Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

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 Informationsverarbeitung

Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

Inhalt

1 Allgemeines

Für die Abwehr „klassischer" Gefahren stehen etablierte Schutz-Standards, insbesondere die Richtlinien der VdS Schadenverhütung GmbH, zur Verfügung. 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.

Die vorliegenden Richtlinien legen Mindestanforderungen an die Informationssicherheit fest und beschreiben ein auf kleine und mittlere Unternehmen (KMU) zugeschnittenes Informationssicherheitsmanagementsystem (ISMS).

1.1 Anwendungshinweise

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

Die Umsetzung der geforderten Maßnahmen bedingt Fachwissen und Erfahrung auf den Gebieten der Informationssicherheit und der Managementsysteme. Sind diese Kenntnisse nicht in ausreichendem Maß vorhanden, empfiehlt sich die Inanspruchnahme qualifizierter Dienstleister, die ein Anerkennungsverfahren gemäß VdS 10003 durchlaufen haben.

Verpflichtende Maßnahmen sind durch die Schlüsselworte MUSS/MÜSSEN, DARF NICHT/DÜRFEN NICHT/DÜRFEN KEINE gekennzeichnet, empfohlene Maßnahmen durch die Schlüsselworte SOLLTE/SOLLTEN, SOLLTE NICHT/SOLLTEN NICHT, KANN/KÖNNEN, DARF/DÜRFEN.

Diese Richtlinien SOLLTEN in bestehende Managementsysteme integriert werden, um potentielle Synergieeffekte zu nutzen.

Insbesondere SOLLTEN sie zusammen mit den Richtlinien VdS 10010 „VdS-Richtlinien zur Umsetzung der DSGVO" und/oder den Richtlinien VdS 10020 „Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme" implementiert werden.

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.

1.2 Anwendungs- und Geltungsbereich

Diese Richtlinien sind für KMU, den gehobenen Mittelstand, Verwaltungen, Verbände und sonstige Organisationen anwendbar.

Die Richtlinien SOLLTEN auf die gesamte Organisation angewendet werden, ihr Geltungsbereich KANN jedoch technisch, geographisch und/oder organisatorisch eingegrenzt werden.

1.3 Gültigkeit

Diese Richtlinien gelten ab dem 01.12.2018 und ersetzen die Richtlinien VdS 3473 vom 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 100-4 Notfallmanagement

BSI-Standard 200-2 IT-Grundschutz-Vorgehensweise

BSI-Standard 200-3 Risikomanagement

DIN EN 1047-1 Wertbehältnisse – Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Teil 1: Datensicherungsschränke und Disketteneinsätze

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

DIN VDE 0100 Normenreihe zum Errichten von Niederspannungsanlagen

ISO 31000 Risk Management – Principles and guidelines

ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements

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

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

3 Begriffe

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: Person, die für Einrichtung, Betrieb, Überwachung und/oder Wartung eines IT-Systems oder Netzwerks zuständig ist.

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.

Archivierung: Entfernen aus der operativen Umgebung und Langzeitspeicherung bis zum Erreichen der Aufbewahrungsfrist.

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

Ausfall: Erliegen eines Prozesses, weil notwendige Ressourcen nicht in ausreichender Menge und/oder in ausreichender Qualität zur Verfügung stehen.

Authentizität: Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.

Authentifizierungsmerkmal: Merkmal, mit dessen Hilfe eine 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: Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

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.

Echtzeitbetrieb: Elektronische Datenverarbeitung, die (nahezu) simultan mit den entsprechenden Prozessen in der Realität abläuft.

Externer: Natürliche Person, die kein Mitarbeiter ist. Externe sind z. B. Geschäftspartner oder Gäste.

Funktion: Bündel von Aufgaben, durch die ein Teil der Ziele der Organisation erreicht werden soll.

Gefahr: Möglichkeit einer Schadwirkung auf ein zu schützendes Objekt.

Gefährdung: Bedrohung, die konkret über eine Schwachstelle auf ein zu schützendes Objekt einwirkt (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 gemäß Abschnitt 4.3 wahrnimmt.

Informationssicherheitsteam (IST): Gremium, das die Aufgaben gemäß 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.

Inventarisierung: Bestandsaufnahme zu einem definierten Zeitpunkt.

IS-Leitlinie: Leitlinie zur Informationssicherheit, die die Anforderungen gemäß Kapitel 5 erfüllt.

IS-Richtlinie: Sammlung von Regelungen zur Informationssicherheit, die die Anforderungen gemäß Kapitel 6 erfüllt.

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, Datenträger, Verbindungen, Daten, Informationen sowie Mitarbeiter.

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

IT-Outsourcing: Auslagerung von IT-Aufgaben an einen von der Organisation rechtlich unabhängigen Anbieter.

IT-System: Technische Anlage, die der Informationsverarbeitung dient und eine abgeschlossene Funktionseinheit aus Hard- und Software bildet. Typische IT-Systeme sind z. B. Server (physisch und virtuell), 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 Prozesse: Zentrale Prozesse der Organisation werden zum Erliegen gebracht und die Rückkehr zum Regelbetrieb ist (innerhalb eines akzeptablen Zeitraums) nicht möglich.
3. Auswirkung auf zentrale Werte: Zentrale Werte der Organisation gehen verloren oder werden zerstört und ihre Wiederherstellung ist (mit den Ressourcen der Organisation) nicht mehr möglich.
4. Auswirkungen auf die Rechtskonformität: Gesetze, Verträge oder Normen werden gebrochen und die daraus resultierende Haftung ist für die Organisation oder für die Verantwortlichen ruinös.

Kritische Individualsoftware: Software, die für den Betrieb von kritischen IT-Systemen zwingend benötigt wird und individuell für die Organisation erstellt oder angepasst wurde.

Kritische Informationen: Informationen, die die Bedingungen gemäß Abschnitt 9.2 erfüllen.

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

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

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

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

Maximal tolerierbare Ausfallzeit (MTA): Zeit, bis zu der eine definierte Leistung (z. B. ein Notbetriebsniveau) wieder verfügbar sein muss.

Maximal tolerierbarer Datenverlust (MTD): Zeitspanne, die als noch akzeptierbar für einen Datenverlust erachtet wird.

Mitarbeiter: Natürliche Person, die in einem Vertragsverhältnis oder in einem öffentlich-rechtlichen Dienst- und Treueverhältnis mit der Organisation steht und eine oder mehrere Positionen in der Organisation einnimmt. Mitarbeiter sind z. B. Angestellte, Arbeiter, Beamte, freier Mitarbeiter, Dienstleister oder deren Mitarbeiter bzw. Erfüllungsgehilfen.

