Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

VdS 10000 : 2025-01 (03)

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 174
D-50735 Köln
Telefon: (0221) 77 66 0; E-Mail: verlag@vds.de

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.

Um eine Beeinträchtigung des Textverständnisses zu vermeiden, verwendet VdS Schadenverhütung durchweg das generische Maskulinum. Eine Bevorzugung oder anderweitige Wertung des männlichen, weiblichen oder sonstigen Geschlechts geht damit ausdrücklich nicht einher.

INHALT

1 Allgemeines

1.1 Einleitung

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 potenzielle 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).

1.2 Anwendungshinweise

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

Die Umsetzung der geforderten Maßnahmen erfordert 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 potenzielle Synergieeffekte zu nutzen.

Insbesondere SOLLTEN sie zusammen mit den VdS-Richtlinien zur Umsetzung der DSGVO*, VdS 10010 und/oder den VdS-Richtlinien* Informationssicherheitsmanagement-system für Industrielle Automatisierungssysteme*, VdS 10020 implementiert werden.*

Bei umfangreicheren Anforderungen an die Informationssicherheit, insbesondere wenn die Erfüllung von NIS-2 gefordert ist, SOLLTE die Umsetzung der VdS-Richtlinien Strukturierte Informationssicherheit gemäß NIS-2*, VdS 10100 geprüft werden.*

1.3 Anwendungs- und Geltungsbereich

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

Der Geltungsbereich der Richtlinien SOLLTE die gesamte Organisation umfassen, KANN jedoch technisch, geografisch und/oder organisatorisch eingegrenzt werden.

Die in diesen Richtlinien definierten Anforderungen und Maßnahmen gelten ausschließlich für den im Rahmen des Informationssicherheitsmanagementsystems (ISMS) festgelegten Geltungsbereich, sofern nicht ausdrücklich anderweitig festgelegt. Die Organisation MUSS sicherstellen, dass Risiken durch Wechselwirkungen innerhalb und außerhalb des Geltungsbereichs entsprechend berücksichtigt werden.

1.4 Gültigkeit

Diese Richtlinien gelten ab dem 01.01.2025 und ersetzen die Richtlinien VdS 10000 : 2018-12 (02).

2 Normative Verweisungen

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 letzte Fassung.

BSI-Standard 200-2 IT-Grundschutz-Methodik

BSI-Standard 200-3 Risikomanagement

BSI-Standard 200-4 Business Continuity Management

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 Resilienz – Business Continuity Management System – Anforderungen

DIN VDE 0100 Normenreihe zum Errichten von Niederspannungsanlagen

Elementare Gefährdungen Aufstellung elementarer Gefährdungen des BSI für die IT-Grundschutz-Methodik und für die Arbeit mit dem IT-Grundschutz-Kompendium

ENISA Thread Taxonomy Bedrohungstaxonomie die auf der Grundlage des verfügbaren ENISA-Materials erstellt wurde

ISO 31000 Risikomanagement – Leitlinien

ISO/IEC 27001 Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen

ISO/IEC 27005 Informationssicherheit, Cybersicherheit und Datenschutz – Leitfaden zur Handhabung von Informationssicherheitsrisiken

ISO/IEC 31010 Risk management – Risk assessment techniques

VdS 2007 Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen

VdS 10003 Richtlinien für die Anerkennung von Beratern für Cyber-Security

VdS 10010 Datenschutzmanagementsystem für kleine und mittlere Unternehmen (KMU) zur Umsetzung der DSGVO – Anforderungen

VdS 10020 Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU) – Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme

VdS 10100 Strukturierte Informationssicherheit gemäß NIS-2

3 Begriffe und Abkürzungen

3.1 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: für Einrichtung, Betrieb, Überwachung und/oder Wartung eines IT-Systems oder Netzwerks zuständige Person

aktive Netzwerkkomponente: über eine eigene Logik wie z. B. Hub, Switch, Repeater, Bridge, Medienkonverter, Gateway, Firewall usw. verfügende Netzwerkkomponente

Hinweis: 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

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

Authentifizierungsmerkmal: Merkmal, mit dessen Hilfe eine anfragende Instanz ihre Identität nachweisen kann

Hinweis: Authentifizierungsmerkmale können Wissen (z. B. Passwort oder PIN), Besitz (z. B. Chipkarte oder Token) oder biometrische Merkmale (z. B. Fingerabdruck oder Iris) sein.

Authentizität: Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit

Bedrohung: Umstand oder Ereignis, durch den oder durch das ein Schaden entstehen kann

Hinweis: 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 ermöglicht, IT-Ressourcen wie Speicher, Rechenleistung oder Anwendungen aus einem zentralen Pool über ein Netzwerk bereitzustellen und zu nutzen

Daten: Anordnung von Zeichen, die auf Basis vereinbarter Konventionen zur Darstellung von Informationen verwendet werden

Datenleitung: physisches Medium, über das Daten ausgetauscht werden können

Dienst: von IT-Systemen bereitgestellte Funktionalität oder Leistung, die bestimmte Aufgaben oder Funktionen erfüllt

Echtzeitbetrieb: Fähigkeit eines Systems, auf ein Ereignis innerhalb eines vorgegebenen Zeitraums zu reagieren

Eigenmächtigkeit: Handeln ohne Auftrag, Erlaubnis oder Befugnis

externe Person: natürliche Person, die kein Mitarbeiter ist

Hinweis: Im normalen Geschäftsbetrieb fallen z. B. Geschäftspartner oder Gäste unter diese Definition.

Funktion: Bündel von Aufgaben, durch deren Umsetzung Teile der Ziele der Organisation erreicht werden sollen

Gefahr: Möglichkeit einer Schadwirkung auf ein Objekt

Gefährdung: Bedrohung, die über eine Schwachstelle auf ein zu schützendes Objekt konkret einwirkt (Bedrohung plus Schwachstelle)

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

Informationssicherheit: Schutz von Informationen hinsichtlich gegebener Sicherheitsanforderungen

Hinweis: Anforderungen beziehen sich i. d. R. auf da Maß an Vertraulichkeit, Verfügbarkeit oder Integrität.

