatzsystem oder –verfahren SOLLTE das Notbetriebsniveau (siehe 10.5.2) des kritischen IT-Systems sicherstellen.

10.5.10 Kritische Individualsoftware

Das Unternehmen MUSS durch vertragliche und/oder organisatorische Regelungen sicherstellen, dass es kritische Individualsoftware (siehe Abschnitt 9.4) auch in Zukunft verwenden und seinen Bedürfnissen anpassen kann.

11 Netzwerke und Verbindungen

Netzwerke und Verbindungen übertragen Informationen und vernetzen IT-Systeme miteinander. Deshalb ist es notwendig, sie angemessen zu sichern.

11.1 Dokumentation

Die Netzwerke des Unternehmens MÜSSEN so dokumentiert sein, dass fachlich versierte Personen folgende Punkte nachvollziehen können:

1. aktive Netzwerkkomponenten
2. Verbindungen untereinander
3. Verbindungen mit externen Netzwerken
4. Aufgabe
5. physikalisches Medium

11.2 Aktive Netzwerkkomponenten

Aktive Netzwerkkomponenten sind IT-Systeme und MÜSSEN gemäß Kapitel 10 behandelt werden.

11.3 Netzübergänge

Die notwendigen Sicherheitsmaßnahmen für Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken MÜSSEN im Zuge einer Risikoanalyse und –behandlung (siehe Anhang A 2) ermittelt werden.

Die Konfiguration der Netzwerkkomponenten, die einen Netzwerkübergang zu weniger oder nicht vertrauenswürdigen Netzwerken implementieren, MUSS jährlich überprüft werden und folgende Anforderungen erfüllen:

1. Für die sicherheitsrelevanten Einstellungen sind folgende Punkte dokumentiert:
    a. wer sie implementiert hat
    b. wann sie implementiert wurden
    c. was sie bewirken
    d. warum sie benötigt werden
2. Die angestrebten Verkehrsbeschränkungen werden wirksam umgesetzt.

11.4 Basisschutz

Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für alle Netzwerke implementiert werden.

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

11.4.1 Netzwerkanschlüsse

Dauerhaft nicht genutzte Netzwerkanschlüsse MÜSSEN vor unberechtigter Nutzung gesichert werden.

Dies KANN bspw. durch eine physische Zugriffs- oder Zutrittsbeschränkung, eine Deaktivierung der Netzwerkanschlüsse oder durch eine Authentifizierung der IT-Systeme geschehen.

11.4.2 Segmentierung

Die Notwendigkeit einer Segmentierung der Netzwerke des Unternehmens MUSS geprüft und die Entscheidung dokumentiert werden.

Die Umsetzung der Segmentierung MUSS eine möglichst umfassende Beschränkung der Verbindungen sowie die Möglichkeit der Protokollierung von blockierten Verbindungen beinhalten.

11.4.3 Fernzugriff

Zugriffe über weniger oder nicht vertrauenswürdige Netzwerke auf nichtöffentliche Daten bzw. nichtöffentliche Bereiche von IT-Systemen des Unternehmens MÜSSEN abgesichert werden.

Dabei MÜSSEN folgende Anforderungen erfüllt werden:

1. Die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen wird geschützt.
2. Der Zugriff wird so gestaltet, dass über ihn nur IT-Systeme erreichbar sind, die der jeweilige Nutzer für seine Aufgabenerfüllung benötigt.

Darüber hinaus SOLLTEN folgende Anforderungen erfüllt werden:

1. Der Zugriff erfolgt über eine Remote-Desktop-Verbindung, die sicherstellt, dass Informationen des Unternehmens nicht auf die zugreifenden IT-Systeme kopiert werden können.
2. Der Nutzer wird, vor allem wenn er umfangreiche Zugriffsrechte besitzt, mit Hilfe einer Mehr-Faktor-Authentifizierung authentifiziert, um die Gefahr eines unberechtigten Zugriffs zu verringern.
3. Der Zugriff wird so gestaltet, dass nicht nur der Nutzer, sondern auch das zugreifende IT-System authentifiziert wird.

