VdS-Richtlinien für die Informationsverarbeitung

Strukturierte Informationssicherheit gemäß NIS-2

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

Mit den gesetzlichen Regelungen zu NIS-2 geht eine erweiterte Reichweite des Anwendungsbereichs sowie deutlich erhöhte Anforderungen gegenüber bisherigen Regelungen zur Informationssicherheit einher. In der Folge sind zahlreiche Organisationen mit neuen und deutlich anspruchsvolleren Verpflichtungen im Bereich der Informationssicherheit konfrontiert.

Die vorliegenden Richtlinien definieren Mindestanforderungen und beschreiben eine Basis für die strukturierte Umsetzung von Informationssicherheitsmaßnahmen im Sinne von NIS-2, wobei weitergehende oder einzelfallbezogene Anforderungen unberührt bleiben.

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* Informationssicherheitsmanagementsystem für Industrielle Automatisierungssysteme*, VdS 10020 implementiert werden.*

1.3 Anwendungs- und Geltungsbereich

Diese Richtlinien KÖNNEN für alle Organisationen, Verwaltungen und Verbände anwendet werden, insbesondere für jene, die als „wichtige“ oder „besonders wichtige“ Einrichtungen im Sinne von NIS-2 gelten.

Die Richtlinien DÜRFEN NICHT als ausreichend für die Umsetzung der Anforderungen an Betreiber kritischer Infrastrukturen gemäß BSI-Gesetz (BSIG n.F.) und der BSI-Kritisverordnung angesehen werden.

Sie KÖNNEN aber als Basis für eine entsprechende Umsetzung dienen.

Die Organisation MUSS prüfen, ob sie zur Umsetzung weiterer Maßnahmen z. B. aufgrund bestehender Durchführungsrechtsakte der Europäischen Kommission wie der Durchführungsverordnung (EU) 2024/2690 oder aufgrund anderer gesetzlicher, vertraglicher oder betrieblicher Anforderungen verpflichtet ist.

Diese Richtlinien MÜSSEN organisationsweit und ohne Einschränkung auf Teilbereiche angewendet werden.

1.3.1 Analyse und Registrierung

Es MUSS ein Verfahren (siehe Anhang A.1) etabliert werden, das die folgenden Anforderungen erfüllt:

1. Es wird geprüft, ob die Organisation als „wichtige“ oder „besonders wichtige“ Einrichtung im Sinne von § 28 BSIG n.F. gilt.

   Hierzu SOLLTE u. a. die entsprechende vom BSI zur Verfügung gestellte Betroffenheitsprüfung genutzt werden.

2. Das Ergebnis der Prüfung wird zusammen mit seiner Begründung dokumentiert.
3. Es wird jährlich auf seine Aktualität geprüft und bei Bedarf die Prüfung wiederholt.

Das Verfahren MUSS sicherstellen, dass bei positiver Prüfung folgende Anforderungen erfüllt werden:

1. Das Registrierungsverfahren gem. § 33 BSIG n.F. wird bei Bedarf durchlaufen und dabei die dort gesetzten Fristen eingehalten.
2. Die vom BSI veröffentlichten Einzelheiten zur Ausgestaltung des Registrierungsverfahrens werden beachtet.
3. Es wird geprüft, ob die Organisation eine Einrichtung im Sinne von § 60 Absatz 1 Satz 1 BSIG n.F. ist.
4. Bei positiver Prüfung werden die in § 34 BSIG n.F. geforderten Informationen über den dafür vorgesehenen Meldeweg an das BSI übermittelt und dabei die in § 33 BSIG n.F. gesetzten Fristen eingehalten.

1.4 Gültigkeit

Diese Richtlinien gelten ab dem <FIXME>.<FIXME>.2026.

2 Verweise

2.1 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 letzte Fassung.

BSI-Standard 200-2	IT-Grundschutz-Methodik
BSI-Standard 200-3	Risikomanagement
BSI-Standard 200-4	Business Continuity Management
Common Criteria / ISO 15408	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security
DIN EN 1047-1	Wertbehältnisse – Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand - Teil 1: Datensicherungsschränke und Diskettenteneinsätze
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
FIPS 140-3	Security Requirements for Cryptographic Modules
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
NIS-2-Geschäftsleitungsschulung	Dokument „NIS-2-Geschäftsleitungsschulung“ des BSI
TR-02102	Technische Richtlinie 02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
VdS 2007	Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen
VdS 10000	Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU)
VdS 10003	Richtlinien für die Anerkennung von Beratern für Cyber-Security
VdS 10005	Mindestanforderungen an die Informationssicherheit von Klein- und Kleinstunternehmen
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

2.2 Verweise auf Gesetzestexte

Diese Richtlinien enthalten Verweise auf Gesetzestexte.

(EU) 2024/2690	Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024
BSIG n.F.	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik in der durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) neu gefassten Version
NIS-2	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148

3 Begriffe und Abkürzungen

3.1 Begriffe

administrativer Zugang: Zugang, der dazu befähigt, Einstellungen zu tätigen, die andere Nutzer oder das IT-System selbst betreffen

administrative Tätigkeit: ändern von Einstellungen, die andere Nutzer oder das IT-System selbst betreffen

Administrator: für Einrichtung, Betrieb, Überwachung und/oder Wartung eines IT-Systems, einer Software oder einer IT-Infrastruktur zuständige Person

aktive Netzwerkkomponente: über eine eigene Logik wie z. B. Hub, Switch, Router, 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.

Beschaffung: geplante und geregelte Tätigkeiten, die darauf gerichtet sind, notwendige Ressourcen von extern zu erlangen und bereitzustellen

Business Continuity Management (BCM): ganzheitlicher Managementprozess für die systematische Vorbereitung auf das Bewältigen von Schadenereignissen mit dem Ziel, zentrale Geschäftsprozesse auch bei Sicherheitsvorfällen und Krisen 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

Erheblicher Sicherheitsvorfall: Sicherheitsvorfall, der schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die Organisation verursachen oder Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigen kann

externe IT-Ressource: IT-Ressource, die von externen Stellen wie z. B. Lieferanten, Partnern oder Verbänden eingekauft oder zur Verfügung gestellt wird

Beispiele: Typische externe IT-Ressourcen sind z. B. eingekaufte oder gehostete Hard- und Software, Clouds, IT-Dienstleistungen oder traditionelle Dienste wie DNS und Domains.

externe Person: natürliche Person, die kein Mitarbeiter ist

Hinweis: Dies können z. B. Geschäftspartner oder Gäste sein.

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 das Maß an Vertraulichkeit, Verfügbarkeit und/oder Integrität.