Informationssicherheitsbeauftragter (ISB): Person, die nach Bestellung und im Auftrag des Topmanagements eines Unternehmens für die Umsetzung der Leitlinie zur Informationssicherheit des Unternehmens zuständig ist

Informationssicherheitsteam (IST): Gremium, das nach Bestellung und im Auftrag des Topmanagements eines Unternehmens zusammengestellt und für definierte Aufgaben zur Aufrechterhaltung der Informationssicherheit zuständig ist

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

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

Inventarisierung: Bestandsaufnahme zu einem definierten Zeitpunkt

IS-Leitlinie: Leitlinie zur vollumfänglichen Beschreibung und Definition der Informationssicherheit einer Organisationseinheit

IS-Richtlinie: unterstützendes, zur Umsetzung der IS-Leitlinie erforderliches Dokument, welches alle erforderliche Zusatzinformationen subsummiert

IT-Infrastruktur: Gesamtheit aller langlebiger Einrichtungen materieller und institutioneller Art für den Betrieb von Anwendungssoftware

IT-Ressource: Betriebsmittel für die elektronische Informationsverarbeitung

Hinweis: Hierzu zählen u. a. IT-Systeme, Datenträger, Verbindungen, Daten, Informationen sowie Mitarbeitende.

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-Sicherheit: technische und organisatorische Maßnahmen zum Schutz der IT-Infrastruktur

Hinweis: Die IT-Sicherheit ist ein Teilbereich der Informationssicherheit.

IT-System: technische Anlage, die der Informationsverarbeitung dient und eine abgeschlossene Funktionseinheit aus Hard- und Software bildet

Beispiele: Typische IT-Systeme sind z. B. Server (physisch und virtuell), Clients, Drucker, Mobiltelefone, Smartphones, Telefonanlagen, Laptops, Tablets und aktive Netzwerkkomponenten.

katastrophaler Schaden: Schaden, mit relevanter oder ruinöser Wirkung auf Leib und Leben von Personen, auf zentrale Prozesse, auf zentrale Werte oder auf die Rechtskonformität einer Organisation

Hinweis: Im Zuge von katastrophalen Schäden können Menschen schwer verletzt oder getötet werden; können zentrale Prozesse einer Organisation zum Erliegen gebracht und die Rückkehr zum Regelbetrieb (innerhalb eines akzeptablen Zeitraums) verhindert werden; können zentrale Werte der Organisation verloren gehen oder zerstört werden wobei die Wiederherstellung (mit den Ressourcen der Organisation) nicht möglich ist; können Gesetze, Verträge oder Normen gebrochen werden woraus resultierende Haftungsverpflichtungen für die Organisation oder für die Verantwortlichen ruinös sein können.

kritische Individualsoftware: für den Betrieb von kritischen IT-Systemen zwingend benötigte und individuell für die Organisation erstellte oder angepasste Software

kritische Informationen: Informationen, mit denen bei bestimmten Aktionen katastrophale Schäden erwirkt werden können

Hinweis: Im Textverlauf sind hierzu Erläuterungen und Konkretisierungen formuliert.

kritisches IT-System: IT-System, das kritische Informationen verarbeitet, speichert oder überträgt oder das für den Betrieb von kritischen IT-Ressourcen zwingend benötigt wird

Hinweis: Im Textverlauf sind hierzu Erläuterungen und Konkretisierungen formuliert.

kritischer mobiler Datenträger: mobiler Datenträger, der die Eigenschaften eines kritischen IT-Systems erfüllt

Hinweis: Im Textverlauf sind hierzu Erläuterungen und Konkretisierungen formuliert

kritische Verbindung: Verbindung, die kritische Informationen überträgt

Hinweis: Im Textverlauf sind hierzu Erläuterungen und Konkretisierungen formuliert.

Leitlinie: vom Topmanagement bereitgestelltes Dokument, das Ziele der Organisation sowie dessen Priorität definiert sowie Verantwortlichkeiten zu deren Erreichung festlegt

maximal tolerierbare Ausfallzeit (MTA): definierte Zeitspanne, innerhalb der eine definierte Leistung (z. B. ein Notbetriebsniveau) wiederhergestellt sein muss

maximal tolerierbarer Datenverlust (MTD): definierte Höchstmenge bzw. Werte oder Inhalte von Daten, deren Verlust im Rahmen eines Systemfehlers oder -ausfalls akzeptabel sind

Hinweis: Die definierte Höchstmenge kann sich sowohl auf die Anzahl der Daten als auch auf eine Zeitspanne beziehen, z. B. die Daten der letzten 24 Stunden.

Mehr-Faktor-Authentifizierung: Nachweis der Authentizität mit Hilfe mehrerer, unabhängiger Merkmale

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

Hinweis: Mitarbeiter sind z. B. Angestellte, Arbeiter, Beamte, freie Mitarbeiter, Dienstleister oder deren Mitarbeiter bzw. Erfüllungsgehilfen.

mobiler Datenträger: nicht fest installierter, sondern transportabel und an unterschiedlichen Örtlichkeiten einsetzbarer Datenträger

Hinweis: Typische mobile Datenträger sind z. B. Speichersticks und -karten sowie externe Festplatten aber auch Speichermedien wie CD-ROMs, DVDs und Disketten.

mobiles IT-System: nicht fest installiertes, sondern transportabel und an unterschiedlichen Örtlichkeiten einsetzbares IT-System

Hinweis: Typische mobile IT-Systeme sind z. B. Notebooks, Smartphones, Tablets oder Digitalkameras.

Netzwerkkomponente: eine der Weiterleitung von Daten dienende technische Anlage

Hinweis: Es werden aktive und passive Netzwerkkomponenten unterschieden.

Netzübergang: Schnittstelle zwischen zwei Netzwerken, die sich hinsichtlich ihrer physikalischen Übertragungsmedien, der verwendeten Protokolle, durch ihre administrative Hoheit oder durch eine unterschiedliche Vertrauenswürdigkeit 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: in einer Organisation prozedural zusammengefasste (Teil-) Aufgaben oder Tätigkeiten

passive Netzwerkkomponente: Netzwerkkomponente, die keine eigene Logik besitzt und keine aktiven Datenverarbeitungs- oder Steuerungsfunktionen ausführt,

Hinweis: Typische passive Netzwerkkomponenten sind z. B. Kabel, Stecker, Patchfelder oder Anschlusspunkte.

Position: Stellung, die ein Mitarbeiter in der Hierarchie einer Organisation einnimmt

Projektverantwortlicher: für die Planung, Steuerung und Überwachung eines Projekts verantwortliche Person

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

Prozess mit hohem Schadenpotential: Prozess, bei dem eine Fehlfunktion oder die Verletzung der zugesicherten Verfügbarkeit ein katastrophaler Schaden entstehen kann

Hinweis: Typische Prozesse mit hohem Schadenpotenzial sind z. B. die Datensicherung und -wiederherstellung.

Prozessverantwortlicher: inhaltlich für einen oder mehrere Prozesse verantwortliche Person

Hinweis: Der Prozessverantwortliche muss den Überblick über die für diese Prozesse benötigten Ressourcen und über die an sie gestellten Anforderungen besitzen.