11.4.4 Netzwerkkopplung

Die Kopplung von Unternehmensnetzwerken über weniger oder nicht vertrauenswürdige Netzwerke hinweg MUSS abgesichert werden.

Dabei MÜSSEN die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen gewährleistet werden.

11.5 Zusätzliche Maßnahmen für kritische Verbindungen

In Ergänzung des Abschnitts 11.4 MUSS für kritische Verbindungen eine Risikoanalyse und -behandlung (siehe Anhang A 2) etabliert werden.

12 Mobile Datenträger

Mobile Datenträger sind aufgrund ihrer exponierten Nutzungsart besonders gefährdet. Deshalb ist es notwendig, die damit verbundenen Risiken angemessen zu behandeln.

12.1 IS-Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 MUSS der Umgang mit mobilen Datenträgern in einer IS-Richtlinie festgelegt werden.

Die IS-Richtlinie MUSS folgende Anforderungen erfüllen:

1. Es wird festgelegt, welche Informationen des Unternehmens auf mobilen Datenträgern gespeichert werden dürfen.
2. Die Nutzer werden über die spezifischen Risiken mobiler Datenträger (z. B. Gefahren durch Verlust oder Diebstahl oder durch das Einschleppen von Schadsoftware) informiert und zur Ergreifung entsprechender Gegenmaßnahmen verpflichtet.
3. Es wird untersagt, mobile Datenträger an unberechtigte Dritte weiterzugeben oder zu verleihen.

12.2 Zusätzliche Maßnahmen für kritische mobile Datenträger

Folgende Maßnahmen MÜSSEN in Ergänzung des Abschnitts 12.1 für alle kritischen mobilen Datenträger umgesetzt werden.

12.2.1 Risikoanalyse und -behandlung

Für kritische mobile Datenträger MUSS eine Risikoanalyse und –behandlung etabliert werden (siehe Anhang 4).

12.2.2 Schutz der gespeicherten Informationen

Die auf kritischen mobilen Datenträgern gespeicherten Informationen des Unternehmens MÜSSEN vor unberechtigter Einsichtnahme und Veränderung geschützt werden.

Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Datenträger erreicht werden.

12.2.3 Verlust

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, wie Nutzer und Administratoren beim Verlust eines kritischen mobilen Datenträgers vorzugehen haben.

13 Umgebung

Das Unternehmen MUSS seine IT-Systeme und Datenleitungen gegen negative Umwelteinflüsse absichern.

Dies SOLLTE auf Basis eines anerkannten Standards wie z. B. VdS 2007 erfolgen.

Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die in den folgenden Abschnitten geforderten Punkte sicherstellt.

13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen

Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen (z. B. Patchfelder) MÜSSEN durch entsprechende Maßnahmen vor Beschädigung und unberechtigtem physischen Zugriff geschützt werden.

Dies KANN z. B. durch bauliche Maßnahmen (Serverraum) oder durch abschließbare Schränke (Server- oder Netzwerkschränke) umgesetzt werden.

Für Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen SOLLTEN folgende Anforderungen ermittelt und deren Erfüllung durch geeignete bauliche, technische und organisatorische Maßnahmen sichergestellt werden:

1. *Umgebungsbedingungen (wie z. B. Temperatur, Luftfeuchtigkeit, Staub oder Rauch)*
2. *Stromversorgung*
3. *Schutz vor Elementarschäden (Feuer, Wasser, Blitz und Überspannung)*
4. *Schutz vor Diebstahl*
5. *Schutz vor unberechtigtem physischen Zugriff*

13.2 Datenleitungen

Fest installierte Datenleitungen MÜSSEN durch entsprechende bauliche Maßnahmen vor Beschädigung geschützt werden.

Dies KANN z. B. durch das Verlegen der Datenleitungen in Kabelkanälen umgesetzt werden.

Sämtliche Datenleitungen SOLLTEN gemäß gängiger Normen und Standards wie z. B. DIN EN 50173/4-Reihe installiert werden.