Informationssicherheitsbeauftragter (ISB): Prozesseigentümer des Informationssicherheitsmanagementsystems (ISMS)

Informationssicherheitsteam (IST): unterstützendes Gremium für die Aufrechterhaltung und Weiterentwicklung der Informationssicherheit

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 für die Informationssicherheit

IS-Richtlinie: Richtlinie für die Informationssicherheit

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

IT-Krise: Krise, die die Informationsverarbeitung betrifft oder die von der Informationsverarbeitung verursacht ist

IT-Ressource: materielle oder immaterielle Mittel für die Informationsverarbeitung wie z. B. IT-Infrastrukturen, IT-Systeme, Datenträger, Verbindungen, Daten, Informationen oder Anwendungen

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

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, Smartphones, Telefonanlagen, Laptops, Tablets und aktive Netzwerkkomponenten aber auch Steuerungsanlagen von Maschinen und Prozessen

katastrophaler Schaden: Schaden mit 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.

Krise: vom Normalzustand abweichende Situation mit dem Potenzial für oder mit bereits eingetretenen Schäden, die mit der normalen Aufbau- und Ablauforganisation nicht mehr bewältigt werden kann

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

kritische Informationen: Informationen, bei denen der Bruch der Informationssicherheit zu einem katastrophale Schaden führen kann

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, auf dem kritische Informationen gespeichert sind

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

Lieferant: Organisation oder Person, die externe IT-Ressourcen liefert bzw. bereitstellt.

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

Nutzer: alle juristischen und natürlichen Personen, die Zugang zur IT besitzen

Nutzung: Gebrauch einer bereits vorhandenen oder frei zugänglichen Ressource ohne vorherige Beschaffung

Organisation: eine rechtlich verfasste Einheit wie ein Unternehmen, eine Behörde oder eine Institution, die strukturiert ist, um bestimmte Ziele zu verfolgen; entspricht dem Begriff „Einrichtung“ von NIS-2

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

Projekt: zielgerichtetes, zeitlich befristetes Vorhaben, das z. B. aufgrund seiner Komplexität oder Bedeutung ein Projektmanagement erfordert

Hinweis: typische Projekte sind z. B. Produktentwicklungs-, (Re-)Organisations-, IT-, Sanierungs- oder Bauprojekte sowie die langfristige Erbringung von IT-Dienstleistungen

Projektverantwortlicher: für das Projektmanagement (die Planung, Steuerung und Überwachung) eines Projekts verantwortliche Person

Prozess: eine strukturierte Gruppe verbundener Aktivitäten, die zusammen ein Resultat erzeugen

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: IT-System, das Dienste über Verbindungen zur Verfügung stellt

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 stationären IT-Systemen), 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 oder verbindlich vorgegebene Qualitätsparameter, 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 Schadenpotenzial, unverzichtbar ist

Hinweis: Dies können z. B. Produktionsanlagen, Wissen, Mitarbeiter sowie das Vertrauen von Kunden und Geschäftspartnern sein.

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

BIA Business Impact Analyse

BSI Bundesamt für Sicherheit in der Informationstechnik

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, entsprechende organisatorische Strukturen zu etablieren.

4.2 Verantwortlichkeiten

4.2.1 Anforderungen

Verantwortlichkeiten (siehe Abschnitte 4.3 bis 4.13) 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, insbesondere gem. § 38 BSIG n.F. für die Umsetzung und Überwachung des Risikomanagements und der Maßnahmen für die Informationssicherheit
2. Inkraftsetzung 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.

Der ISB SOLLTE direkt dem Topmanagement unterstellt sein.

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 geänderte Bedrohungen, geänderte Schwachstellen und an geänderte 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. IT-Krisenmanager
5. Mitarbeiter (z. B. über Betriebsrat)
6. 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-Krisenmanager

Das Topmanagement MUSS einen IT-Krisenmanager bestellen.

Dieser MUSS im Fall einer IT-Krise die folgenden Verantwortlichkeiten wahrnehmen:

1. Leitung des IT-Krisenmanagements, insbesondere das Koordinieren der notwendigen Maßnahmen zur Bewältigung der IT-Krise
2. Berichten an das Topmanagement
3. Nachbereitung der Bewältigung der IT-Krise

4.7 IT-Krisenstab

Das Topmanagement MUSS einen IT-Krisenstab bestellen.

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

1. Topmanagement
2. IT-Krisenmanager
3. ISB
4. IT-Verantwortliche
5. Prozesseigentümer der zentralen Prozesse und der Prozesse mit hohem Schadenpotential

Der IT-Krisenstab MUSS den IT-Krisenmanager unterstützen, insbesondere beim Bewerten der Lage in einer IT-Krise sowie dem organisationsweiten Steuern und Koordinieren der Maßnahmen zu deren Bewältigung.

4.8 IT-Verantwortliche

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

IT-Verantwortliche MÜSSEN alle Maßnahmen, sowie deren Planung, Koordination und Umsetzung, mit dem ISB abstimmen, die zur Verbesserung und Erhaltung der Informationssicherheit in ihrem Verantwortungsbereich ergriffen werden müssen.

4.9 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.

4.10 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.

4.11 Mitarbeiter

Mitarbeiter MÜSSEN folgende Aufgaben wahrnehmen:

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

4.12 Projektverantwortliche

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

4.13 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 Informationstechnik (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 Fassung 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 4.13) 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 der Organisation.
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 der kontinuierlichen Verbesserung und Anpassung 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
   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. Hard- und Software wird nicht eigenmächtig in der IT-Infrastruktur installiert, genutzt oder betrieben.
   b. Im Internet angebotene Dienste werden nicht eigenmächtig genutzt.
   c. Netzübergänge (wie z. B. Zugänge zum Internet, Fernwartungszugänge oder VPN-Verbindungen) werden nicht eigenmächtig installiert; es werden ausschließlich die von der Organisation bereitgestellten Netzübergänge genutzt.
   d. Die in der IT-Infrastruktur installierten Sicherheitseinrichtungen werden nicht eigenmächtig deinstalliert, deaktiviert oder in ihrer Konfiguration verändert bzw. mutwillig umgangen.
   e. 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.
   b. Informationen der Organisation werden nicht eigenmächtig an Dritte weitergegeben oder öffentlich zugänglich gemacht.
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 Kapitel 12)

3. Beschaffung von IT-Ressourcen (siehe Kapitel 14)
4. Speicherorte (siehe Kapitel 16)
5. Sicherheitsvorfälle (siehe Kapitel 17)
6. IT-Krisen (siehe Kapitel 18)

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 Authentifizierungsmerkmale wie Schlüssel, Transponder, Zertifikate 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 von Authentifizierungsmerkmalen wie Schlüssel, Transponder, Zertifikate 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.

   Hierzu SOLLTE u. a. die Online-Plattform des BSI zum Informationsaustausch mit anderen von NIS-2 betroffenen Organisationen genutzt werden.
3. Es findet in der Organisation ein regelmäßiger Austausch über die aktuellen gesetzlichen, 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.