Regelung: verbindliche Vorgabe

Ressource: der Organisation gehörendes und/oder von ihr nutzbares Betriebsmittel

Risiko: nach Eintrittswahrscheinlichkeit und Schadenhöhe bewertete Gefährdung

Schnittstelle: der Kommunikation dienender Teil eines IT-Systems

Hinweis: Dies können z. B. Ethernet- und Wireless-LAN-Adapter, ISDN-Karten, Modems, USB-Ports, NFC- und Infrarot-Schnittstellen, SD-Slots oder Tastaturen sein.

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

Server: Dienste über Verbindungen zur Verfügung stellendes zentrales IT-System

Sicherheit: Abwesenheit nicht beherrschbarer Gefahren

Hinweis: Eine vollständige Sicherheit kann in der Praxis nicht erreicht werden. Das angemessene Maß an Sicherheit muss deshalb von den beteiligten Parteien definiert und fortlaufend an die Erfordernisse und die Umgebungsbedingungen angepasst werden.

Sicherheitsvorfall: unerwünschtes Ereignis, das die Informationssicherheit beeinträchtigt

Speicherort: Ort, an dem die dauerhafte Speicherung von Daten durch Nutzer oder Applikationen erfolgt

Hinweis: Bei einem Speicherort kann es sich um einen lokalen Speicherort (wie z. B. Verzeichnisse auf Servern oder Workstations), einen mobilen Speicherort (wie z. B. Smartphones oder Digitalkameras) oder um einen entfernt gelegenen Speicherort (wie z. B. ausgelagerte Server oder Cloud-Dienste) handeln.

Systemsoftware: Firmware, Betriebssystem und systemnahe Software, die interne und externe Hardwarekomponenten eines IT-Systems verwaltet

Topmanagement: oberste Führungsebene einer Organisation

Hinweis: Dies können Vorstände, Geschäftsführer oder Behördenleiter sein.

Verbindung: Kanal, über den Daten ausgetauscht werden können

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

Verfügbarkeit: Eigenschaft einer Ressource, nutzbar zu sein

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

zentraler Prozess: Prozess, der mitentscheidend für die Aufgabenerfüllung der Organisation ist

Hinweis: Dies kann z. B. ein Prozess für die Wertschöpfung oder für den Erhalt bzw. die Verbesserung der Wettbewerbsfähigkeit sein.

zentraler Wert: materielles oder immaterielles Element, das für die Aufgabenerfüllung der Organisation, insbesondere für die Durchführung zentraler Prozesse und solche mit hohem Schadenspotenzial, unverzichtbar ist

Hinweis: Hierzu sind beispielsweise Produktionsanlagen, Wissen, Mitarbeiter sowie das Vertrauen von Kunden und Geschäftspartnern zu zählen.

Zugang: Einrichtung, die es erlaubt, die nichtöffentliche IT einer 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

3.2 Abkürzungen

BCM Business Continuity Management

ISB Informationssicherheitsbeauftragter

ISMS Informationssicherheitsmanagementsystem

IST Informationssicherheitsteam

KMU kleine und mittlere Unternehmen

MTA maximal tolerierbare Ausfallzeit

MTD maximal tolerierbarer Datenverlust

4 Organisation der Informationssicherheit

4.1 Grundlagen

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.

4.2 Verantwortlichkeiten

4.2.1 Anforderungen

Verantwortlichkeiten (siehe Abschnitte 4.2 bis 4.11) MÜSSEN eindeutig und widerspruchsfrei zugewiesen werden.

4.2.2 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 Verantwortlichen wahrnehmen.

4.2.3 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 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 4.2.2) besonders hervorgehoben und begründet.

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

4.2.4 Zeitliche Ressourcen

Um zugewiesene Verantwortlichkeiten wahrzunehmen, MÜSSEN die entsprechenden Mitarbeiter im erforderlichen Umfang (siehe Abschnitt 4.2.2) von anderen Tätigkeiten freigestellt werden.

4.2.5 Delegieren von Aufgaben

Verantwortliche für Informationssicherheit KÖNNEN Aufgaben an andere Personen delegieren.

Die Verantwortung für delegierte Aufgaben verbleibt jedoch bei der ursprünglich verantwortlichen Person, so dass sie die Erfüllung und das Ergebnis der delegierten Aufgaben überprüfen MÜSSEN.

4.3 Topmanagement

Das Topmanagement MUSS sich zur Wahrnehmung folgender Verantwortlichkeiten verpflichten:

1. Übernahme der Gesamtverantwortung für die Informationssicherheit
2. In Kraft Setzung von Richtlinien für die Informationssicherheit (IS-Richtlinien)
3. Bereitstellung der notwendigen technischen, finanziellen und personellen Ressourcen für die Informationssicherheit
4. Einbettung der Informationssicherheit in die Strukturen, Hierarchien und Arbeitsabläufe der Organisation

4.4 Informationssicherheitsbeauftragter

Das Topmanagement MUSS einen Informationssicherheitsbeauftragten (ISB) bestellen.

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. Steuerung, Koordinierung und Prüfung der technischen und organisatorischen Maßnahmen im Bereich der Informationssicherheit
2. Kontinuierliche Verbesserung der Informationssicherheit
3. Anpassung der Informationssicherheit an neue Bedrohungen, neue Schwachstellen und an neue gesetzliche, betriebliche und vertragliche Anforderungen
4. Jährlicher Bericht 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.

4.5 Informationssicherheitsteam

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

4.6 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

4.7 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.

4.8 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.

4.9 Mitarbeiter

Mitarbeiter MÜSSEN folgende Aufgaben wahrnehmen:

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

4.10 Projektverantwortliche

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

4.11 Externe Personen

Externe Personen 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)

5.1 Grundlagen

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.

5.2 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 initial und nach jeder Aktualisierung zeitnah bekannt gegeben werden und in der jeweils aktuellen Form allen Betroffenen zur Verfügung stehen.

5.3 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 4.3 bis 4.11) und weist auf deren Aufgaben hin.

Die Leitlinie SOLLTE auf die Konsequenzen ihrer Nichtbeachtung hinweisen.

6 Richtlinien zur Informationssicherheit (IS-Richtlinien)

6.1 Grundlagen

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.

6.2 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, betrieblichen und vertraglichen Anforderungen ermittelt und entsprechend umgesetzt werden.

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

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

IS-Richtlinien MÜSSEN umgesetzt oder vom Topmanagement aufgehoben werden.

6.3 Inhalte

Jede IS-Richtlinie MUSS folgende Anforderungen erfüllen:

1. Sie definiert, 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.

6.4 Aufbau und Funktionsweise des ISMS

Aufbau und Funktionsweise des ISMS MUSS in einer IS-Richtlinie verbindlich festgelegt werden.