13.3 Zusätzliche Maßnahmen für kritische IT-Systeme

Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.5.1) MÜSSEN für jedes kritische IT-System folgende Bedrohungen behandelt werden:

1. ungeeignete Umgebungsbedingungen (wie z. B. Temperatur, Luftfeuchtigkeit, Staub oder Rauch)
2. unzuverlässige Stromversorgung und elektrische Anlagen
3. Elementarschäden (Feuer, Wasser, Blitz und Überspannung)
4. Einbruch, Diebstahl, Sabotage, Vandalismus
5. Unberechtigter physischer Zugriff

14 IT-Outsourcing und Cloud Computing

Wenn IT-Ressourcen ausgelagert werden, ist es notwendig, dass die Sicherheitsinteressen des Unternehmens berücksichtigt werden.

14.1 Vorbereitung

Jedes Vorhaben, das zur Auslagerung von IT-Ressourcen führt, MUSS vom Topmanagement genehmigt werden.

Für jedes Vorhaben MÜSSEN folgende Parameter dokumentiert werden:

1. welche IT-Ressourcen ausgelagert werden sollen
2. welche betrieblichen, gesetzlichen und vertraglichen Bestimmungen, insbesondere in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität der ausgelagerten IT-Ressourcen, erfüllt werden müssen
3. ob die auszulagernden IT-Ressourcen kritisch sind

Wenn IT-Ressourcen ausgelagert werden, MUSS das Unternehmen mit den folgenden Schritten darauf vorbereitet werden:

1. Kompetenzen für die Steuerung der auszulagernden IT-Ressourcen werden aufgebaut.
2. Die IT-Infrastruktur wird auf das Zusammenspiel mit den auszulagernden IT-Ressourcen vorbereitet.

14.2 Vertragsgestaltung

Wenn IT-Ressourcen ausgelagert werden sollen, so MUSS mit dem Anbieter ein Vertrag geschlossen werden, der die Anforderungen aus Abschnitt 14.1 enthält und den Anbieter zu deren Erfüllung verpflichtet.

Darüber hinaus SOLLTE sichergestellt sein, dass Ansprüche aus Vertragsverletzungen durchgesetzt werden können, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie das Unternehmen befindet.

14.3 Zusätzliche Maßnahmen für kritische IT-Ressourcen

Wenn kritische IT-Ressourcen (siehe Kapitel 9) ausgelagert werden, MÜSSEN die Anforderungen aus Abschnitt 14.1 an ihre Vertraulichkeit, Verfügbarkeit und Integrität im Rahmen einer Risikoanalyse ermittelt und folgende Punkte vertraglich geregelt werden:

1. Leistungen
    a. Die vom Anbieter zu erbringende Leistungen werden definiert sowie deren Messung und Überwachung werden vereinbart.
    b. Die Standorte, an denen Leistungen erbracht werden, werden festgelegt.
    c. Die Sicherheitsmaßnahmen, die der Anbieter zum Schutz der ausgelagerten IT-Ressourcen treffen muss, werden vereinbart.
    d. Eine Beschreibung der Schnittstellen zwischen der IT-Infrastruktur des Unternehmens und den ausgelagerten IT-Ressourcen wird definiert.

2. Kommunikation
    a. Die Ansprechpartner auf Seiten des Unternehmens und des Anbieters werden benannt.
    b. Eine Vertraulichkeitsvereinbarung wird getroffen.
    c. Es wird vereinbart, ob und unter welchen Bedingungen der Anbieter dazu berechtigt ist, Daten an Dritte weiterzugeben.
    d. Eine Informationspflicht des Anbieters bei Sicherheitsvorfällen die die ausgelagerten IT-Ressourcen betreffen, wird vereinbart.
3. Leistungsänderungen und Vertragsauflösung
    a. Die Mitwirkungspflichten des Anbieters im Falle einer Vertragsauflösung oder Insolvenz werden vereinbart, insbesondere die vollständige Herausgabe der IT-Ressourcen des Unternehmens sowie die aktive Unterstützung des Migrationsprozesses durch den Anbieter.
    b. Eine schriftliche Dokumentation und Meldung bei Änderungen an einem der oben genannten Punkte wird vereinbart.
    c. Konsequenzen bei Nichteinhaltung der vertraglich vereinbarten Leistungen werden vereinbart.