8.3 Schulung und Sensibilisierung

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

1. Schulungs- und Sensibilisierungsmaßnahmen 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

Zusätzlich MUSS das Verfahren sicherstellen, dass das Topmanagement alle drei Jahre sowie bei Bedarf an speziellen Schulungen teilnimmt.

Diese Schulungen MÜSSEN ausreichende Kenntnisse und Fähigkeiten im Bereich der Informationssicherheit vermitteln, damit das Topmanagement seine gesetzliche Verantwortung gem. § 38 BSIG n.F. für die Umsetzung und Überwachung des Risikomanagements und der Maßnahmen für die Informationssicherheit nachkommen kann.

Die Inhalte der Schulung SOLLTEN sich an den Vorgaben im Dokument „NIS-2-Geschäftsleitungsschulung" des BSI orientieren.

Die Inhalte aller Schulungen und die Teilnahme an ihnen MÜSSEN dokumentiert werden.

9 Schutzkategorien

9.1 Grundlagen

Die Organisation MUSS ihre IT-Ressourcen (insbesondere ihre IT-Systeme, mobilen Datenträger, Verbindungen, Individualsoftware und ihre externen IT-Ressourcen) in die Schutzkategorien „nachrangig", „standard", „wichtig" und „kritisch" einteilen:

1. IT-Ressourcen der Schutzkategorie „nachrangig" sind IT-Ressourcen, bei denen ein Sicherheitsvorfall nur zu einem vernachlässigbaren Schaden führen kann (siehe Anhang A.2.5) und die von der restlichen IT-Infrastruktur getrennt oder umfassend abgeschottet sind.
2. IT-Ressourcen der Schutzkategorie „standard" sind alle IT-Ressourcen, die nicht nachrangig sind.
3. IT-Ressourcen der Schutzkategorie „wichtig" sind IT-Ressourcen, die für den Betrieb eines zentralen Prozesses oder eines Prozesses mit hohem Schadenpotential (siehe Abschnitt 9.2) zwingend benötigt werden. Sie sind eine Untermenge der IT-Ressourcen der Schutzkategorie „standard".
4. IT-Ressourcen der Schutzkategorie „kritisch" sind IT-Ressourcen, die kritische Informationen (siehe Abschnitt 9.4) verarbeiten, speichern oder übertragen oder die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden. Sie sind eine Untermenge der Schutzkategorie „wichtig".

Die Organisation MUSS jährlich prüfen, ob die Einteilung aktuell und vollständig ist und sie bei Bedarf anpassen.

Hierfür KANN ein Top-Down-Ansatz (prozessorientierte Sicht), ein Bottom-Up-Ansatz (systemorientierte Sicht) oder eine Mischung aus beiden verwendet werden; eine Mischung aus beiden Ansätzen bietet die Möglichkeit, IT-Ressourcen zuverlässig einer Kategorie zuzuordnen.

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 der folgenden 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 Wichtige IT-Ressourcen

Die Organisation MUSS ihre wichtigen IT-Ressourcen ermitteln und dokumentieren.

Dies SOLLTE mit einer Business Impact Analyse (BIA) gemäß eines anerkannten Standards wie z. B. ISO 22301 oder BSI-Standard 200-4 durchgeführt werden.

Die Dokumentation MUSS folgende Anforderungen erfüllen:

1. Sie enthält eine kurze Beschreibung der wichtigen IT-Ressource.
2. Sie begründet, warum die IT-Ressource wichtig ist.
3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der IT-Ressource.
4. Sie benennt, wer für die IT-Ressource verantwortlich ist.

Die MTA 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 wichtigen IT-Ressource direkt oder indirekt abhängig sind.

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

9.4 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.

9.5 Kritische IT-Ressourcen

Die Organisation MUSS ihre kritischen IT-Ressourcen dokumentieren.

Hierfür MÜSSEN die kritischen Informationen (siehe Abschnitt 9.4) untersucht 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.

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

9.6 Weitere Schutzkategorien

Die Organisation SOLLTE prüfen, ob es notwendig oder sinnvoll ist, weitere Kategorien von IT-Ressourcen zu definieren, diese zyklisch oder fortlaufend zu erfassen und sie mit individuell abgestimmten technischen und organisatorischen Maßnahmen abzusichern.

10 IT-Systeme

10.1 Grundlagen

Informationsverarbeitung geschieht heute 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 10.3.1 und 10.3.2) 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
4. Schutzkategorie (siehe Kapitel 9)

Darüber hinaus SOLLTEN für jedes IT-System weitere Informationen erhoben und aktuell gehalten werden, wie z. B. Ansprechpartner, 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 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. Die Schutzkategorie des IT-Systems wird ermittelt bzw. seine Schutzkategorie überprüft (siehe Kapitel 9).
2. Die Maßnahmen der entsprechenden Schutzkategorie werden für das IT-System 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.

10.3.2 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.
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 der Schutzkategorie „standard“ und höher 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).
3. Es handelt sich um IT-Systeme, für die die Organisation keinen administrativen Zugang besitzt.

Zusätzlich SOLLTE durch die Beschränkung des Netzwerkverkehrs sichergestellt werden, dass administrative Tätigkeiten über das Netzwerk nur von festgelegten IT-Systemen bzw. Netzwerkbereichen aus möglich sind.

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 und/oder heuristische Erkennung).

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

Erkannte Schadsoftware SOLLTE als Sicherheitsvorfall (siehe Kapitel 17) behandelt werden.

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 Firmware-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.

   Das systematische Ausprobieren von Anmeldeinformationen aus der IT-Infrastruktur der Organisation heraus SOLLTE als Sicherheitsvorfall (siehe Kapitel 17) behandelt werden.

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 ausschließlich Mehr-Faktor-Authentifizierungen verwendet oder die Identität des Nutzers wird auch nach seiner Anmeldung zyklisch bzw. fortlaufend überprüft und bei auffälligem Verhalten der Zugriff eingeschränkt, eine erneute Authentifizierung verlangt oder der Zugriff wird beendet (kontinuierliche Authentifizierung).

3. Es werden keine trivialen Authentifizierungsmerkmale (z. B. Standard-Passwörter oder einfach zu erratende Passwörter) verwendet.

10.4.9 Zugänge und Zugriffe

Für jeden Zugang SOLLTEN folgende Anforderungen erfüllt werden:

1. *Über ihn kann nur auf Informationen lesend zugegriffen werden, wenn dies für die Aufgabenerfüllung notwendig ist („Need-to-Know“).*

2. *Über ihn kann nur auf Informationen schreibend zugegriffen werden, wenn dies für die Aufgabenerfüllung notwendig ist („Least-Privileges“).*

3. *Über ihn können nur jene Funktionen genutzt werden, die für die Aufgabenerfüllung benötigt werden („Least-Functionality“).*

10.4.10 Administrative Zugänge

Administrative Tätigkeiten MÜSSEN über die speziell dafür vorgesehenen Zugänge erfolgen.