Die IS-Richtlinie MUSS darüber hinaus eine Aufstellung sämtlicher für das ISMS relevanten Dokumente beinhalten und Informationen bereitstellen, wo diese zu finden sind:

1. IS-Leitlinie (siehe Kapitel 5)
2. IS-Richtlinien (siehe Kapitel 6)
3. Für die Informationssicherheit relevante Verfahren (siehe Anhang A.1)
4. Die in diesen Richtlinien geforderten Dokumente (wie z. B. Dokumentationen)
5. Dokumente, die im Zuge des Betriebs des ISMS und im Zuge des Kontinuierlichen Verbesserungsprozesses (KVP) entstehen (wie z. B. Nachweise über durchgeführte Tätigkeiten)

6.5 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

   Es wird definiert, ob die private Nutzung der IT erlaubt ist.
   a. Wenn die private Nutzung der IT erlaubt ist, so wird sie im Sinne der Organisation ausgestaltet.
3. Grundlegende Verhaltensregeln
   a. Hard- und Software darf nicht eigenmächtig in der IT-Infrastruktur installiert, genutzt oder betrieben werden.

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 eigenmächtig weitergegeben.

4. Umgang mit 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 zu den von 1. bis 6. genannten Regelungen MÜSSEN vom ISB genehmigt werden.

6.6 Weitere Richtlinien

Es MÜSSEN weitere spezifische IS-Richtlinien erarbeitet werden, sofern die folgenden Punkte in der Organisation relevant sind:

1. Mobile IT-Systeme (siehe Abschnitt 10.5)
2. Mobile Datenträger (siehe Abschnitt 12)
3. IT-Outsourcing und Cloud Computing (siehe Abschnitt 14)
4. Datensicherung (siehe Abschnitt 16)
5. Sicherheitsvorfälle (siehe Abschnitt 17)

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

7 Mitarbeiter

7.1 Grundlagen

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

7.2 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.

7.3 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 8.3).
4. Mitarbeiter erhalten die benötigten IT-Ressourcen, Zugänge, Zugriffsrechte sowie physischen Zugangsmittel wie Schlüssel, Transponder etc. und werden in deren Nutzung geschult.

7.4 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.
3. Die Zutrittsrechte des Mitarbeiters werden unverzüglich überprüft, und falls erforderlich, erfolgt die Einziehung oder Deaktivierung der physischen Zugangsmittel wie Schlüssel, Transponder etc.

8 Wissen

8.1 Grundlagen

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.

8.2 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 gesetzliche, betriebliche und vertragliche Anforderungen sowie über neue Bedrohungen und Schwachstellen im Bereich der Informationssicherheit informiert werden.

Das Verfahren MUSS folgende Punkte sicherstellen:

1. Es werden regelmäßig aus verlässlichen Quellen Informationen über die aktuellen gesetzlichen Anforderungen an die Informationssicherheit bezogen.
2. Es werden regelmäßig aus verlässlichen Quellen Informationen über neue Bedrohungen und Schwachstellen und über mögliche Gegenmaßnahmen bezogen.
3. Es findet in der Organisation ein regelmäßiger Austausch über die aktuellen betrieblichen und vertraglichen Anforderungen im Bereich der Informationssicherheit statt.
4. Die Informationen werden im Hinblick auf die Bedeutung für die Informationssicherheit zeitnah ausgewertet, um geänderte Gefahrenlagen zu erkennen.
5. 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.

8.3 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 Sicherheitsvorfällen.
5. Sie vermitteln den Teilnehmern ihre Verantwortung für die Informationssicherheit und fördern bei ihnen die Akzeptanz der technischen und organisatorischen 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

9.1 Grundlagen

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.

9.2 Prozesse

Die Organisation MUSS ihre zentralen Prozesse und ihre Prozesse mit hohem Schadenpotenzial 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 Schadenpotenzial ist.
3. Sie benennt, wer für den Prozess verantwortlich ist (Prozessverantwortlicher).
4. Sie definiert die maximal tolerierbare Ausfallzeit (MTA) des Prozesses.

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

9.3 Kritische 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 *Zugesicherte Verfügbarkeit*)

Hierfür MÜSSEN die zentralen Prozesse und die Prozesse mit hohem Schadenpotential (siehe Abschnitt 9.2) 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.

9.4 Kritische IT-Ressourcen

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

Kritische IT-Ressourcen sind IT-Ressourcen, die kritische Informationen (siehe Abschnitt 9.3) verarbeiten, speichern oder übertragen oder die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden.

Hierfür MÜSSEN die kritischen Informationen (siehe Abschnitt 9.3) 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 definiert die maximal tolerierbare Ausfallzeit (MTA) der kritischen IT-Ressource.

Die MTA der kritischen Ressource MUSS ebenso kurz oder kürzer sein als die kürzeste MTA aller zentralen Prozesse und Prozesse mit hohem Schadenpotential (siehe Abschnitt 9.2), 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

10.1 Grundlagen

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

10.2 Inventarisierung

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

Die Inventarisierung MUSS durch entsprechende Verfahren (siehe Abschnitte 10.3.2 und 10.3.3) 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.

10.3 Lebenszyklus

10.3.1 Beschreibung

IT-Systeme bilden eine abgeschlossene Funktionseinheit aus Hard- und Software (siehe Abschnitt 10.4). Sie unterliegen einem Lebenszyklus, der sich von der Inbetriebnahme bis zur Ausmusterung erstreckt.

10.3.2 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 9.4).
2. Die entsprechenden Schutzmaßnahmen werden umgesetzt.
3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.2) und der Netzwerkplan (siehe Abschnitt 11.2) werden aktualisiert.
4. Bei Inbetriebnahme werden die Arbeitsschritte dokumentiert.

10.3.3 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.
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 10.2) und der Netzwerkplan (siehe Abschnitt 11.2) werden aktualisiert.
4. Im Zuge der Ausmusterung werden die damit einhergehenden Arbeitsschritte dokumentiert.

10.4 Basisschutz

10.4.1 Funktionalitäten und Maßnahmen

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, SOLLTEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MÜSSEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

10.4.2 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 in Betrieb genommen werden.

10.4.3 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 sich nicht beheben lassen oder bewusst beibehalten werden (z. B. wenn keine Sicherheitsupdates installiert werden können, Authentifizierungsmerkmale nicht geändert werden können oder unsichere technische Verfahren eingesetzt werden müssen).
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 sowie von und zu solchen, die wichtige oder sicherheitskritische Funktionen bereitstellen, auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden.

Die Beschränkung des Netzwerkverkehrs KANN z. B. durch eine geeignete Segmentierung des Netzwerks (siehe Abschnitt 11.5.3), lokale Filtermechanismen oder durch das Deaktivieren nicht benötigter Dienste erfolgen.