Es MUSS sichergestellt sein, dass Ansprüche aus Vertragsverletzungen durchgesetzt werden können, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie das Unternehmen befindet.

15 Zugänge und Zugriffsrechte

Zugänge und Zugriffsrechte erlauben es, auf die nichtöffentliche IT des Unternehmens und seine Daten zuzugreifen. Deshalb ist es notwendig, beide strukturiert zu verwalten.

15.1 Verwaltung

Es MÜSSEN Verfahren (siehe Anhang A 1) für das Anlegen und Ändern von Zugängen und Zugriffsrechte sowie für das Zurücksetzen von Authentifizierungsmerkmalen implementiert werden, die folgende Punkte sicherstellen:

1. Die jeweiligen Vorgänge werden vor ihrer Umsetzung beantragt, geprüft und genehmigt.
2. Zugänge und Zugriffsrechte werden nur genehmigt, wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers oder für die betrieblichen Abläufe des Unternehmens notwendig sind.
3. Wenn ein Nutzer administrative Zugänge oder Zugriffsrechte erhalten soll, wird dies besonders begründet und vom IT-Verantwortlichen entschieden.
4. Antragssteller und Nutzer werden zeitnah über die erfolgte Durchführung informiert; wenn Zugänge entzogen werden, muss nur der Antragssteller informiert werden.
5. Vor dem Löschen eines Zugangs werden die Daten, die mit ihm verknüpft sind, weitergegeben, gelöscht oder gesichert bzw. archiviert.
6. Die jeweiligen Vorgänge werden dokumentiert.

15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Daten

Alle Zugänge zu kritischen IT-Systemen (siehe Abschnitt 9.3) sowie sämtliche Zugriffsrechte auf kritische Informationen (siehe Abschnitt 9.2) MÜSSEN jährlich erfasst und

daraufhin überprüft werden, ob sie gemäß der Verfahren aus Abschnitt 15.1 angelegt wurden und benötigt werden.

Nicht ordnungsgemäß angelegte Zugänge und Zugriffsrechte MÜSSEN als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.

16 Datensicherung und Archivierung

Daten können unbrauchbar werden oder verloren gehen. Deshalb ist es notwendig, durch eine Datensicherung die Integrität und Verfügbarkeit der Daten sicherzustellen.

Die Datensicherung SOLLTE auf Basis eines anerkannten Standards wie z. B. BSI-Standard 100-2 unter Berücksichtigung der IT-Grundschutz-Kataloge des BSI implementiert werden.

Wenn eine andere Vorgehensweise gewählt wird, so MÜSSEN die Anforderungen folgender Abschnitte erfüllt werden.

16.1 IS-Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 MÜSSEN die Speicherorte für die Daten des Unternehmens in einer IS-Richtlinie festgelegt werden.

Die Daten des Unternehmens SOLLTEN möglichst zentral gespeichert werden, um eine effektive Datensicherung zu ermöglichen.

16.2 Archivierung

Das Unternehmen MUSS prüfen, welche Daten archiviert werden müssen, um betrieblichen, gesetzlichen und vertraglichen Anforderungen zu genügen.

16.3 Verfahren

Für die Datensicherung, -wiederherstellung und -archivierung MÜSSEN Verfahren (siehe Anhang A 1) implementiert werden, die folgende Punkte sicherstellen:

1. Die gesicherten Daten werden bei Übertragung, Lagerung und Transport vor Änderungen, Beschädigung, Verlust und unberechtigter Einsichtnahme geschützt.
2. Die gesicherten Daten werden nicht im gleichen Brandabschnitt wie die gesicherten IT-Systeme aufbewahrt.

Einzelne Datensicherungen SOLLTEN an einem entfernten Standort aufbewahrt werden, damit die Datensicherung auch im Katastrophenfall verfügbar bleibt.

16.4 Weiterentwicklung

Der ISB MUSS jährlich prüfen, ob Änderungen an IT-Systemen sowie betrieblichen, gesetzlichen oder vertraglichen Rahmenbedingungen eine Anpassung der Sicherungs-, Wiederherstellungs- und Archivierungsverfahren erforderlich machen.