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 Anlage, die der Weiterleitung von Daten dient. 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.

Notbetrieb: Auf ein Minimum reduzierte Funktionstüchtigkeit, mit der ein Prozess aufrechterhalten werden kann.

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

Organisationseinheit: Einheit, in der artverwandte (Teil-)Aufgaben oder Tätigkeiten zusammengefasst sind.

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

Position: Platz, den ein Mitarbeiter in der Hierarchie einer Organisation einnimmt.

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

Prozess: System von Tätigkeiten, das Eingaben mit Hilfe von Ressourcen 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 Prozesse verantwortlich ist. Sie besitzt den Überblick über die für diese Prozesse benötigten Ressourcen und über die an sie gestellten Anforderungen.

Regelung: Verbindliche Vorgabe.

Ressource: Betriebsmittel, das der Organisation gehört oder ihr zur Verfügung steht.

Risiko: Eine nach Eintrittswahrscheinlichkeit und Schadenshöhe bewertete Gefährdung.

Schnittstelle: Teil eines IT-Systems, das der Kommunikation dient, wie z. B. Ethernet- und Wireless-LAN-Adapter, 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/oder infrastrukturelle Netzdienste realisiert werden.

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

Speicherort: Ort, an dem Nutzer bzw. Applikationen ihre Daten speichern.

Störung: Situation, in der Prozesse oder Ressourcen 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: Eine Ressource kann wie vorgesehen genutzt werden.

Vertraulichkeit: Eigenschaft einer Information, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

Zentraler Prozess: Prozess, der mitentscheidend für die Aufgabenerfüllung der Organisation 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, die nichtöffentliche IT der Organisation zu nutzen.

Zugriff: Datenaustausch zwischen einer zugreifenden Instanz und einer IT-Ressource.

Zutritt: Umstand, der es ermöglicht, physisch mit einer IT-Ressource zu interagieren.

4 Organisation der Informationssicherheit

Um mit möglichst geringem Aufwand das notwendige Sicherheitsniveau zu definieren, umzusetzen und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage anzupassen, ist es notwendig, eine entsprechende Organisation zu etablieren.

4.1 Verantwortlichkeiten

Verantwortlichkeiten (siehe Abschnitte 4.2 bis 4.10) MÜSSEN eindeutig und widerspruchsfrei zugewiesen werden.

4.1.1 Zuweisung und Dokumentation

Es MUSS für jede Verantwortlichkeit 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 MUSS das Prinzip der Funktionstrennung umgesetzt werden. Widersprüchliche Verantwortlichkeiten DÜRFEN NICHT von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

Wenn eine Funktionstrennung nicht oder nur mit einem unverhältnismäßig hohen Aufwand durchführbar ist, KÖNNEN widersprüchliche Verantwortlichkeiten von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

In diesem Fall MÜSSEN folgende Anforderungen erfüllt werden:

1. Die rechtliche Zulässigkeit wurde geprüft.
2. Es werden andere Maßnahmen wie Überwachung von Tätigkeiten, Kontrollen oder Leitungsaufsicht umgesetzt.
3. Die nicht durchgeführte Funktionstrennung wird in der Dokumentation der Funktionsverteilung (siehe Abschnitt 4.1.1) besonders hervorgehoben und begründet.

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

4.1.3 Zeitliche Ressourcen

Um zugewiesene Verantwortlichkeiten wahrzunehmen, MÜSSEN die entsprechenden Mitarbeiter im erforderlichen Umfang (siehe Abschnitt 4.1.1) von anderen Tätigkeiten freigestellt werden.

4.1.4 Delegieren von Aufgaben

Verantwortliche für Informationssicherheit KÖNNEN Aufgaben an andere Personen delegieren.

Die Verantwortung für delegierte Aufgaben verbleibt 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. In Kraft setzen von Richtlinien für die Informationssicherheit (IS-Richtlinien)
3. Bereitstellen der notwendigen technischen, finanziellen und personellen Ressourcen für die Informationssicherheit
4. Einbetten der Informationssicherheit in die Strukturen, Hierarchien und Arbeitsabläufe der Organisation

4.3 Informationssicherheitsbeauftragter (ISB)

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

Dieser MUSS darauf hinwirken, dass die in der Leitlinie zur Informationssicherheit (IS-Leitlinie) definierten Ziele der Informationssicherheit erreicht werden.

Hierfür MUSS er insbesondere die folgenden Verantwortlichkeiten wahrnehmen:

1. Steuern, Koordinieren und Prüfen der technischen und organisatorischen Maßnahmen, kontinuierliches Verbessern der Informationssicherheit, insbesondere Anpassen der Informationssicherheit an neue Bedrohungen, Änderungen im technischen und organisatorischen Umfeld und an neue gesetzliche, betriebliche und vertragliche Anforderungen
2. jährliches Berichten an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit, insbesondere über Mängel, Risiken und Sicherheitsvorfälle

Es SOLLTE sichergestellt werden, dass die Verantwortlichkeiten des ISB auch in seiner Abwesenheit wahrgenommen werden.

Dies KANN z. B. durch eine Stellvertreterregelung umgesetzt werden.

4.4 Informationssicherheitsteam (IST)

Das Topmanagement MUSS ein Informationssicherheitsteam (IST) bestellen.

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

1. Topmanagement
2. ISB
3. IT-Verantwortliche

4. Mitarbeiter (z. B. über Betriebsrat)
5. Verantwortliche für den Datenschutz (z. B. Datenschutzmanager und/oder Datenschutzbeauftragter)

Das Team MUSS den ISB unterstützen, insbesondere bei den folgenden Tätigkeiten:

1. Erkennen und Bewerten neuer Bedrohungen und Schwachstellen
2. Entwickeln und Bewerten von Maßnahmen zur Informationssicherheit
3. organisationsweites Steuern und Koordinieren der Maßnahmen zur Informationssicherheit

4.5 IT-Verantwortliche

Die Aufgaben eines IT-Verantwortlichen MÜSSEN vom Topmanagement mindestens 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 in Abstimmung mit dem IT-Verantwortlichen die technischen Maßnahmen für die Informationssicherheit implementieren.

4.7 Vorgesetzte

Vorgesetzte, die Verantwortung für Mitarbeiter tragen, MÜSSEN sicherstellen, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeiter umgesetzt werden.