10.4.4 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 dem keine gesetzlichen oder vertraglichen Lösch- oder Aufbewahrungspflichten entgegenstehen.

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

10.4.5 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.

10.4.6 Schadsoftware

Jedes IT-System MUSS über einen Echtzeitschutz vor Schadsoftware verfügen, der alle Dateien bei Zugriff entsprechend prüft (musterbasierte Erkennung).

Zusätzlich SOLLTE das Verhalten ausgeführter Programme überwacht werden, um schädliche Software zu erkennen.

Das Ausführen erkannter Schadsoftware MUSS verhindert werden.

Die Software zum Schutz gegen Schadsoftware MUSS automatisch und in kurzen zeitlichen Abständen (z. B. stündlich oder täglich) die neuesten Suchmuster der Hersteller ermitteln und diese verwenden.

10.4.7 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.

10.4.8 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.

10.4.9 Zugänge und Zugriffe

Administrative Tätigkeiten MÜSSEN über die speziell dafür vorgesehenen Zugänge erfolgen.

Diese DÜRFEN NICHT für die alltägliche Nutzung der IT-Systeme verwendet 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“).*
3. *Nutzer können nur jene Funktionen nutzen, die sie für die Erfüllung ihrer Aufgaben benötigen („Least-Functionality“).*

10.5 Zusätzliche Maßnahmen für mobile IT-Systeme

10.5.1 Grundlagen

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.

10.5.2 IS-Richtlinie

In Ergänzung zu Abschnitt 6.4 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.

10.5.3 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.

10.5.4 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 zu erfolgen hat.

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 17) behandelt werden.

10.6 Zusätzliche Maßnahmen für kritische IT-Systeme

10.6.1 Grundlagen

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

Wenn Maßnahmen nicht umgesetzt werden, MÜSSEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

10.6.2 Risikomanagement

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

10.6.3 Notbetriebsniveau

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

10.6.4 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.

10.6.5 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.

10.6.6 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 10.6.10).

10.6.7 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 ist für das IT-System verantwortlich?
2. Wie und mit welchen Zugängen und Authentifizierungsmerkmalen ist der administrative Zugang zum IT-System möglich?
3. Welche grundlegenden Designentscheidungen wurden bei der Installation getroffen?
4. Welche Änderungen wurden vorgenommen?
5. Wann wurden sie vorgenommen?
6. Wer hat sie vorgenommen?
7. Warum wurden sie vorgenommen?

Eine unvollständige oder falsche Dokumentation SOLLTE als Sicherheitsvorfall (siehe Kapitel 17) behandelt werden.

10.6.8 Datensicherung

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

10.6.9 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.

10.6.10 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 Schadenpotential weiter zu betreiben.

Das Ersatzsystem oder -verfahren SOLLTE das Notbetriebsniveau (siehe Abschnitt 10.6.3) des kritischen IT-Systems sicherstellen.

10.6.11 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

11.1 Grundlagen

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

11.2 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 11.5.3), deren Einsatzzweck und deren Verbindungen untereinander
   b. Fernzugänge (siehe Abschnitt 11.5.4)
   c. Netzwerkkopplungen (siehe Abschnitt 11.5.5)
   d. Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken (siehe Abschnitt 11.4)

11.3 Aktive Netzwerkkomponenten

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

11.4 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 17) behandelt.

Wenn Maßnahmen nicht umgesetzt werden, MÜSSEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang *A.2).*

Weitere Sicherheitsmaßnahmen SOLLTEN im Zuge einer Risikoidentifikation, -analyse 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 hat sie implementiert?
   b. Wann wurden sie implementiert?
   c. Was bewirken sie?
   d. Warum werden sie benötigt?
2. Die angestrebten Verkehrsbeschränkungen werden wirksam umgesetzt.

11.5 Basisschutz

11.5.1 Grundanforderungen

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

Wenn eine entsprechende Funktionalität nicht gegeben ist, SOLLTEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MÜSSEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

11.5.2 Netzwerkanschlüsse

Dauerhaft nicht genutzte Netzwerkanschlüsse MÜSSEN vor unberechtigter Nutzung gesichert werden.

Dies KANN z. B. durch eine Zutrittsbeschränkung, eine Deaktivierung der Netzwerkanschlüsse oder durch eine Netzwerkzugangskontrolle geschehen.

11.5.3 Segmentierung

Es MÜSSEN Kriterien definiert werden, anhand derer die Netzwerke in einzelne Sicherheitszonen unterteilt werden (Segmentierung).

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

11.5.4 Fernzugang

Der Zugang zu nichtöffentlichen Bereichen von IT-Systemen 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.

3. 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.

Darüber hinaus SOLLTE der Zugang so gestaltet werden, 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.

11.5.5 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.

11.6 Zusätzliche Maßnahmen für kritische Verbindungen

Für alle kritischen Verbindungen MUSS eine Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) etabliert werden.

12 Mobile Datenträger

12.1 Grundlagen

Mobile Datenträger sind aufgrund ihrer exponierten Nutzungsart besonders gefährdet. Die damit verbundenen Risiken sind angemessen zu behandeln.

12.2 IS-Richtlinie

In Ergänzung zu Abschnitt 6.4 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit mobilen Datenträgern die folgenden Maßnahmen umgesetzt 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.

12.3 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.

12.4 Zusätzliche Maßnahmen für kritische mobile Datenträger

Für alle kritischen mobilen Datenträger MUSS eine Risikoidentifikation, -analyse und -behandlung (siehe Anhang) etabliert werden.

13 Umgebung

13.1 Grundlagen

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.

13.2 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.

Zusätzlich 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 (z. B. durch Löschmittel, Vandalismus, Diebstahl)*

13.3 Datenleitungen

Sämtliche Datenleitungen SOLLTEN gemäß einschlägiger Normen und Standards, 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.

13.4 Zusätzliche Maßnahmen für kritische IT-Systeme

Im Zuge der Risikoidentifikation, -analyse und -behandlung (siehe Abschnitt 10.6.2) MÜSSEN für alle kritischen IT-Systeme folgende Bedrohungen berücksichtigt werden, um deren Auswirkung zu reduzieren:

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

14.1 Grundlagen

Wenn IT-Ressourcen ausgelagert werden, ist es notwendig, die Sicherheitsinteressen der Organisation zu berücksichtigen, um diese nicht zu kompromittieren.

14.2 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie die Bedingungen, unter welchen IT-Ressourcen ausgelagert werden dürfen, festgelegt werden.