Notwendige Anpassungen MÜSSEN zeitnah implementiert und dokumentiert werden.

16.5 Basisschutz

Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für Speicherorte (siehe Abschnitt 16.1), Server, aktive Netzwerkkomponenten und mobile IT-Systeme implementiert werden.

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

16.5.1 Speicherorte

Speicherorte MÜSSEN so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist.

16.5.2 Server

Server MÜSSEN so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand (Systemsoftware, Konfigurationen, Anwendungssoftware und Anwendungsdaten) nicht älter als 24 Stunden ist.

16.5.3 Aktive Netzwerkkomponenten

Systemsoftware und Konfiguration der aktiven Netzwerkkomponenten MÜSSEN nach jeder Änderung gesichert werden.

16.5.4 Mobile IT-Systeme

Es MUSS ein technisches Verfahren für die Datensicherung von den Administratoren vorgegeben werden.

16.5.5 Tests

Sicherungs- und Wiederherstellungsverfahren MÜSSEN getestet werden:

1. Einmal jährlich wird ein gesichertes IT-System nach dem Zufallsprinzip ausgewählt und in einer Testumgebung wiederhergestellt.
2. Nach jeder Änderung des Sicherungs- oder des Wiederherstellungsverfahrens wird eines der betroffenen IT-Systeme gesichert und in einer Testumgebung wiederhergestellt.

Die Tests SOLLTEN ohne Unterstützung durch den jeweiligen Verantwortlichen für die Datensicherung erfolgen. Vielmehr SOLLTEN sie von einem anderen Mitarbeiter anhand der vorliegenden Dokumentation bewältigt werden.

Die vorhandenen Sicherungs- und Wiederherstellungsverfahren MÜSSEN anhand der Ergebnisse und Erkenntnisse der Tests zeitnah überarbeitet werden.

Die Durchführung und die Ergebnisse der Tests MÜSSEN dokumentiert werden.

16.6 Zusätzliche Maßnahmen für kritische IT-Systeme

Jedes kritische IT-System MUSS über eine Datensicherung verfügen, die in Ergänzung des Abschnitts 16.5 folgende Anforderungen erfüllt.

16.6.1 Risikoanalyse

Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.5.1) MÜSSEN die Folgen eines Datenverlusts analysiert und dabei der maximal tolerierbare Datenverlust (MTD) sowie die MTA bestimmt werden.

16.6.2 Verfahren

Die Verfahren zur Datensicherung und -wiederherstellung MÜSSEN folgende Punkte sicherstellen:

1. Kritische IT-Systeme werden vollständig gesichert (Systemsoftware, Konfigurationen, Anwendungssoftware und Anwendungsdaten).
2. Der MTD wird nicht überschritten.
3. Die Wiederherstellung innerhalb der MTA wird gewährleistet, sofern keine Ersatzsysteme oder -verfahren verfügbar sind (siehe Abschnitt 10.5.9).

16.6.3 Tests

Sicherungs- und Wiederherstellungsverfahren für kritische IT-Systeme MÜSSEN jährlich gemäß 16.5.5 an einem kritischen IT-System getestet werden.

17 Störungen und Ausfälle

Eine angemessene Reaktion auf Ausfälle ermöglicht es einem Unternehmen zügig den Regelbetrieb wieder aufzunehmen und so Schäden zu minimieren.

Zu diesem Zweck SOLLTE das Unternehmen ein BCM auf Basis eines anerkannten Standards wie BSI-Standard 100-4 oder DIN EN ISO 22301 implementieren.

Wenn eine andere Vorgehensweise gewählt wird, so MÜSSEN die Anforderungen folgender Abschnitte erfüllt werden.

17.1 IS-Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 MUSS der Umgang mit Störungen und Ausfällen in einer IS-Richtlinie festgelegt werden.