4.8 Mitarbeiter

Mitarbeiter MÜSSEN folgende Aufgaben wahrnehmen:

1. Einhalten und Umsetzen aller sie oder ihre Tätigkeit betreffenden Maßnahmen zur Informationssicherheit
2. Melden von Störungen, Ausfällen und Sicherheitsvorfällen

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 Externe

Externe MÜSSEN verpflichtet werden, die sie betreffenden Maßnahmen und Regelungen zur Informationssicherheit einzuhalten bzw. umzusetzen, sofern sie Zugriff auf kritische Informationen besitzen oder sie nichtöffentliche Bereiche der Informationstechnologie (IT) der Organisation nutzen.

5 Leitlinie zur Informationssicherheit (IS-Leitlinie)

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

5.1 Allgemeine Anforderungen

Die Leitlinie MUSS vom Topmanagement erstellt und in Kraft gesetzt werden.

Das Topmanagement MUSS die Leitlinie jährlich auf Aktualität prüfen und bei Bedarf aktualisieren.

Die Leitlinie MUSS nach jeder Aktualisierung zeitnah bekannt gegeben werden und in der jeweils aktuellen Form allen Betroffenen zur Verfügung stehen.

5.2 Inhalte

Die Leitlinie MUSS folgende Anforderungen erfüllen:

1. Sie definiert die Ziele und den Stellenwert der Informationssicherheit in der Organisation.
2. Sie definiert sämtliche erforderlichen Positionen (siehe Abschnitte 4.2 bis 4.10) und weist auf deren Aufgaben hin.

Die Leitlinie SOLLTE auf die Konsequenzen ihrer Nichtbeachtung hinweisen.

6 Richtlinien zur Informationssicherheit (IS-Richtlinien)

Zur Unterstützung und Konkretisierung der IS-Leitlinie ist es notwendig, weitere Regelungen 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. aktualisieren.

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 umgesetzt oder vom Topmanagement aufgehoben werden.

6.2 Inhalte

Jede IS-Richtlinie MUSS folgende Anforderungen erfüllen:

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

IS-Richtlinien KÖNNEN begründete Ausnahmen ermöglichen, sofern diese im Vorfeld genehmigt und dokumentiert werden.

IS-Richtlinien KÖNNEN auf weitere mitgeltende Unterlagen verweisen.

6.3 Regelungen für Nutzer

Es MÜSSEN Regelungen für den Umgang mit der IT getroffen werden, die in ihrer Gesamtheit für alle Nutzer (inkl. aller Führungsebenen) sowie für die gesamte IT verbindlich sind:

1. Generelle Nutzungsbedingungen
    a. Das unrechtmäßige Abrufen oder Verbreiten von urheberrechtlich geschützten Inhalten 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 der Organisation ausgestaltet.
3. Grundlegende Verhaltensregeln
    a. Es wird nur freigegebene Hard- und Software in der IT-Infrastruktur installiert, genutzt oder betrieben.
    b. Es wird untersagt, eigenmächtig Netzübergänge (wie z. B. Zugänge zum Internet, Fernwartungszugänge oder VPN-Verbindungen) zu installieren; es werden ausschließlich die von der Organisation bereitgestellten Netzübergänge genutzt.
    c. Die in der IT-Infrastruktur installierten Sicherheitseinrichtungen werden nicht eigenmächtig deinstalliert, deaktiviert oder in ihrer Konfiguration verändert bzw. mutwillig umgangen.
    d. Authentifizierungsmerkmale werden nicht weitergegeben.
4. Umgang mit den Informationen der Organisation
    a. Informationen der Organisation werden nicht eigenmächtig verschlüsselt oder vor lesendem Zugriff geschützt; hierfür werden die von der Organisation explizit freigegebenen technischen Verfahren genutzt.
5. 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.

6. Missbrauchskontrolle

   a. Es werden Mechanismen zur Missbrauchskontrolle definiert und den Betroffenen mitgeteilt.

Bei der Umsetzung von Überwachungs- und Protokollierungsmaßnahmen SOLLTEN die gesetzlichen Vorgaben, insbesondere die des Datenschutzes, beachtet werden.

Ausnahmen MÜSSEN vom ISB genehmigt werden.

6.4 Weitere Regelungen

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

1. Mobile IT-Systeme (siehe Abschnitt 10.4)
2. Mobile Datenträger (siehe Abschnitt 12.1)
3. IT-Outsourcing und Cloud Computing (siehe Abschnitt 14.1)
4. Datensicherung (siehe Abschnitt 16.1)
5. Störungen und Ausfälle (siehe Abschnitt 17.1)
6. Sicherheitsvorfälle (siehe Abschnitt 18.1)

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

7 Mitarbeiter

Die Mitarbeiter sind ein zentraler Faktor für die Implementierung und Aufrechterhaltung der Informationssicherheit. Es ist deshalb notwendig, folgende Anforderungen der Informationssicherheit zu berücksichtigen.

7.1 Vor Aufnahme der Tätigkeit

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

7.2 Aufnahme der Tätigkeit

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das im Zuge der Aufnahme der Tätigkeit eines Mitarbeiters folgende Punkte sicherstellt:

1. Mitarbeiter verpflichten sich mittels einer schriftlichen Erklärung zur Vertraulichkeit; die Erklärung definiert auch die Pflichten in Bezug auf Informationssicherheit, die nach Beendigung oder Veränderung des Arbeitsverhältnisses fortbestehen.
2. Mitarbeiter werden in die IS-Leitlinie und in sämtliche für sie relevante Regelungen zur Informationssicherheit (wie z. B. in die Inhalte entsprechender Richtlinien und Verfahren) eingewiesen.

3. Mitarbeiter werden im Umgang mit den für sie relevanten Sicherheitsmaßnahmen geschult (siehe Abschnitt 8.2).
4. Mitarbeiter erhalten die benötigten IT-Ressourcen, Zugänge und Zugriffsrechte und werden in deren Nutzung geschult.

7.3 Beendigung oder Wechsel der Tätigkeit

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das bei Beendigung oder Wechsel der Tätigkeit eines Mitarbeiters folgende Punkte sicherstellt:

1. Soweit erforderlich, werden Mitarbeiter, Kunden sowie relevante externe Stellen über die Änderungen informiert.
2. Die zur Verfügung gestellten IT-Ressourcen, Zugänge und Zugriffsrechte 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 die Organisation über aktuelles Wissen in Bezug auf Informationssicherheit verfügt, die Mitarbeiter ihre Verantwortlichkeiten verstehen und für ihre Aufgaben geeignet und qualifiziert sind.