14.3 Vorbereitung

Für jede Maßnahme zur Auslagerung von IT-Ressourcen MÜSSEN folgende Punkte dokumentiert sein:

1. Welche IT-Ressourcen sollen ausgelagert werden?
2. Welche gesetzlichen, betrieblichen und vertraglichen Anforderungen, insbesondere in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität der ausgelagerten IT-Ressourcen, sind zu erfüllen?
3. Sind die auszulagernden IT-Ressourcen kritisch?

Die Organisation MUSS auf die Auslagerung der entsprechenden IT-Ressourcen 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.

14.4 Vertragsgestaltung

Wenn IT-Ressourcen ausgelagert werden, MUSS mit dem Anbieter ein Vertrag geschlossen werden, der die Anforderungen aus Abschnitt 14.3 vertraglich festhält und den Anbieter zu deren Erfüllung verpflichtet.

Darüber hinaus SOLLTEN folgende Punkte sichergestellt werden:

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

14.5 Zusätzliche Maßnahmen für kritische IT-Ressourcen

Wenn kritische IT-Ressourcen ausgelagert werden, MÜSSEN die Anforderungen aus Abschnitt 14.3 an ihre Vertraulichkeit, Verfügbarkeit und Integrität im Rahmen einer Risikoidentifikation und -analyse (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.
4. Eine schriftliche Dokumentation und Meldung bei Änderungen an einem der oben genannten Punkte MUSS vereinbart werden.

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, Zugriffs- und Zutrittsrechte

15.1 Grundlagen

Zugänge, Zugriffs- und Zutrittsrechte erlauben es, auf die nichtöffentliche IT der Organisation und ihre Daten zuzugreifen. Deshalb ist es notwendig, diese strukturiert zu verwalten.

15.2 Verwaltung

Es MÜSSEN Verfahren (siehe Anhang A.1) für das Anlegen und Ändern von Zugängen, Zugriffsrechten und Zutrittsrechten 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 sowie Zutrittsrechte zu Serverräumen, Server- oder Netzwerkschränken oder zu kritischen IT-Systemen werden nur genehmigt, wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers notwendig sind.
3. Wenn ein Nutzer administrative Zugänge oder Zugriffsrechte oder Zutrittsrechte zu Serverräumen, Server- oder Netzwerkschränken oder zu kritischen IT-Systemen erhalten soll, wird dies besonders begründet und vom IT-Verantwortlichen entschieden.
4. Antragssteller und Nutzer werden zeitnah über die erfolgte Durchführung informiert.
5. *Wenn Zugänge, Zugriffsrechte oder Zutrittsrechte 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.

15.3 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen

Alle Zugänge zu kritischen IT-Systemen, sämtliche Zugriffsrechte auf kritische Informationen sowie sämtliche Zutrittsrechte zu kritischen IT-Systemen MÜSSEN jährlich erfasst und daraufhin überprüft werden, ob sie gemäß der Verfahren aus Abschnitt 15.2 angelegt wurden und benötigt werden.

Nicht ordnungsgemäß angelegte Zugänge, Zugriffsrechte oder Zutrittsrechte MÜSSEN als Sicherheitsvorfall (siehe Kapitel 17) behandelt werden.

16 Datensicherung

16.1 Grundlagen

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-Bausteine des BSI implementiert werden.

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

16.2 IS-Richtlinie

In Ergänzung zu Abschnitt 6.4 MÜSSEN in einer IS-Richtlinie die Speicherorte für die Daten der Organisation festgelegt werden.

16.3 Verfahren

Für die Datensicherung und -wiederherstellung 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 selben 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 Sicherung der Daten setzt das Mehr-Generationen-Prinzip um; es gibt z. B. zusätzliche Wochen-, Monats- und Jahressicherungen, damit bei Bedarf mehrere Versionen der gesicherten Daten zur Verfügung stehen.
4. Datensicherungen werden an mehreren Orten gelagert, damit die gesicherten Daten auch bei größeren Schadenereignissen verfügbar bleiben.
6. *Dazu KANN eine vollständige Datensicherung in festen zeitlichen Abständen (z. B. wöchentlich) an einen entfernten Standort ausgelagert werden.*
5. Für die Datensicherung werden mehrere Medien eingesetzt und dabei ist sichergestellt, dass der Ausfall eines Mediums nicht zum Verlust von wesentlichen Teilen der gesicherten Daten führt - wenn die Datensicherung ausschließlich über Cloud-Dienste erfolgt, MUSS sichergestellt sein, dass diese Dienste eine entsprechende Verfügbarkeit garantieren oder dass die Datensicherung auch bei einem Ausfall eines Cloud-Dienstes gewährleistet bleibt (z. B. durch die Nutzung mehrerer unabhängiger Cloud-Anbieter).
6. 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.

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

16.4 Weiterentwicklung

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

Notwendige Anpassungen MÜSSEN zeitnah implementiert werden.

16.5 Basisschutz

16.5.1 Basisschutz-Maßnahmen

Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für Speicherorte (siehe Abschnitt 16.2), Server, aktive Netzwerkkomponenten und mobile IT-Systeme implementiert werden.

Wenn eine entsprechende Funktionalität nicht gegeben ist, SOLLTEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MÜSSEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

16.5.2 IT-Systeme für die Datensicherung und -wiederherstellung

Die für die Datensicherung und -wiederherstellung eingesetzten IT-Systeme MÜSSEN besonders vor unbefugtem Zugang geschützt werden. Dazu sind die folgenden Punkte umzusetzen:

1. Auf den IT-Systemen dürfen ausschließlich Zugänge für administrative Tätigkeiten vorhanden sein.
2. Die Anzahl der administrativen Zugänge ist auf das für den Betrieb notwendige Minimum reduziert.
3. Die administrativen Zugänge werden unabhängig von der restlichen IT verwaltet und sie verfügen über eigene, exklusive Authentifizierungsmerkmale oder sie nutzen eine Mehr-Faktor-Authentifizierung, die unabhängig von der restlichen IT arbeitet.
4. Der Netzwerkverkehr von und zu den IT-Systemen ist auf das für die Funktionsfähigkeit notwendige Minimum beschränkt.

16.5.3 Speicherorte

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

16.5.4 Server

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

16.5.5 Aktive Netzwerkkomponenten

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

16.5.6 Mobile IT-Systeme

Es MUSS eine Vorgehensweise für die Datensicherung von mobilen IT-Systemen vorhandenen Daten von einem Administrator vorgegeben werden.

16.6 Zusätzliche Maßnahmen für kritische IT-Systeme

16.6.1 Datensicherung

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

16.6.2 Risikoanalyse

Im Zuge der Risikoanalyse und -behandlung (siehe Abschnitt 10.6.2) MÜSSEN die Folgen eines Datenverlusts analysiert und dabei der MTD bestimmt werden.