Diese DÜRFEN NICHT für die alltägliche Nutzung verwendet werden.

Für administrative Zugänge MÜSSEN folgende Anforderungen erfüllt werden:

1. Die Anzahl der administrativen Zugänge ist auf das für den Betrieb notwendige Minimum reduziert.
2. Administrative Zugänge verfügen über ein eigenes, exklusives Authentifizierungsmerkmal.
3. Es wird definiert, für welchen Aufgabenbereich ein administrativer Zugang genutzt wird.
4. Es werden stets die administrativen Zugänge mit den geringstmöglichen Privilegien genutzt.

Zusätzlich SOLLTEN Zugänge für die Administration von IT-Systemen einer Schutzkategorie nicht für die Administration von IT-Systemen höherer Schutzkategorien gültig sein.

10.5 Zusätzliche Maßnahmen für mobile IT-Systeme

10.5.1 Grundlagen

Mobile IT-Systeme sind in besonderer Weise Gefährdungen wie z. B. 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 mobilen IT-Systemen von den Nutzern installiert werden darf.
6. Es wird definiert, ob und unter welchen Bedingungen ein Administrator mobile IT-Systeme orten darf.
7. Es wird definiert, ob und unter welchen Bedingungen ein Administrator die auf mobilen IT-Systemen gespeicherten Informationen aus der Ferne löschen darf.

10.5.3 Schutz der Informationen

Die auf den mobilen IT-Systemen gespeicherten Informationen der Organisation MÜSSEN vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

Es MUSS mit Hilfe einer Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) festgelegt werden, welche Informationen auf mobilen IT-Systemen durch kryptografische Maßnahmen geschützt 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 wichtige IT-Systeme

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

Dabei KÖNNEN wichtige IT-Systeme in Gruppen zusammengefasst werden, wenn sie sich in Hard- und Software ähneln und für ähnliche Zwecke eingesetzt werden.

Zusätzlich MÜSSEN für alle wichtigen IT-Systeme die Maßnahmen der folgenden Abschnitte umgesetzt werden.

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

10.6.1 Dokumentation

Für jedes wichtige IT-System MUSS eine Dokumentation der administrativen Tätigkeiten 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.

10.6.2 Notbetriebsniveau

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

10.6.3 Überwachung

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

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

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

10.6.4 Beschränkung des Netzwerkverkehrs

Der Netzwerkverkehr von und zu wichtigen IT-Systemen SOLLTE 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.

10.6.5 Robustheit

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

10.6.6 Kryptografische Maßnahmen

Im Zuge der Risikoidentifizierung, -analyse und -behandlung (siehe Abschnitt 10.7.1) MUSS festgelegt werden, welche Informationen auf wichtigen IT-Systemen durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

10.6.7 Änderungsmanagement

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

Für wichtige 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 10.6.8).

10.6.8 Ersatzsysteme und -verfahren

Wenn ein wichtiges IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, MUSS die Organisation über ein Ersatzsystem oder -verfahren verfügen, das es ermöglicht, die vom wichtigen IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenpotential weiter zu betreiben.

Das Ersatzsystem oder -verfahren SOLLTE das Notbetriebsniveau (siehe Abschnitt 10.6.2) des wichtigen IT-Systems sicherstellen.

10.6.9 Wichtige Individualsoftware

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

10.7 Zusätzliche Maßnahmen für kritische IT-Systeme

10.7.1 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).

10.7.2 Beschränkung des Netzwerkverkehrs

Der Netzwerkverkehr von und zu kritischen IT-Systemen MUSS 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.

10.7.3 Robustheit

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

10.7.4 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.

10.7.5 Änderungsmanagement

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

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. physikalische Medien der Verbindungen
2. logische Netzwerkstruktur
   a. Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken (siehe Abschnitt 11.4)
   b. Netzwerksegmente (siehe Abschnitt 11.5.3), deren Einsatzzweck und deren Verbindungen untereinander
   c. Fernzugänge (siehe Abschnitt 11.5.4)
   d. Netzwerkkopplungen (siehe Abschnitt 11.5.5)

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 Netzübergang 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.

Eine fehlerhafte Dokumentation oder eine fehlerhafte Umsetzung der angestrebten Verkehrsbeziehungen SOLLTE als Sicherheitsvorfall (siehe Kapitel 17) behandelt werden.

11.5 Basisschutz

11.5.1 Grundanforderungen

Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für alle Netzwerke der Schutzkategorie „standard“ und höher 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).

IT-Systeme einer Schutzkategorie MÜSSEN durch die Segmentierung möglichst umfassend von IT-Systemen anderer Schutzkategorien abgeschottet werden.

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.

   Dies KANN durch den Einsatz von kryptografischen Maßnahmen sichergestellt werden.

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 oder durch eine kontinuierliche Authentifizierung authentifiziert, um die Gefahr eines unberechtigten Zugangs zu verringern.

4. Fernzugriffe erfolgen zeitlich begrenzt und innerhalb festgelegter Zeitfenster.

5. Fernzugriffe werden protokolliert.

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.

Dies KANN durch den Einsatz von kryptografischen Maßnahmen sichergestellt werden.

11.6 Zusätzliche Maßnahmen für wichtige Verbindungen

Für alle wichtigen Verbindungen MUSS eine Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) etabliert werden in der folgende Bedrohungen berücksichtigt werden:

1. Ausfall
2. unsichere Protokolle
3. unzureichende Authentisierung der Kommunikationspartner
4. unberechtigte Nutzung

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 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.

12.3 Zusätzliche Maßnahmen für wichtige mobile Datenträger

Für alle wichtigen mobilen Datenträger MUSS eine Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) etabliert werden.

Dabei MUSS festgelegt werden, welche Informationen auf mobilen Datenträgern durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt 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 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.

13.4 Zusätzliche Maßnahmen für wichtige IT-Systeme

Im Zuge der Risikoidentifikation, -analyse und -behandlung (siehe Abschnitt 10.6) MÜSSEN für alle wichtigen IT-Systeme folgende Bedrohungen berücksichtigt 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
7. Sabotage

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

14 Externe IT-Ressourcen

14.1 Grundlagen

Wenn externe IT-Ressourcen beschafft werden, ist es notwendig, die Sicherheitsinteressen der Organisation angemessen zu berücksichtigen.

14.2 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 MÜSSEN in einer IS-Richtlinie die Bedingungen für die Beschaffung von IT-Ressourcen festgelegt werden.

14.3 Vertragsgestaltung

Es MUSS ein Vertrag mit dem Lieferanten geschlossen werden, der die externen IT-Ressourcen spezifiziert und den Lieferanten zur Erfüllung der vereinbarten Leistungen verpflichtet.