8.1 Aktualität des Wissens

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, mit dem alle relevanten Stellen der Organisation 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 relevante 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 Schulung und Sensibilisierung

Es MUSS ein Verfahren (siehe Anhang A 1) für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden, das folgende Punkte sicherstellt:

1. Sie werden regelmäßig sowie bei Bedarf durchgeführt.
2. Ihre Art und ihr Intervall werden zielgruppenorientiert festgelegt.
3. Sie vermitteln in ihrer Gesamtheit die Inhalte der IS-Leitlinie und sämtlicher für die Zielgruppe relevanter Regelungen zur Informationssicherheit (wie z. B. die Inhalte entsprechender IS-Richtlinien und Verfahren).

4. Sie klären über Gefährdungen auf und schulen den Umgang mit den vorhandenen Sicherheitsmaßnahmen sowie das Verhalten bei Störungen, Ausfällen und Sicherheitsvorfällen.
5. Sie vermitteln den Teilnehmern ihre Verantwortung für die Informationssicherheit und fördern bei ihnen die Akzeptanz der Sicherheitsmaßnahmen.
6. Ihre Inhalte und die Teilnahme an ihnen werden dokumentiert.

Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN mit einer Lernerfolgskontrolle abschließen, um das Verständnis der Teilnehmer und den Bedarf weiterer Schulungs- oder Sensibilisierungsmaßnahmen zu ermitteln.

Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN von den Teilnehmern bewertet werden, um ihren Inhalt, ihre Form und ihren Ablauf zu verbessern.

9 Identifizieren kritischer IT-Ressourcen

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

Die Organisation SOLLTE deshalb eine Informationsklassifizierung auf Basis eines anerkannten Standards wie ISO/IEC 27001 oder eine Schutzbedarfsanalyse gemäß BSI-Standard 200-2 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

Die Organisation MUSS ihre zentralen Prozesse und ihre 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 die maximal tolerierbare Ausfallzeit (MTA) des Prozesses.

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

9.2 Informationen

Die Organisation MUSS ermitteln, ob sie kritische Informationen verarbeitet, überträgt und/oder speichert und diese dokumentieren.

Kritische Informationen sind Informationen, bei denen folgende Faktoren zu katastrophalen Schäden führen können:

1. unberechtigte Einsicht, Kenntnisnahme oder Weitergabe (Kriterium „Vertraulichkeit“)
2. Verfälschung (Kriterium „Integrität“)

3. Datenverlust von weniger als 24 Stunden (Kriterium „Maximal tolerierbarer Datenverlust – MTD“)
4. Nichtverfügbarkeit im Echtzeitbetrieb (Kriterium „Unmittelbare Verfügbarkeit“)

Hierfür MÜSSEN die zentralen Prozesse und die Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1) untersucht werden.

Die Dokumentation MUSS folgende Anforderungen erfüllen:

1. Sie enthält die Kriterien, anhand derer die Informationen als kritisch eingestuft wurden.

   Kritische Informationen SOLLTEN anhand ihrer qualitativen und quantitativen Merkmale beschrieben werden. Qualitative Merkmale definieren die Eigenschaften der kritischen Informationen. Quantitative Merkmale definieren, ab welcher Menge die Informationen mit den genannten Eigenschaften kritisch sind. Die Erfassung quantitativer und qualitativer Merkmale bietet die Möglichkeit, kritische Informationen zuverlässiger zu erfassen.

2. Sie begründet, warum die Informationen kritisch sind.

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

9.3 IT-Ressourcen

Die Organisation MUSS ihre kritischen IT-Ressourcen (insbesondere die kritischen IT-Systeme, mobilen Datenträger, Verbindungen sowie die kritische Individualsoftware) bestimmen und diese dokumentieren.

Kritische IT-Ressourcen sind IT-Ressourcen, die kritische Informationen (siehe Abschnitt 9.2) verarbeiten, speichern oder übertragen oder die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden.

Hierfür MÜSSEN die kritischen Informationen (siehe Abschnitt 9.2) untersucht werden.

Um IT-Ressourcen zu ermitteln, die kritische Informationen verarbeiten, speichern oder übertragen 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 verarbeitet, gespeichert und übertragen werden. Bei Bottom-Up hingegen werden die einzelnen Elemente der IT-Infrastruktur (insbesondere IT-Systeme, mobile Datenträger und Verbindungen) untersucht, ob sie kritische Informationen verarbeiten, speichern oder übertragen. Eine Mischung aus beiden Ansätzen bietet die Möglichkeit, die entsprechenden IT-Ressourcen zuverlässig zu identifizieren.

Um IT-Ressourcen zu ermitteln, die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden, KANN ebenfalls ein Top-Down-Ansatz, ein Bottom-Up-Ansatz oder eine Mischung aus beiden Ansätzen verwendet werden.

Die Dokumentation MUSS folgende Anforderungen erfüllen:

1. Sie enthält eine kurze Beschreibung der kritischen IT-Ressource.
2. Sie begründet, warum die IT-Ressource kritisch ist.
3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der IT-Ressource.

Die MTA MUSS ebenso kurz oder kürzer sein, als die kürzeste MTA aller zentralen Prozesse und Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1), die von der kritischen IT-Ressource direkt oder indirekt abhängig sind.

Bei der Bestimmung der MTA SOLLTEN Abhängigkeiten zwischen kritischen IT-Ressourcen berücksichtigt werden.

Die Aufstellung der kritischen IT-Ressourcen und deren Dokumentation MUSS vom IT-Verantwortlichen freigegeben werden.

10 IT-Systeme

Die Informationsverarbeitung einer Organisation 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 der Organisation verzeichnet sind.

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

In ihr MÜSSEN folgende Informationen für jedes IT-System verzeichnet sein:

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

Darüber hinaus SOLLTEN für jedes IT-System weitere Informationen erhoben und aktuell gehalten werden, wie z. B. Namen, Versionen und Lizenzinformationen der installierten System- und Anwendungssoftware, Seriennummern von Hardwarekomponenten sowie Informationen über Garantien und Serviceverträge.

Besonderheiten der Installation und Konfiguration SOLLTEN in einer Dokumentation verzeichnet sein.

10.2 Lebenszyklus

IT-Systeme bilden eine abgeschlossene Funktionseinheit aus Hard- und Software (siehe Abschnitt 10.3). Sie unterliegen einem Lebenszyklus, der sich üblicherweise von der Inbetriebnahme bis zu deren Ausmusterung erstreckt.