16.6.3 Verfahren

Die Verfahren zur Datensicherung und -wiederherstellung MÜSSEN in Ergänzung zu Abschnitt 16.4 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 10.6.10).

17 Sicherheitsvorfälle

17.1 Vorbereitung auf Sicherheitsvorfälle

Eine angemessene Reaktion auf Sicherheitsvorfälle ermöglicht es, den Regelbetrieb zügig wieder aufzunehmen und so Schäden zu minimieren. Deshalb ist es notwendig, angemessen auf Sicherheitsvorfälle vorbereitet zu sein.

Zu diesem Zweck SOLLTE die Organisation ein Business Continuity Management (BCM) auf Basis eines anerkannten Standards wie BSI-Standard 200-4 oder DIN EN ISO 22301 implementieren.

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

17.2 IS-Richtlinie

In Ergänzung zu Abschnitt 6.4 MÜSSEN in einer IS-Richtlinie Regelungen für den Umgang mit Sicherheitsvorfällen getroffen werden:

1. Der Begriff *Sicherheitsvorfall* wird klar definiert.

   Es SOLLTE beschrieben werden, welche Ereignisse oder Auffälligkeiten dazu führen, dass ein Vorfall als Sicherheitsvorfall eingestuft wird.

2. Jeder Mitarbeiter meldet mögliche Sicherheitsvorfälle über die dafür vorgesehenen Meldewege.

3. Administratoren untersuchen, ggf. in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, dem IT-Verantwortlichen und dem ISB, Sicherheitsvorfälle vordringlich.
4. Es wird definiert, in welchen Fällen das Topmanagement über Sicherheitsvorfälle informiert wird.
5. Es wird definiert, wie die Organisation intern und extern akute und bewältigte Sicherheitsvorfälle kommuniziert.

17.3 Erkennen

Es SOLLTEN Maßnahmen implementiert werden, die es ermöglichen, Sicherheitsvorfälle zu erkennen, wie z. B.:

1. Systeme zum Erkennen und Verhindern von Angriffen (host- oder netzwerkbasierte IDS/IDP-Systeme)
2. Systeme zur Isolation und Analyse potenziell schädlicher Software (Sandboxing-Technologien)
3. Integritätsprüfungen auf Prüfsummenbasis
4. Sensor-Systeme (Honeypots)
5. Überwachen der Zugriffe auf besonders sensible Informationen
6. Erfassen und Auswerten von Logmeldungen

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

17.4 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 Sicherheitsvorfall und der Schaden werden so dokumentiert, dass die Organisation ihre Informationspflichten erfüllen kann.
5. Entsprechende Stellen wie Versicherungen und Aufsichtsbehörden werden zeitnah informiert.
6. Beweismittel werden gesichert.
7. Der Schaden wird behoben und der Regelbetrieb wieder aufgenommen.
8. 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.

17.5 Zusätzliche Maßnahmen für kritische IT-Systeme

17.5.1 Anforderungen

Die folgenden Maßnahmen MÜSSEN zusätzlich zu allen zuvor in diesem Kapitel genannten Punkten für alle kritischen IT-Systeme umgesetzt werden.

17.5.2 Wiederanlaufpläne

Für jedes kritische IT-System MUSS ein Verfahren (siehe Anhang A.1) für den Wiederanlauf implementiert werden (Wiederanlaufplan), das folgende Anforderungen erfüllt:

1. Das Verfahren enthält alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, das IT-System innerhalb seiner MTA soweit wiederherzustellen, dass zumindest das Notbetriebsniveau (siehe Abschnitt 10.6.3) erreicht ist.
2. Wenn das IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, enthält das Verfahren alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, die entsprechenden Ersatzsysteme oder -verfahren (siehe Abschnitt 10.6.10) so weit in Betrieb zu nehmen, dass die vom IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenpotential betrieben werden können.
3. Das Verfahren enthält eine Aufstellung der für die Wiederherstellung zwingend benötigten Ressourcen, wie z. B. Mitarbeiter und deren Kontaktdaten, Hardware, Software, Netzwerke, Dienste, Authentifizierungsmerkmale, kryptografische Schlüssel und Lizenzinformationen.
4. Es ist verständlich und übersichtlich strukturiert.
5. Es kann im Bedarfsfall schnell aktiviert werden.
6. Es wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.

17.5.3 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.

Anhang A Verfahren und Risikomanagement

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.
7. *Zusätzlich SOLLTE definiert werden, wer für die Etablierung des Verfahrens 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.

Es KÖNNEN mehrere Vorgehensweisen in einem Verfahren definiert werden, sofern sie sich ähneln oder logisch zusammengefasst werden können.

Die Prüfung der Umsetzung, Angemessenheit und Effektivität derartiger Verfahren KANN durch eine stichprobenartige Prüfung einzelner Vorgehensweisen erfolgen.

A.2 Risikomanagement

A.2.1 Definitionen und Analysen

Die Organisation MUSS die in diesen Richtlinien geforderten Risikoidentifikationen und 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.2.2 Methodik

Die Vorgehensweisen für die Risikoidentifikation, -analyse und -behandlung MÜSSEN festgelegt sein.

Die Vorgehensweisen MÜSSEN so gewählt sein, dass sie zu reproduzierbaren und schlüssigen Ergebnissen führen.

Die Auswahl der Vorgehensweisen SOLLTE auf Basis eines anerkannten Standards wie z. B. ISO 31010 erfolgen.

A.2.3 Risikoidentifikation

Jede Risikoidentifikation MUSS folgende Anforderungen erfüllen:

1. Ihre Durchführung und ihre Ergebnisse werden dokumentiert.
2. Ihre Vorgehensweise gewährleistet, dass umfassend nach möglichen Bedrohungen und Schwachstellen gesucht wird.

Hierzu SOLLTEN entsprechende Kataloge wie z. B. ENISA Thread Taxonomy, der Annex der ISO 27005 oder die Aufstellung Elementare Gefährdungen *des BSI berücksichtigt werden.*

A.2.4 Risikoanalyse

Jede Risikoanalyse MUSS folgende Anforderungen erfüllen:

1. Ihre Durchführung und ihre Ergebnisse werden dokumentiert.
2. Die Bewertung der Risiken erfolgt auf Basis der potenziellen Schäden und deren Eintrittswahrscheinlichkeit anhand einheitlicher, zuvor festgelegter Kriterien.
3. Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.

A.2.5 Risikobehandlung

Identifizierte Risiken MÜSSEN zeitnah und priorisiert behandelt werden.

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

Die Umsetzung der entsprechenden Maßnahmen MUSS kontrolliert und auf Wirksamkeit geprüft werden.