Zusätzlich SOLLTEN im Vertrag die folgenden Punkte mit dem Lieferanten vereinbart sein:

1. *Anforderungen an die Informationssicherheit der externen IT-Ressourcen*
2. *Mitwirkungspflichten des Lieferanten bei Vertragsauflösung, sowie bei seiner Geschäftsaufgabe oder Insolvenz, wie z. B. die vollständige Herausgabe von IT-Ressourcen der Organisation sowie die aktive Unterstützung des Migrationsprozesses durch den Lieferanten*
3. *Reaktions- und Servicezeiten*
4. *Garantiebedingungen*
5. *Zeitraum, über den die externen IT-Ressourcen mit Anpassungen und Fehlerkorrekturen versorgt werden und wie die Organisation über Schwachstellen und Updates informiert wird*
6. *Dokumentationspflichten*
7. *Verpflichtung des Lieferanten zur Einhaltung grundlegender Maßnahmen für die Informationssicherheit (z. B. gemäß VdS 10000 oder VdS 10005)*

Darüber hinaus SOLLTE sichergestellt sein, dass Ansprüche aus Vertragsverletzungen durchgesetzt werden können, auch wenn sich der Lieferant nicht im demselben Rechtsraum wie die Organisation befindet.

14.4 Zusätzliche Maßnahmen für wichtige externen IT-Ressourcen

14.4.1 Sicherheitsanforderungen

Wenn wichtige externe IT-Ressourcen für die Informationsverarbeitung beschafft werden, MÜSSEN die Anforderungen an deren Informationssicherheit im Rahmen einer Risikoidentifikation, -analyse und -behandlung (siehe Anhang A.2) ermittelt werden.

14.4.2 Vertragsgestaltung

Zusätzlich MÜSSEN folgende Punkte vertraglich geregelt werden:

1. Leistungen
   a. Die vom Lieferanten zu erbringenden Leistungen werden definiert und deren Messung und Überwachung werden vereinbart.
   b. Die Standorte, an denen Leistungen erbracht werden, werden festgelegt.
   c. Eine Beschreibung der Schnittstellen zwischen der IT-Infrastruktur der Organisation und den externen IT-Ressourcen wird definiert.
2. Sicherheitsmaßnahmen
   a. Es werden die Sicherheitsmaßnahmen vereinbart, die der Lieferant zur Erfüllung der Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität der externen IT-Ressourcen treffen muss.

      Dies KÖNNEN z. B. Risikomanagementmaßnahmen, Maßnahmen zur Bewältigung von Sicherheitsvorfällen, Patchmanagement, sowie die Berücksichtigung oder Implementierung von Sicherheitsmaßnahmen gemäß eines anerkannten Standards, die Durchführung von automatisierten oder händischen Sicherheitsuntersuchungen und/oder die Beachtung von grundsätzlichen Prinzipien wie Security by Design oder Security by Default sein.
3. Kommunikation

a. Die Ansprechpartner auf Seiten der Organisation und des Lieferanten werden benannt.

b. Eine Vertraulichkeitsvereinbarung wird getroffen.

c. Es wird vereinbart, ob und unter welchen Bedingungen der Lieferant dazu berechtigt ist, Daten an Dritte weiterzugeben.

d. Es wird eine Informationspflicht des Lieferanten bei Sicherheitsvorfällen, die die erbrachten Leistungen betreffen oder die sich auf die Sicherheit der IT-Ressourcen der Organisation auswirken können, vereinbart.

4. Leistungsänderungen und Vertragsauflösung

   a. Die Mitwirkungspflichten des Anbieters im Falle einer Vertragsauflösung oder Insolvenz werden vereinbart, wie z. B. die vollständige Herausgabe von IT-Ressourcen der Organisation sowie die aktive Unterstützung des Migrationsprozesses durch den Lieferanten.

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 Lieferant nicht im gleichen Rechtsraum wie die Organisation befindet.

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

Wenn einzelne Punkte nicht vereinbart werden können, MUSS dem dadurch entstehenden Risiko durch eine Risikoidentifizierung, -analyse und -behandlung (siehe Anhang A.2) begegnet werden.

14.4.3 Vorbereiten der Nutzung

Die Organisation MUSS auf die Nutzung der externen IT-Ressourcen vorbereitet werden:

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

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 in ihrer Gesamtheit folgende Punkte sicherstellen:

1. Die jeweiligen Vorgänge werden vor ihrer Umsetzung beantragt, geprüft und genehmigt.
2. Folgende Rechte werden nur genehmigt, wenn sie für die Aufgabenerfüllung notwendig sind:

   a. sämtliche Zugänge und Zugriffsrechte

   b. Zutrittsrechte zu Serverräumen, Server- oder Netzwerkschränken

   c. Zutrittsrechte zu kritischen IT-Systemen

3. Wenn ein Nutzer administrative Zugänge oder Zugriffsrechte oder Zutrittsrechte zu Serverräumen, Server- oder Netzwerkschränken sowie 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.

   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.
6. Die jeweiligen Vorgänge werden dokumentiert.

15.3 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen

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

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

16 Datensicherung und -wiederherstellung

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 Speicherorte

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.

   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 ist sichergestellt,

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, gemäß des Verfahrens 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).

Speicherorte, Server, aktive Netzwerkkomponenten und mobile IT-Systeme der Schutzkategorie „nachrangig“ KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes ausgenommen werden.

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:

1. Die IT-Systeme arbeiten autark und können auch bei einer Störung oder einem Ausfall der restlichen IT in Betrieb genommen und genutzt werden.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 ein eigenes, exklusives Authentifizierungsmerkmal oder sie nutzen eine Mehr-Faktor-Authentifizierung.
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 vorgegeben werden.

16.6 Zusätzliche Maßnahmen für wichtige IT-Systeme

16.6.1 Datensicherung

Jedes wichtige IT-System MUSS über eine Datensicherung verfügen, die in Ergänzung zu Abschnitt 16.5 die Anforderungen der folgenden Abschnitte erfüllt.

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

16.6.2 Risikomanagement

Im Zuge des Risikomanagements der wichtigen IT-Systeme (siehe Abschnitt 10.6) 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. Wichtige 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 10.6.8).

17 Sicherheitsvorfälle

17.1 Grundlagen

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. Die Begriffe *Sicherheitsvorfall* und „erheblicher Sicherheitsvorfall“ werden klar definiert.

Es SOLLTE beschrieben werden, welche Ereignisse oder Auffälligkeiten dazu führen, dass ein Vorfall als Sicherheitsvorfall bzw. als ein erheblicher Sicherheitsvorfall eingestuft und wann eine IT-Krise festgestellt wird (siehe Kapitel 18).