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. Der Basisschutz (siehe Abschnitt 10.3) wird umgesetzt.
3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.
4. Bei Inbetriebnahme werden die Arbeitsschritte dokumentiert.

10.2.2 Ausmusterung und Wiederverwendung

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

1. Die auf dem IT-System gespeicherten Informationen werden bei Bedarf gesichert bzw. archiviert.
2. 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.
3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.
4. Bei Ausmusterung werden die Arbeitsschritte dokumentiert.

10.3 Basisschutz

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

Wenn eine entsprechende Funktionalität nicht gegeben ist, SOLLTE dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet 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 Software

System- und Anwendungssoftware MUSS aus vertrauenswürdigen Quellen bezogen werden.

Es SOLLTE ausschließlich System- und Anwendungssoftware eingesetzt werden, die Sicherheitsupdates des Herstellers erhält.

Es SOLLTE nur Software auf IT-Systemen installiert werden, die zur Aufgabenerfüllung benötigt wird; nicht benötigte Software SOLLTE deinstalliert werden.

Sämtliche Zugriffsrechte und Privilegien der Anwendungssoftware SOLLTEN auf ein Mindestmaß reduziert werden.

Vom Hersteller zur Verfügung gestellte 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, Authentifizierungsmerkmale 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 oder die in weniger vertrauenswürdigen Umgebungen eingesetzt werden).

Zusätzlich SOLLTE der Netzwerkverkehr von und zu IT-Systemen, für die die Organisation keinen administrativen Zugang besitzt, auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden.

Die Beschränkung des Netzwerkverkehrs KANN bspw. durch eine geeignete Segmentierung des Netzwerks (siehe Abschnitt 11.4.2), lokale Filtermechanismen oder durch das Deaktivieren nicht benötigter Dienste erfolgen.

10.3.3 Protokollierung

Jedes IT-System MUSS erfolgreiche und erfolglose Anmeldeversuche, 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 die Aufgabenerfüllung 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 bei Zugriff auf Schadsoftware prüft.

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 in kurzen zeitlichen Abständen (z. B. stündlich oder 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 Zutrittsschutz umgesetzt werden.

10.3.7 Authentifizierung

Der Zugang zu allen nichtöffentlichen Bereichen 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. Interaktive Sitzungen werden beendet oder gesperrt, wenn der Nutzer innerhalb einer vorgegebenen Zeitspanne keine Eingaben tätigt.
3. 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. Standard-Passwörter oder einfach zu erratende Passwörter) verwendet.

Es SOLLTE Mehr-Faktor-Authentifizierung eingesetzt werden, um die Gefahr eines unberechtigten Zugangs zu verringern, insbesondere wenn Nutzer umfangreiche Zugriffsrechte besitzen.

10.3.8 Zugänge und Zugriffe

Es MUSS sichergestellt werden, dass Nutzer keine administrativen Arbeiten durchführen können.

Dies KANN mit Hilfe getrennter Zugänge und geeigneter Zugriffsrechte umgesetzt werden.

Darüber hinaus SOLLTEN folgende Anforderungen erfüllt werden:

1. *Nutzer können nur auf Informationen lesend zugreifen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist („Need-to-Know“).*
2. *Nutzer können nur auf Informationen schreibend zugreifen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist („Least-Privileges“).*

10.4 Zusätzliche Maßnahmen für mobile IT-Systeme

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

Folgende Maßnahmen MÜSSEN für alle mobilen IT-Systeme umgesetzt werden.

10.4.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit mobilen IT-Systemen getroffen werden:

1. Es wird festgelegt, welche Informationen 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 der Organisation 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 MÜSSEN Verfahren (siehe Anhang A 1) implementiert werden, die festlegen, wie Nutzer und Administratoren bei Verlust eines mobilen IT-Systems vorzugehen haben.

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

Die Verfahren MÜSSEN sicherstellen, dass die auf dem Gerät hinterlegten Zugänge der Organisation 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 zusätzlich 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.

10.5.4 Externe Schnittstellen und Laufwerke

Externe Schnittstellen und Laufwerke, die nicht für die Aufgabenerfüllung 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 seiner MTA wiederhergestellt werden kann, sofern keine Ersatzsysteme oder -verfahren verfügbar sind (siehe Abschnitt 10.5.9).

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 Zugang zum 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 Abschnitt 16.6) 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 die Organisation über ein Ersatzsystem oder -verfahren verfügen, das es ermöglicht, die vom kritischen IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenspotential weiter zu betreiben.

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

10.5.10 Kritische Individualsoftware

Die Organisation MUSS durch vertragliche und/oder organisatorische Regelungen sicherstellen, dass sie kritische Individualsoftware auch in Zukunft verwenden und ihren Bedürfnissen anpassen kann.

11 Netzwerke und Verbindungen

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

11.1 Netzwerkplan

Die Netzwerke der Organisation MÜSSEN so erfasst sein, dass fachlich versierte Personen folgende Punkte nachvollziehen können:

1. physikalische Netzwerkstruktur
   a. aktive Netzwerkkomponenten und deren Verbindungen untereinander
   b. physikalisches Medium der Verbindungen
2. logische Netzwerkstruktur
   a. Netzwerksegmente (siehe Abschnitt 11.4.2), deren Einsatzzweck und deren Verbindungen untereinander
   b. Fernzugänge (siehe Abschnitt 11.4.3)
   c. Netzwerkkopplungen (siehe Abschnitt 11.4.4)
   d. Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken (siehe Abschnitt 11.3)

11.2 Aktive Netzwerkkomponenten

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

11.3 Netzübergänge

Folgende Maßnahmen MÜSSEN für alle Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken umgesetzt werden:

1. Der Netzwerkverkehr wird auf das für die Funktionsfähigkeit notwendige Minimum beschränkt.

2. Der Inhalt erlaubter Verbindungen wird auf Schadsoftware und Angriffe untersucht; erkannte Schadsoftware und Angriffe werden blockiert.
3. Hinweise auf Schadsoftware in der IT-Infrastruktur der Organisation und Angriffe aus der IT-Infrastruktur der Organisation heraus werden als Sicherheitsvorfall (siehe Kapitel 18) behandelt.