Die IS-Richtlinie MUSS folgende Punkte sicherstellen:

1. Die Begriffe „Störung“ und „Ausfall“ werden klar definiert.

   Hierbei SOLLTE aufgezählt werden, welche Auffälligkeiten zur Meldung einer möglichen Störung bzw. eines möglichen Ausfalls führen müssen.
2. Jeder Mitarbeiter meldet mögliche Störungen und Ausfälle an einen Administrator.
3. Administratoren untersuchen, ggf. in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, dem IT-Verantwortlichen und dem ISB, Störungen und Ausfälle vordringlich.
4. Es wird definiert, in welchen Fällen das Topmanagement über Störungen und Ausfälle informiert wird.
5. Es wird definiert, wie das Unternehmen intern und nach außen über akute und bewältigte Störungen und Ausfälle kommuniziert.

17.2 Reaktion

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das beim Auftreten einer Störung oder eines Ausfalls folgende Reaktionen in folgender Reihenfolge sicherstellt:

1. Es wird ein Überblick über die Situation gewonnen.
2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.
3. Der Schaden wird durch Sofortmaßnahmen eingedämmt.
4. Der Schaden wird dokumentiert.
5. Beweismittel werden gesichert.
6. Der Schaden wird behoben und die regulären Geschäftsprozesse wieder aufgenommen.
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden.

Bei geringfügigen Störungen oder Ausfällen SOLLTE es möglich sein, das Verfahren vorzeitig zu beenden.

17.3 Zusätzliche Maßnahmen für kritische IT-Systeme

17.3.1 Wiederanlaufpläne

Für jedes kritische IT-System MUSS ein Wiederanlaufplan erstellt werden, der folgende Anforderungen erfüllt:

1. Er enthält alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, das IT-System innerhalb der MTA soweit wieder herzustellen, dass das Notbetriebsniveau erreicht ist.
2. Er enthält die benötigten Ressourcen, wie z. B. Personal und dessen Kontaktdaten, Hardware, Software, Netzwerke, Dienste, Passwörter.
3. Er ist verständlich und übersichtlich strukturiert.
4. Er ist auch bei einem Notfall schnell verfügbar.
5. Er wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.

17.3.2 Abhängigkeiten

Es MÜSSEN die Abhängigkeiten der kritischen IT-Systeme untereinander dokumentiert werden.

Die Dokumentation MUSS folgende Anforderungen erfüllen:

1. Aus ihr geht eindeutig hervor, in welcher Reihenfolge die kritischen IT-Systeme wiederhergestellt werden müssen.
2. Sie ist verständlich und übersichtlich strukturiert.
3. Sie auch bei einem Notfall schnell verfügbar.
4. Sie wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.

18 Sicherheitsvorfälle

Eine angemessene Reaktion auf Sicherheitsvorfälle ermöglicht es einem Unternehmen, Schäden schnell einzudämmen und beheben zu können. Deshalb ist es notwendig, angemessen auf Sicherheitsvorfälle vorbereitet zu sein.

18.1 IS-Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 MUSS der Umgang mit Sicherheitsvorfällen in einer IS-Richtlinie festgelegt werden.

Die IS-Richtlinie MUSS folgende Punkte sicherstellen:

1. Der Begriff des Sicherheitsvorfalls wird klar definiert.

   Hierbei SOLLTE aufgezählt werden, welche Auffälligkeiten zur Meldung eines potentiellen Sicherheitsvorfalles führen müssen.

2. Jeder Mitarbeiter meldet mögliche Sicherheitsvorfälle an den ISB.
3. Der ISB untersucht, ggf. in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, dem IT-Verantwortlichen und den Administratoren, Sicherheitsvorfälle vordringlich.
4. Es wird definiert, in welchen Fällen das Topmanagement über Sicherheitsvorfälle informiert wird.
5. Es wird definiert, wie das Unternehmen intern und nach außen über akute und bewältigte Sicherheitsvorfälle kommuniziert.

18.2 Erkennen

Das Unternehmen SOLLTE Maßnahmen implementieren, die es ermöglichen, Sicherheitsvorfälle zu erkennen, wie z. B.