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

Die Organisation MUSS prüfen, welche Maßnahmen notwendig sind, um mögliche Sicherheitsvorfälle und Schwachstellen erkennen zu können.

Mögliche Maßnahmen zum Erkennen von Sicherheitsvorfällen und Schwachstellen KÖNNEN sein:

1. *Systeme zum Erkennen und Verhindern von Angriffen (host- oder netzwerkbasierte IDS/IPS-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*
7. *Durchführen von automatisierten oder händischen Untersuchungen der technischen und/oder organisatorischen Sicherheitsmaßnahmen (Audits, Penetrationstests oder Security Scans)*

Das Ergebnis der Prüfung MUSS zusammen mit seiner Begründung dokumentiert werden.

Das Erkennen von Sicherheitsvorfällen und Schwachstellen SOLLTE durch eine konstruktive Fehlerkultur und anonyme Meldewege gefördert werden.

17.4 Reaktion auf Sicherheitsvorfälle

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. Bei Bedarf werden Beweismittel gesichert.
7. Der Schaden wird behoben und der Regelbetrieb wieder aufgenommen.
8. Es findet eine Nachbereitung statt, bei der die Ursachen des Sicherheitsvorfalls ermittelt, die Bewältigung des Sicherheitsvorfalls bewertet und konkrete Verbesserungen erarbeitet werden.

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

Zusätzlich MUSS das Verfahren bei einem erheblichen Sicherheitsvorfall die folgenden Punkte sicherstellen:

1. Es stehen autarke Kommunikationswege für die interne und externe Kommunikation zur Verfügung, die auch bei einer Störung oder einem Ausfall der IT-Infrastruktur genutzt werden können.
2. Entsprechende interne Stellen (wie *z. B.* Topmanagement, Abteilungsleiter oder Prozesseigentümer) und entsprechende externe Stellen (wie *z. B.* Partner, Kunden, Versicherungen oder Aufsichtsbehörden) werden zeitnah informiert; entsprechende Adresslisten und Inhalte sind vorbereitet.
3. Einem Mitarbeiter mit der benötigten Fachkompetenz wird die Verantwortlichkeit zugeordnet, mit dem BSI zu kommunizieren.

   Diese Verantwortlichkeit KANN z. B. der ISB oder der Krisenmanager wahrnehmen.
4. Die Informationspflichten gem. § 32 BSIG n.F. (Erstmeldung, Bewertung des Sicherheitsvorfalls, Zwischenmeldungen auf Anfrage des BSI, ggf. Fortschrittsmeldungen und Abschlussmeldung) werden über das entsprechende Meldeverfahren des BSI erfüllt; die dabei verbindlichen Meldefristen werden eingehalten.
5. Auf Anweisung des BSI werden die Empfänger der betroffenen Dienste unverzüglich über den Sicherheitsvorfall unterrichtet; hierzu werden entsprechende Inhalte, Empfängerlisten und Kommunikationswege vorbereitet.
6. Fällt die Organisation unter § 35 Abs. 2 BSIG n.F., werden dem BSI und den Empfängern der betroffenen Dienste darüber hinaus Informationen über die Bedrohung selbst und über mögliche Schutzmaßnahmen mitgeteilt, hierzu werden entsprechende Inhalte vorbereitet, die im Bedarfsfall nur noch angepasst werden müssen.

Das BSI SOLLTE in besonderen Fällen hinzugezogen werden, z. B. wenn ein Angriff besonderer technischer Qualität vorliegt oder wenn die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit der betroffenen IT-Ressourcen von besonderem öffentlichem Interesse ist.

17.5 *Vorbereitung auf* den Ausfall wichtiger IT-Ressourcen

Die Maßnahmen der folgenden Abschnitte MÜSSEN für alle wichtigen IT-Ressourcen umgesetzt werden.

Dabei KÖNNEN wichtige IT-Ressourcen in Gruppen zusammengefasst werden, wenn sie sich in Hard- und Software ähneln und für ähnliche Zwecke eingesetzt werden.

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

17.5.1 Wiederanlaufpläne

Für jede wichtige IT-Ressource 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, die IT-Ressource innerhalb ihrer MTA soweit wiederherzustellen, dass zumindest ihr Notbetriebsniveau erreicht ist.
2. Wenn die IT-Ressource innerhalb ihrer 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 so weit in Betrieb zu nehmen, dass die von der IT-Ressource 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, Schlüssel für kryptografische Maßnahmen 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.

17.5.2 Abhängigkeiten

Die Abhängigkeiten der wichtigen IT-Ressourcen untereinander MÜSSEN dokumentiert und dabei die Reihenfolge ihrer Wiederherstellung festgelegt werden.

Dabei SOLLTEN die Möglichkeiten von parallelen Wiederherstellungen und Redundanzen von IT-Ressourcen ermittelt werden.

Wenn IT-Ressourcen nur sequentiell wiederhergestellt werden können, MUSS deren MTA so angepasst werden, dass die MTA der letzten wiederherstellbaren IT-Ressource nicht überschritten wird.

Die Dokumentation MUSS folgende Anforderungen erfüllen:

1. Aus ihr geht eindeutig hervor, in welcher Reihenfolge die wichtigen IT-Ressourcen wiederhergestellt werden müssen.
2. Sie ist verständlich und übersichtlich strukturiert.
3. Sie ist im Bedarfsfall schnell verfügbar.
4. Sie wird nicht in einem Brandabschnitt aufbewahrt, in dem sich wichtigen IT-Ressourcen befinden.

18 IT-Krisen

18.1 Grundlagen

Eine strukturierte Vorbereitung ermöglicht es, schnell auf Krisen die für oder durch die IT entstehen zu reagieren, Schäden zu begrenzen und die Handlungsfähigkeit der Organisation wieder herzustellen.

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.

18.2 IS-Richtlinie

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

1. Der Begriff IT-Krise wird klar definiert.

   Es SOLLTE beschrieben werden, welche Ereignisse dazu führen, dass eine Situation als IT-Krise eingestuft wird.

2. Im IT-Krisenfall tritt unter dem Vorsitz des IT-Krisenmanagers das IT-Krisenteam zusammen.
3. Alle Mitarbeiter unterstützen bei Bedarf den IT-Krisenmanager und das IT-Krisenteam.
4. Die Richtlinie definiert, wie die Organisation intern und extern akute und bewältigte IT-Krisen kommuniziert.