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

Weitere Sicherheitsmaßnahmen SOLLTEN im Zuge einer Risikoanalyse und -behandlung (siehe Anhang A 2) ermittelt und umgesetzt 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 eine entsprechende Funktionalität nicht gegeben ist, SOLLTE dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet 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 Zutrittsbeschränkung, eine Deaktivierung der Netzwerkanschlüsse oder durch eine Netzwerkzugangskontrolle geschehen.

11.4.2 Segmentierung

Die Notwendigkeit einer Segmentierung der Netzwerke der Organisation 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 Fernzugang

Der Zugang zu nichtöffentlichen Bereichen von IT-Systemen der Organisation über weniger oder nicht vertrauenswürdige Netzwerke MUSS abgesichert werden.

Dabei MÜSSEN folgende Anforderungen erfüllt werden:

1. Die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen wird geschützt.
2. Der Zugang 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 Zugang wird so gestaltet, dass der Nutzer und das zugreifende IT-System authentifiziert werden und sichergestellt ist, dass das IT-System grundlegende Sicherheitsanforderungen erfüllt oder der Zugang erfolgt über eine Remote-Desktop-Verbindung, die sicherstellt, dass Informationen 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 Zugangs zu verringern.*

11.4.4 Netzwerkkopplung

Die Kopplung von Netzwerken der Organisation 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

Für alle kritischen Verbindungen, MUSS 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 zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit mobilen Datenträgern getroffen werden:

1. Es wird festgelegt, welche Informationen der Organisation 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. Mobile Datenträger, auf denen Daten der Organisation gespeichert sind, werden grundsätzlich vertraulich behandelt; sie werden nicht an unberechtigte Dritte weitergegeben oder verliehen und nicht für andere Personen zugänglich aufbewahrt.

12.2 Schutz der Informationen

Die auf den mobilen Datenträgern gespeicherten Informationen der Organisation SOLLTEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

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

12.3 Zusätzliche Maßnahmen für kritische mobile Datenträger

Für alle kritischen mobilen Datenträger MUSS eine Risikoanalyse und -behandlung (siehe Anhang A 2) etabliert werden.

13 Umgebung

Die Organisation MUSS ihre 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 Anforderungen folgender Abschnitte erfüllt.

13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen

Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen (z. B. Patchfelder) MÜSSEN vor Beschädigung und unberechtigtem Zutritt geschützt werden.

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

Insbesondere SOLLTEN folgende Bedrohungen bewertet und behandelt werden:

1. *ungeeignete Umgebungsbedingungen (wie z. B. ungeeignete Temperatur oder Luftfeuchtigkeit, Staub oder Rauch)*
2. *negative Umwelteinflüsse (wie z. B. Feuer, Wasser, Blitzschlag)*
3. *unzuverlässige Stromversorgung (wie z. B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)*

   Fest installierte Niederspannungsanlagen SOLLTEN gemäß gängiger Normen und Standards wie z. B. der DIN VDE 0100-Reihe errichtet sein.
4. *Beschädigung und Verlust (wie z. B. Löschmittel, Vandalismus, Diebstahl)*

13.2 Datenleitungen

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

Wenn eine andere Vorgehensweise gewählt wird, MÜSSEN fest installierte Datenleitungen durch entsprechende bauliche Maßnahmen vor Beschädigung geschützt werden.

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

13.3 Zusätzliche Maßnahmen für kritische IT-Systeme

Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.5.1) MÜSSEN für alle kritischen IT-Systeme folgende Bedrohungen behandelt werden:

1. ungeeignete Umgebungsbedingungen (wie z. B. ungeeignete Temperatur oder Luftfeuchtigkeit, Staub oder Rauch)
2. negative Umwelteinflüsse (wie z. B. Feuer, Wasser, Blitzschlag)
3. unzuverlässige Stromversorgung (wie z. B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)
4. Beschädigung und Verlust (wie z. B. Löschmittel, Vandalismus, Diebstahl)
5. unautorisierter Zutritt
6. Ausspähen vertraulicher Informationen

Insbesondere SOLLTE geprüft werden, kritische IT-Systeme in zusätzlich abgesicherten Gebäuden oder Gebäudeteilen unterzubringen (Sicherheitszonen).

14 IT-Outsourcing und Cloud Computing

Wenn IT-Ressourcen ausgelagert werden, ist es notwendig, dass die Sicherheitsinteressen der Organisation berücksichtigt werden.

14.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.2 MÜSSEN in einer IS-Richtlinie die Bedingungen, unter welchen IT-Ressourcen ausgelagert werden dürfen, festgelegt werden.

14.2 Vorbereitung

Für Jedes Vorhaben, das zur Auslagerung von IT-Ressourcen führt, MÜSSEN folgende Punkte 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 die Organisation 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.

14.3 Vertragsgestaltung

Wenn IT-Ressourcen ausgelagert werden sollen, so MUSS mit dem Anbieter ein Vertrag geschlossen werden, der die Anforderungen aus Abschnitt 14.2 enthält und den Anbieter zu deren Erfüllung verpflichtet.

Darüber hinaus SOLLTEN folgende Punkte sichergestellt sein:

1. *Ansprüche aus Vertragsverletzungen können durchgesetzt werden, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie die Organisation befindet.*
2. *Die Mitwirkungspflichten des Anbieters im Falle einer Vertragsauflösung oder Insolvenz sind vereinbart, insbesondere die vollständige Herausgabe der IT-Ressourcen der Organisation sowie die aktive Unterstützung des Migrationsprozesses durch den Anbieter.*

14.4 Zusätzliche Maßnahmen für kritische IT-Ressourcen

Wenn kritische IT-Ressourcen ausgelagert werden, MÜSSEN die Anforderungen aus Abschnitt 14.2 an ihre Vertraulichkeit, Verfügbarkeit und Integrität im Rahmen einer Risikoanalyse (siehe Anhang A 2.1) ermittelt und folgende Punkte vertraglich geregelt werden:

1. Leistungen
   a. Die vom Anbieter zu erbringenden Leistungen werden definiert und 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 der Organisation und den ausgelagerten IT-Ressourcen wird definiert.

   Es SOLLTEN Konsequenzen bei Nichteinhaltung der vertraglich vereinbarten Leistungen vereinbart werden.

2. Kommunikation
   a. Die Ansprechpartner auf Seiten der Organisation 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 der Organisation 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.

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

15 Zugänge und Zugriffsrechte

Zugänge und Zugriffsrechte erlauben es, auf die nichtöffentliche IT der Organisation und ihre 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 Zugriffsrechten 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 der Organisation 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 oder Zugriffsrechte entzogen werden, KANN auf das Informieren des Nutzers verzichtet 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 Informationen

Alle Zugänge zu kritischen IT-Systemen sowie sämtliche Zugriffsrechte auf kritische Informationen 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 200-2 unter Berücksichtigung der IT-Grundschutz-Kataloge des BSI implementiert werden.