Risiken KÖNNEN generell akzeptiert werden, wenn ihre Schadenhöhen und/oder Eintrittswahrscheinlichkeiten unterhalb einer einheitlichen, zuvor definierten Grenze liegen (Risikoakzeptanzgrenze).

Wenn erhebliche Risiken nicht angemessen behandelt werden können, MÜSSEN sie vom Topmanagement akzeptiert werden.

Die Akzeptanz von erheblichen Risiken durch das Topmanagement MUSS dokumentiert werden.

A.2.6 Wiederholung und Anpassung

Risikoidentifikationen, -analysen und -behandlungen MÜSSEN jährlich auf ihre Aktualität geprüft und bei Bedarf wiederholt werden.

Sie MÜSSEN darüber hinaus zeitnah überarbeitet werden, wenn eine der folgenden Faktoren auftritt:

1. Der untersuchte Gegenstand hat sich wesentlich verändert (z. B. Hardware, Software oder Konfiguration eines IT-Systems).
2. Der Einsatzzweck des untersuchten Gegenstands hat sich wesentlich geändert.
3. Neue Bedrohungen, neue Schwachstellen und/oder neue gesetzliche, betriebliche oder vertragliche Anforderungen wurden bekannt.

Anhang B Änderungen zur Vorversion

Gegenüber Vorversion VdS 10000 : 2018-12 (02) wurden folgende Änderungen vorgenommen:

- redaktionelle Änderungen

Kapitel 1 (Allgemeines)

- 1.1 Anwendungshinweise: Verweis auf die VdS-Richtlinien 10100 aufgenommen.
- 1.2 Anwendungs- und Geltungsbereich: Kommunen explizit in den Anwendungsbereich aufgenommen, Geltungsbereich klarer gefasst

Kapitel 2 (Normative Verweise)

- Aktualisierung der Verweise (BSI-Standard 200-2)
- neue Verweise aufgenommen („Elementare Gefährdungen“ des BSI sowie „ENISA Thread Taxonomy“)

Kapitel 3 (Begriffe)

- nicht mehr genutzte Begriffe gestrichen (z. B. „Archivierung“)
- Begriff „Eigenmächtigkeit“ ergänzt
- Begriffe redaktionell überarbeitet

Kapitel 4 (Organisation der Informationssicherheit)

- 4.4 Informationssicherheitsbeauftragter: Bestellung des ISB aufgenommen
- 4.5 Informationssicherheitsteam: Bestellung des ISB aufgenommen

Kapitel 5 (Leitlinie zur Informationssicherheit)

- 5.2 Allgemeine Anforderungen: Verpflichtung zur initialen Veröffentlichung aufgenommen

Kapitel 6 (Richtlinien zu Informationssicherheit)

- 6.2 Allgemeine Anforderungen: Verpflichtung zur initialen Veröffentlichung aufgenommen
- 6.4 Aufbau und Funktionsweise des ISMS: Abschnitt neu aufgenommen
- 6.5 Regelungen für Nutzer: Anforderungen für Installation, Nutzung oder Betreiben von Hard- und Software vereinfacht

Kapitel 7 (Mitarbeiter)

- 7.3 Aufnahme der Tätigkeit: physische Zugangsmittel wie Schlüssel und Transponder berücksichtigt
- 7.4 Beendigung oder Wechsel der Tätigkeit: physische Zugangsmittel wie Schlüssel und Transponder berücksichtigt

Kapitel 8 (Wissen)

- 8.2 Aktualität des Wissens: klarer formuliert, interner Austausch über betriebliche und vertragliche Anforderungen an die Informationssicherheit aufgenommen

Kapitel 10 (IT-Systeme)

- 10.4.2 Software: Sicherheitsupdates müssen in Betrieb genommen werden.
- 10.4.3 Beschränkung des Netzwerkverkehrs: Empfehlung ergänzt (wichtige oder sicherheitskritische Funktionen)
- 10.4.4 Protokollierung: allgemeiner gefasst
- 10.4.6 Schadsoftware: Echtzeitschutz als MUSS-Kriterium aufgenommen
- 10.4.9 Zugänge und Zugriffe: Empfehlung zu „Least-Functionality“ aufgenommen
- 10.6.7 Dokumentation: Empfehlung aufgenommen, eine unvollständige oder falsche Dokumentation bei kritischen IT-Systemen als Sicherheitsvorfall zu behandeln

Kapitel 11 (Netzwerke und Verbindungen)

- 11.5.3 Segmentierung: Aufstellen von Kriterien aufgenommen
- 11.5.4 Fernzugang: Mehr-Faktor-Authentifizierung als Basisschutz aufgenommen

Kapitel 14 (IT-Outsourcing und Cloud Computing)

- 14.3 Vorbereitung: klarer gefasst
- 14.4 Vertragsgestaltung: klarer gefasst
- 14.5 Zusätzliche Maßnahmen für kritische IT-Ressourcen: sämtliche Änderungen bei vertraglichen Regelungen müssen schriftlich dokumentiert und gemeldet werden

Kapitel 15 (Zugänge, Zugriffs- und Zutrittsrechte)

- 15.2 Verwaltung: Zutrittsrechte aufgenommen
- 15.3 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen: Prüfung der Zutrittsrechte aufgenommen

Kapitel 16 (Datensicherung und Archivierung)

- ehem. 16.1 Archivierung: gestrichen
- 16.3 Verfahren: Anforderungen an die Datensicherung überarbeitet
- 16.5.2 IT-Systeme für die Datensicherung und -wiederherstellung: hinzugefügt

Kapitel 17 (Störungen und Ausfälle) und Kapitel 18 (Sicherheitsvorfälle)

- zusammengefasst zu Kapitel 17 (Sicherheitsvorfälle)
- 17.4 Reaktion: Dokumentation und Informieren von Versicherungen und Aufsichtsbehörden neu aufgenommen

Anhang A.1 (Verfahren)

- Empfehlung ergänzt (Verantwortlichkeit für die Etablierung eines Verfahrens)
- Mehrere Vorgehensweisen können in einem Verfahren zusammengefasst werden, um die Prüfaufwand zu verringern

Anhang A.2 (Risikomanagement)

- Überarbeitet und klarer gefasst
- Anhang A.2.2 Methodik: neu aufgenommen
- Anhang A.2.3 Risikoidentifikation: neu aufgenommen
- Anhang A.2.4 Risikobehandlung: Risikoakzeptanzgrenze aufgenommen
- Anhang A.2.5 Akzeptanz von erheblichen Risiken durch das Topmanagement klarer gefasst
- Anhang A.2.6 Risikoidentifikationen, -analysen und -behandlungen klarer gefasst