18.3 IT-Krisenplan

Es MUSS ein Verfahren (siehe Anhang A.1) für die Bewältigung von IT-Krisen implementiert werden (IT-Krisenplan), das folgende Reaktionen zeitnah sicherstellt:

1. Es wird ein Überblick über die Situation gewonnen.
2. Der IT-Krisenmanager ruft den IT-Krisenfall aus.

3. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.
4. Der Schaden wird durch Sofortmaßnahmen eingedämmt.
5. Es wird ein konkreter Plan zur Bewältigung der IT-Krise erstellt und fortlaufend an die Entwicklungen angepasst.
6. Die zur Bewältigung der IT-Krise benötigten Ressourcen werden identifiziert und bereitgestellt.
7. Die Ressourcen werden unterstützt und geschützt, z. B. durch ihre zyklische Rotation, die Bereitstellung von Verpflegung, Ruhezeiten und/oder durch Supervision.
8. Es wird eine gesteuerte Krisenkommunikation etabliert mit der entsprechende interne und externe Stellen wie Mitarbeiter, Versicherungen, Aufsichtsbehörden, Kunden usw. angemessen über Entwicklungen informiert werden.

   Hierzu SOLLTEN entsprechende Adresslisten und Inhalte vorbereitet werden.
9. Die Entwicklung der IT-Krise, die Reaktionen auf sie und der entstandene Schaden werden so dokumentiert, dass die Organisation ihre Informationspflichten erfüllen und die IT-Krise nachbereiten kann.
10. Bei Bedarf werden Beweismittel gesichert.
11. Es findet eine Nachbereitung statt, bei der die Ursachen der IT-Krise ermittelt, ihre Bewältigung bewertet und konkrete Verbesserungen erarbeitet werden.
12. Das Verfahren ist auch bei IT-Krisen schnell verfügbar.

18.4 Vorbereitung auf IT-Krisen

Die Organisation MUSS die wahrscheinlichsten IT-Krisen identifizieren.

Dies SOLLTE durch eine Risikoidentifizierung und -analyse (siehe Anhang A.2) geschehen.

Für jede identifizierte IT-Krise MUSS ein Verfahren (siehe A.1) implementiert werden, das die Organisation in die Lage versetzt schnell und zielgerichtet auf die IT-Krise zu reagieren.

Die Verfahren MÜSSEN die Anforderungen an den IT-Krisenplan (siehe Abschnitt 18.3) erfüllen.

Darüber hinaus SOLLTEN Sie die folgenden Anforderungen erfüllen:

1. *Sie definieren, für welche Art von Krisen sie zutreffend sind (z.B. für technische Störungen, Naturkatastrophen, Reputationskrisen usw.).*
2. *Sie begründen, warum sie erstellt wurden und legen fest, was mit ihnen erreicht werden soll.*

Die Verfahren MÜSSEN jährlich getestet werden, indem ein Verfahren nach dem Zufallsprinzip ausgewählt und getestet wird.

Dies SOLLTE in Form eines Planspiels oder einer Diskussion der einzelnen Punkte des Verfahrens und einer zusätzlichen Simulation der Krisenkommunikation geschehen.

Die Durchführung und die Ergebnisse der Tests MÜSSEN dokumentiert werden.

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

18.5 Gesicherte Kommunikation

Für den IT-Krisenfall MÜSSEN Kommunikationskanäle zur Verfügung stehen, die auch bei einer Störung oder einem Ausfall der IT-Infrastruktur genutzt werden können.

Dies KANN über unabhängige oder besonders gesicherte Kommunikationskanäle umgesetzt werden.

19 Kryptografie

19.1 Grundlagen

Kryptografie ist eine unverzichtbare Technologie für die Informationssicherheit. Mit ihrer Hilfe können Informationen zuverlässig vor unberechtigtem Zugriff bewahrt, Manipulationen erkannt und Kommunikationspartner authentifiziert werden.

Deshalb SOLLTE die Organisation ein Konzept für den Einsatz von Kryptografie auf Basis eines anerkannten Standards wie ISO/IEC 27001 oder auf Basis einer anerkannten Vorgehensweise wie dem IT-Grundschutz-Baustein CON.1 des BSI etablieren.

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

19.2 Basisschutz

Die Maßnahmen der folgenden Abschnitte MÜSSEN, sofern eine entsprechende Funktionalität gegeben ist, für alle eingesetzten kryptografischen Maßnahmen 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).

Kryptografische Maßnahmen bei nachrangigen IT-Ressourcen KÖNNEN von der Umsetzung der Maßnahmen des Basisschutzes ausgenommen werden.

19.2.1 Auswahl und Konfiguration

Kryptografische Maßnahmen MÜSSEN die folgenden Anforderungen erfüllen:

1. Sie basieren auf etablierten Algorithmen, die von der Fachwelt als ausreichend sicher angesehen werden.
2. Sie werden mit Sicherheitsparametern (wie z. B. Schlüssellängen und Betriebsarten) betrieben, die von der Fachwelt als ausreichend sicher angesehen werden.

Für die Auswahl der Algorithmen und Sicherheitsparameter SOLLTEN die technische Richtlinien BSI-TR-02102 genutzt werden.

Alternativ KÖNNEN Produkte eingesetzt werden, die gemäß eines entsprechenden Standards wie z. B. FIPS 140-3 oder Common Criteria / ISO 15408 zertifiziert sind.

Kryptografischen Maßnahmen MÜSSEN zeitnah verbessert oder ersetzt werden, wenn sie als unsicher erkannt werden.

19.2.2 Schlüsselmanagement

Für das Management der Schlüssel für kryptografische Maßnahmen MUSS ein Verfahren (siehe Anhang A.1) implementiert werden, das folgende Anforderungen erfüllt:

1. Schlüssel werden bei Erzeugung, Übertragung, Lagerung und Transport vor unberechtigter Erzeugung, Änderung, Beschädigung, Verlust, Einsichtnahme und Nutzung geschützt.
2. Wenn der begründete Verdacht besteht, dass die Vertraulichkeit, Integrität und/oder Authentizität von Schlüsseln verletzt wurde werden sie umgehend zurückgezogen und ersetzt.
3. Die Verletzung der Vertraulichkeit, Integrität und/oder Authentizität von Schlüsseln wird als Sicherheitsvorfall (siehe Kapitel 17) behandelt.
4. Schlüssel werden in regelmäßigen, definierten Abständen erneuert.
5. Nicht mehr benötigte Schlüssel werden umgehend zurückgezogen oder gelöscht.

6. Schlüssel werden vor jeder Nutzung geprüft, ob sie zurückgezogen wurden; zurückgezogene Schlüssel werden als ungültig zurückgewiesen.

   Der Versuch, einen zurückgezogenen Schlüssel zu nutzen, SOLLTE als Sicherheitsvorfall (siehe Kapitel 17) behandelt werden.

7. Schlüssel werden in die Datensicherung aufgenommen.

19.3 Kritische Informationen

Es MUSS festgelegt werden, wie kritische Informationen im Ruhezustand als auch bei der Übertragung durch kryptografische Maßnahmen vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

Dies SOLLTE mithilfe einer Risikoidentifizierung, -analyse und -behandlung (siehe Anhang A.2) geschehen.