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

16.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie die Speicherorte für die Daten der Organisation festgelegt werden.

16.2 Archivierung

Die Organisation 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 die folgenden Punkte sicherstellen:

1. Die gesicherten Daten werden bei Übertragung, Lagerung und Transport vor Änderungen, Beschädigung, Verlust und unberechtigter Einsichtnahme geschützt.

   Der Schutz der Vertraulichkeit KANN z. B. durch eine Verschlüsselung der Daten oder der Sicherungsmedien erreicht werden.

2. Die gesicherten Daten werden nicht im gleichen Brandabschnitt wie die gesicherten IT-Systeme aufbewahrt.

   Ein eigener Brandabschnitt KANN durch geeignete Datensicherungsschränke umgesetzt werden. In Bereichen mit Brandmeldesystemen SOLLTEN Datensicherungsschränke nach DIN EN 1047-1, Ausführung S 60 DIS, und in Bereichen ohne Brandmeldesysteme nach DIN EN 1047-1, Ausführung S 120 DIS zertifiziert sein.

3. Die Datensicherung und -wiederherstellung wird jährlich oder bei einer Änderung des Verfahrens getestet, indem ein betroffenes IT-System nach dem Zufallsprinzip ausgewählt, gesichert und in einer Testumgebung wiederhergestellt wird.

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

4. Die Durchführung und die Ergebnisse der Tests werden dokumentiert.

Die Verfahren SOLLTEN darüber hinaus die folgenden Punkte sicherstellen:

1. *Einzelne Datensicherungen werden in festen zeitlichen Abständen (z. B. wöchentlich) an einen entfernten Standort ausgelagert, damit die gesicherten Daten auch bei größeren Schadensereignissen verfügbar bleiben.*
2. *Die Datensicherung wird nach dem Mehr-Generationen-Prinzip durchgeführt, um die Wahrscheinlichkeit eines umfangreichen Datenverlusts weiter zu verringern.*

16.4 Weiterentwicklung

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

Notwendige Anpassungen MÜSSEN zeitnah implementiert 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 eine entsprechende Funktionalität nicht gegeben ist, SOLLTE dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet 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, Anwendungs-, Logdaten, usw.) nicht älter als 24 Stunden ist.

16.5.3 Aktive Netzwerkkomponenten

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

16.5.4 Mobile IT-Systeme

Es MUSS eine Vorgehensweise für die Datensicherung von einem Administrator vorgegeben werden.

16.6 Zusätzliche Maßnahmen für kritische IT-Systeme

Jedes kritische IT-System MUSS über eine Datensicherung verfügen, die in Ergänzung zu Abschnitt 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 MTD bestimmt werden.

16.6.2 Verfahren

Die Verfahren zur Datensicherung und -wiederherstellung MÜSSEN in Ergänzung zu Abschnitt 16.3 folgende Punkte sicherstellen:

1. Kritische IT-Systeme werden vollständig gesichert (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.).
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).

17 Störungen und Ausfälle

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

Zu diesem Zweck SOLLTE die Organisation ein Business Continuity Management (BCM) auf Basis eines anerkannten Standards wie BSI-Standard 100-4 oder DIN EN ISO 22301 implementieren.

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

17.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit Störungen und Ausfällen getroffen werden:

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 die Organisation 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 zeitnah 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 der Regelbetrieb wieder aufgenommen.
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden.

Bei geringfügigen Störungen oder Ausfällen KÖNNEN einzelne Punkte ausgelassen und/oder das Verfahren vorzeitig beendet werden.

17.3 Zusätzliche Maßnahmen für kritische IT-Systeme

Folgende Maßnahmen MÜSSEN zusätzlich für alle kritischen IT-Systeme umgesetzt werden.

17.3.1 Wiederanlaufpläne

Für jedes kritische IT-System MUSS ein Verfahren (siehe Anhang A 1) für den Wiederanlauf implementiert werden (Wiederanlaufplan), das 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 wiederherzustellen, dass zumindest das Notbetriebsniveau (siehe Abschnitt 10.5.2) erreicht ist.
2. Wenn das IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, enthält der Wiederanlaufplan alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, die entsprechenden Ersatzsysteme oder -verfahren (siehe Abschnitt 10.5.9) soweit in Betrieb zu nehmen, dass die vom IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenspotential betrieben werden können.
3. Er enthält eine Aufstellung der für die Wiederherstellung zwingend benötigten Ressourcen, wie z. B. Mitarbeiter und deren Kontaktdaten, Hardware, Software, Netzwerke, Dienste und Authentifizierungsmerkmale.
4. Er ist verständlich und übersichtlich strukturiert.
5. Er ist im Bedarfsfall schnell verfügbar.
6. 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.

Darüber hinaus SOLLTEN die Abhängigkeiten der kritischen IT-Systeme von sämtlichen kritischen IT-Ressourcen dokumentiert und dabei die Notwendigkeit weiterer Wiederanlaufpläne geprüft 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 ist im Bedarfsfall schnell verfügbar.
4. Sie wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.

18 Sicherheitsvorfälle

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

18.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit Sicherheitsvorfällen getroffen werden:

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 die Organisation intern und nach außen über akute und bewältigte Sicherheitsvorfälle kommuniziert.

18.2 Erkennen

Es SOLLTEN Maßnahmen implementiert werden, 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*

Das Melden von Sicherheitsvorfällen SOLLTE durch eine positive Fehlerkultur und/oder anonyme Meldewege gefördert werden.

18.3 Reaktion

Es MUSS ein Verfahren (siehe Anhang A 1) implementiert werden, das beim Auftreten eines Sicherheitsvorfalls folgende Reaktionen zeitnah 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 der Regelbetrieb wieder aufgenommen.
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden.

Bei geringfügigen Sicherheitsvorfällen KÖNNEN einzelne Punkte ausgelassen und/oder das Verfahren vorzeitig beendet werden.

Das Verfahren SOLLTE so gestaltet werden, dass auch bei Abwesenheit des ISB eine zeitnahe Reaktion gewährleistet ist.