1. *Intrusion Detection Systeme (IDS)*
2. *Integritätsprüfungen auf Prüfsummenbasis*
3. *Sensor-Systeme (Honeypots)*
4. *überwachen der Zugriffe auf besonders sensible Dateien*
5. *erfassen und auswerten von Logmeldungen*

18.3 Reaktion

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das beim Auftreten eines Sicherheitsvorfalls folgende Reaktionen in folgender Reihenfolge sicherstellt:

1. Es wird ein Überblick über die Situation gewonnen.
2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.
3. Der Schaden wird durch Sofortmaßnahmen eingedämmt.
4. Der Schaden wird dokumentiert.
5. Beweismittel werden gesichert.
6. Der Schaden wird behoben und die regulären Geschäftsprozesse wieder aufge-nommen.
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden.

Bei geringfügigen Sicherheitsvorfällen SOLLTE es möglich sein, das Verfahren vorzeitig zu beenden.

Anhang A Anhang

A.1 Verfahren

Das Unternehmen MUSS die in diesen Richtlinien geforderten Verfahren planen, steuern und stetig verbessern.

Dies SOLLTE im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z. B. DIN EN ISO 9001 geschehen.

Wenn eine andere Vorgehensweise gewählt wird, so MÜSSEN folgende Anforderungen erfüllt werden:

1. Es wird definiert, wer für die Durchführung verantwortlich ist.
2. Verfahren werden in einer für die jeweilige Zielgruppe zugänglichen und verständlichen Form definiert, dokumentiert und bekannt gegeben.
3. Verfahren werden verbessert, wenn Mängel in ihrer Umsetzung, Angemessenheit und Effektivität erkannt werden.
4. Umsetzung, Angemessenheit und Effektivität werden jährlich bei einem Drittel der Verfahren überprüft. Die zu überprüfenden Verfahren werden nach dem Zufallsprinzip ausgewählt. Wenn die jährliche Überprüfung ergibt, dass mehr als die Hälfte der überprüften Verfahren mängelbehaftet ist, werden alle Verfahren überprüft.

A.2 Risikoanalyse und -behandlung

Das Unternehmen MUSS die in diesen Richtlinien geforderten Risikoanalysen durchführen und erkannte Risiken zeitnah und angemessen behandeln.

Dies SOLLTE im Rahmen eines Risikomanagements auf Basis eines anerkannten Standards wie BSI-Standard 100-3, ISO/IEC 27005 oder ISO 31000 erfolgen.

Wenn eine andere Vorgehensweise gewählt wird, so MUSS hierfür ein Verfahren (siehe Anhang A 1) implementiert werden, das die Anforderungen folgender Abschnitte erfüllt.

A.2.1 Risikoanalyse

Eine Risikoanalyse MUSS folgende Anforderungen erfüllen:

1. Die Dokumentation beinhaltet das Vorgehen für das Identifizieren und Bewerten von Risiken.
2. Die Vorgehensweise gewährleistet, dass Bedrohungen und Schwachstellen zuverlässig erkannt werden können.
3. Die Bewertung von Risiken erfolgt auf Basis der potentiellen Schäden für das Unternehmen und deren Eintrittswahrscheinlichkeit.
4. Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.

A.2.2 Risikobehandlung

Identifizierte Risiken MÜSSEN zeitnah und priorisiert behandelt werden, indem geeignete Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken (z. B. durch den Abschluss einer Versicherung) definiert, dokumentiert und umgesetzt werden.

Die Umsetzung MUSS kontrolliert und auf Wirksamkeit geprüft werden.

Wenn Risiken nicht angemessen behandelt werden können, MÜSSEN sie vom Topmanagement akzeptiert und dies dokumentiert werden.

A.2.3 Wiederholung und Anpassung

Risikoanalysen MÜSSEN jährlich auf ihre Aktualität geprüft und bei Bedarf wiederholt werden.

Risikoanalysen MÜSSEN darüber hinaus zeitnah überarbeitet werden, wenn eine der folgenden Bedingungen auftritt:

1. Der Gegenstand der Risikoanalyse hat sich wesentlich verändert (z. B. die Hardware, die Software oder die Konfiguration eines IT-Systems).
2. Der Einsatzzweck des untersuchten Gegenstands hat sich wesentlich geändert.
3. Die Gefährdungslage hat sich erhöht (z. B. wenn eine neue Gefährdung bekannt wurde oder eine bestehende Gefährdung sich wesentlich erhöht hat).