20 Entwicklungen und Anpassungen

20.1 Grundlagen

Wenn IT-Ressourcen entwickelt oder angepasst werden ist es notwendig, die Anforderungen der Informationssicherheit angemessen zu berücksichtigen, um Schwachstellen zu vermeiden und gesetzliche, vertragliche und betriebliche Anforderungen zu erfüllen.

20.2 Generelle Anforderungen

Wenn IT-Ressourcen entwickelt oder angepasst werden MUSS der Projektverantwortliche sicherstellen, dass in der Planungsphase die Anforderungen an deren Informationssicherheit festgelegt werden, ein entsprechendes Sicherheitskonzept definiert und im Laufe des Projekts umgesetzt wird.

Das Sicherheitskonzept SOLLTE durch ein Risikoidentifikation und -analyse (siehe Anhang A.2) erstellt werden und die wahrscheinlichsten Bedrohungen und Schwachstellen sowie die entsprechenden technischen und/oder organisatorischen Sicherheitsmaßnahmen beinhalten.

Die Sicherheitsmaßnahmen SOLLTEN folgende Aspekte berücksichtigen:

1. *sichere Datenübertragung und -speicherung*
2. *Validierung der Eingabedaten*
3. *ausreichend starke Authentifizierung der nutzenden Instanzen*
4. *Autorisierung der nutzenden Instanzen (Zugriffskontrolle)*
5. *Protokollierung erfolgreicher und erfolgloser Anmeldeversuche, von Fehlern und Informationssicherheitsereignissen*
6. *Abfangen und strukturierte Behandlung von Ausnahme- und Fehlerzuständen*
7. *Anleitungen für die sichere Inbetriebnahme, den sicheren Betrieb und die sichere Außerbetriebnahme*

Zusätzlich MUSS festgelegt werden, wie lange die IT-Ressource mit Anpassungen und Fehlerkorrekturen versorgt wird und wie die Nutzer über Schwachstellen und Updates informiert werden.

Wenn Maßnahmen dieses Abschnitts für eine Entwicklung bzw. Anpassung nicht umgesetzt werden, MÜSSEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

20.3 Software

Bei der Entwicklung bzw. Anpassung von Software SOLLTEN zusätzlich die folgenden Anforderungen erfüllt werden:

1. *Es werden ausschließlich Entwicklungsumgebungen und Bibliotheken genutzt, die aus vertrauenswürdigen Quellen stammen und die vom Hersteller aktiv mit Sicherheitsupdates versehen werden.*
2. *Die Sicherheit der Software wird mithilfe entsprechender Tests überprüft.*
3. *Die Software wird in einer sicheren Standard-Konfiguration ausgeliefert.*
4. *Integrität und Authentizität von Updates werden z. B. durch entsprechende kryptografische Maßnahmen sichergestellt.*
5. *Die Software ist so gestaltet, dass sie im Betrieb nur ein Mindestmaß an Zugriffsrechten und Privilegien benötigt.*
6. *Authentifizierungsmerkmale können geändert werden.*

21 Überwachung und Steuerung

21.1 Grundlagen

Um die Wirksamkeit und Effizienz der Sicherheitsmaßnahmen für die Verantwortlichen transparent zu machen und um frühzeitig Probleme und Verbesserungspotential zu erkennen, ist es notwendig, den Zustand der Informationssicherheit messbar zu machen.

21.2 Kennzahlen

Die Organisation MUSS nach einem implementierten Verfahren (siehe Anhang A.1) jährlich Kennzahlen erheben.

Die Kennzahlen MÜSSEN die folgenden Anforderungen erfüllen:

1. Sie basieren auf objektiv messbaren Fakten.
2. Sie zeigen einen Status oder eine Entwicklung über einen definierten Zeitraum.
3. Für jede Kennzahl ist definiert, wie sie erhoben wird.

   Kennzahlen SOLLTEN möglichst einfach (z. B. automatisiert) erhoben werden.
4. Für jede Kennzahl ist ein Grenzwert festgelegt, der erreicht werden muss, damit eine gemessene Maßnahme als wirksam gilt.

Mit den Kennzahlen MUSS die Wirksamkeit der Sicherheitsmaßnahmen für folgende Bereiche erfasst werden:

1. Sicherheitsvorfälle (wie z. B. Anzahl und Schwere zurückliegender Sicherheitsvorfälle oder die Qualität der Reaktion auf Sicherheitsvorfälle)
2. Verfügbarkeit der IT-Infrastruktur (z. B. die Verfügbarkeit ausgewählter IT-Systeme, der zentralen Prozesse und von Prozessen mit hohem Schadenpotential)
3. Ergebnisse von Audits und von sonstigen Überprüfungen (z. B. Penetrationstests, Security Scans oder Überprüfungen ausgewählter Sicherheitsmaßnahmen, Logfiles oder anderer Meldungen)
4. Awareness und Verhalten der Mitarbeiter (z. B. Ergebnisse von Lernerfolgskontrollen von Schulungs- und Sensibilisierungsmaßnahmen oder die Anzahl der Verstöße gegen IS-Richtlinien)
5. Management und kontinuierliche Verbesserung (z. B. die Anzahl identifizierter und umgesetzter Verbesserungen oder die Anzahl erkannter mängelbehafteter Verfahren).
6. Funktionieren des ISMS (z. B. die erfolgte Prüfung von Dokumenten, die Anzahl der Zuständigkeitslücken oder die Anzahl der Überschneidungen von Verantwortlichkeiten)
7. Risikomanagement (z. B. allgemeine Kennzahlen, die im Zuge des Risikomanagements erhoben werden)

Die Kennzahlen und die Bewertung der Wirksamkeit der erfassten Sicherheitsmaßnahmen MÜSSEN im Zuge des jährlichen Berichts des ISB an das IST (siehe Abschnitt 4.4) vorgestellt werden.

Wenn anhand der Kennzahlen Mängel erkannt werden, MÜSSEN die dadurch entstehenden Risiken identifiziert, analysiert und behandelt werden (siehe Anhang A.2).

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.

   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.

Verfahren KÖNNEN auf mitgeltende Unterlagen verweisen.

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 anhand einheitlicher, zuvor festgelegter Kriterien, die folgende Aspekte berücksichtigen:
   a. das Ausmaß der Risikoexposition
   b. die Größe der Organisation
   c. die Umsetzungskosten
   d. die Eintrittswahrscheinlichkeit
   e. die Schwere von Sicherheitsvorfällen (die potentiellen Schäden) sowie
   f. die gesellschaftlichen und wirtschaftlichen Auswirkungen
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.

Hierzu SOLLTE ein zentraler Risikobehandlungsplan aufgestellt werden, in dem alle Risiken und der Stand ihrer Behandlung fortlaufend erfasst werden.

Risiken KÖNNEN 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.