Anhang A Anhang

A.1 Verfahren

Die Organisation 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, 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 dokumentiert und bekannt gegeben.
3. Verfahren werden verbessert, wenn Mängel in ihrer Umsetzung, Angemessenheit oder 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

Die Organisation 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 200-3, 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. Ihre 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 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 werden. Dies MUSS 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 Faktoren 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 sich eine bestehende Gefährdung wesentlich erhöht hat).

Anhang B Register der Änderungen gegenüber der Vorgängerversion VdS 3473 : 2015-07 (01)

Kapitel 1 (Allgemeines)

– Möglichkeit, den Geltungsbereich technisch, geographisch und/oder organisatorisch einzugrenzen, wurde aufgenommen (Abschnitt 1.2)

Kapitel 2 (Normative Verweise)

– Aktualisierung der Verweise
– Ergänzungen der Verweise aufgrund neu aufgenommener Empfehlungen (DIN EN 1047-1, DIN VDE 0100, ISO/IEC 27001)

Kapitel 3 (Begriffe)

– Begriffe ergänzt, um Lesbarkeit zu erhöhen (z. B. Inventarisierung, Maximal Tolerierbare Ausfallzeit MTA, Maximal Tolerierbarer Datenverlust MTD, Notbetrieb)
– aufgrund neuer Formulierungen bzw. Inhalte benötigte Begriffe aufgenommen (z. B. Echtzeitbetrieb, Externer, Zutritt)
– nach Änderungen nicht mehr benötigte Begriffe gestrichen (z. B. Notfall, physischer Zugriff, Personal)
– Annäherung an die Ausdrucksweise des BSI (Zugang, Zutritt, Zugriff)
– Annäherung an die Ausdrucksweise von ISO/IEC 27001 (Organisation)

Kapitel 4 (Organisation der Informationssicherheit)

– Prüfung der rechtlichen Zulässigkeit bei nicht erfolgten Funktionstrennungen hinzugefügt (Abschnitt 4.1.2)
– Anforderungen an ISB abstrakter gefasst (Abschnitt 4.3)
– Empfehlung für Stellvertretungsregelung des ISB neu aufgenommen (Abschnitt 4.3)
– Zusammensetzung und Aufgaben des IST konkreter gefasst (Abschnitt 4.4)
– Abschnitt "Lieferanten und sonstige Auftragnehmer" entfallen (ehemals 4.10), da dieser Personenkreis unter "Mitarbeiter" subsumiert wurde (Abschnitt 4.8)
– Neuer Abschnitt "Externe" eingeführt (Abschnitt 4.10)

Kapitel 5 (Leitlinie zur Informationssicherheit)

– Hinweise auf Konsequenzen der Nichtbeachtung von Maßnahmen auf Empfehlung herabgestuft (Abschnitt 5.2)

Kapitel 6 (Richtlinien zu Informationssicherheit)

– Richtlinien nun flexibler gestaltbar (Abschnitt 6.1)
– Anforderungen an Richtlinien für Nutzer vereinfacht und vereinheitlicht (Abschnitt 6.3), so dass spezielle Richtlinien für Externe entfallen sind (ehemals Abschnitt 6.4)

Kapitel 7 (Mitarbeiter)

– Ausgabe und Einziehen von IT-Ressourcen aufgenommen (Abschnitte 7.2 und 7.3)

Kapitel 8 (Wissen)

– Maßnahmen für Schulungen und Sensibilisierungen konkretisiert und erweitert (Abschnitt 8.2)

Kapitel 9 (Identifizieren kritischer IT-Ressourcen)

– Vorgehen im Analyseprozess uniformer gestaltet (Abschnitte 9.1 bis 9.3)
– Analyse vereinfacht, indem die Kriterien für kritische Informationen vereinfacht und klarer gefasst wurden (Abschnitt 9.2 und Kapitel 3)

Kapitel 10 (IT-Systeme)

– Dokumentation vereinfacht (Abschnitte 10.2.1 und 10.2.2)
– Maßnahmen zur System- und Anwendungssoftware (Abschnitt 10.3.1) erweitert

Kapitel 11 (Netzwerke und Verbindungen)

– Anforderungen an den Netzwerkplan (Abschnitt 11.1) erweitert
– verpflichtende Risikoanalyse für die Absicherung von Netzübergängen entfernt (Abschnitt 11.3)

Kapitel 12 (Mobile Datenträger)

– Empfehlungen zum Schutz der Informationen auf mobilen Datenträgern (Abschnitt 12.2) neu aufgenommen
– Maßnahmen für kritische mobile Datenträger gekürzt, dadurch entfallen Maßnahmen zum Schutz der gespeicherten Daten und Verfahren bei Verlust (ehemals Abschnitte 12.2.2 und 12.2.3)

Kapitel 13 (Umgebung)

– Empfehlung der DIN VDE 0100-Reihe und der DIN EN 50173/4-Reihe aufgenommen (Abschnitte 13.1 und 13.2)
– Empfehlung für das Errichten von Sicherheitszonen aufgenommen (Abschnitt 13.3)

Kapitel 14 (IT-Outsourcing und Cloud Computing)

– Entscheidungen über IT-Outsourcing und Cloud Computing vereinfacht (Abschnitt 14.1)
– Anforderungen identisch/kompatibel mit den Anforderungen des Kompetenznetzwerk Trusted Cloud e. V. (siehe https://www.trusted-cloud.de) gestaltet (Abschnitt 14.4)

Kapitel 15 (Zugänge und Zugriffsrechte)

– keine inhaltlichen Änderungen

Kapitel 16 (Datensicherung und Archivierung)

– Vorgehensweisen für die Datensicherung, -wiederherstellung sowie -archivierung als Verfahren (Abschnitt 16.3), unterliegt somit dem KVP
– Testen der Sicherungs- und Wiederherstellungsverfahren in die Verfahren zur Datensicherung, -wiederherstellung sowie -archivierung aufgenommen (Abschnitt 16.3); dadurch entfällt Abschnitt 16.5.5 der Vorversion.

Kapitel 17 (Störungen und Ausfälle)

– Reaktion auf Störungen und Ausfälle (Abschnitt 17.2) flexibler gestaltet
– Wiederanlaufpläne müssen als Verfahren definiert werden und unterliegen somit dem KVP (Abschnitt 17.3.1)

Kapitel 18 (Sicherheitsvorfälle)

– Reaktion auf Sicherheitsvorfälle (Abschnitt 18.3) flexibler gestaltet

Anhang A1 (Verfahren)

– keine inhaltlichen Änderungen

Anhang A2 (Risikoanalyse und -behandlung)

– keine inhaltlichen Änderungen