Leitfaden zur Informationssicherheit für Digitalisateprovider

Informationssicherheit ist eine kontinuierliche Herausforderung, die sowohl technische als auch organisatorische Maßnahmen erfordert. Digitalisateprovider sollten ihre IT-Sicherheitsstrategie und die daraus resultierenden IT-Sicherheitsmaßnahmen regelmäßig überprüfen und anpassen, um sich gegen die wachsende Bedrohungslage zu wappnen.

Die Umsetzung der in diesem Leitfaden enthaltenen Maßnahmen ist entsprechend sehr zu empfehlen, aber keine Voraussetzung für die Anbindung von Digitalisateprovidern an den Kulturpool.

- Einleitung
- Überblick / Grundlagen
- Gefährdungs- und Problempotentiale
- Maßnahmen zur Informationssicherheit
- Technische und organisatorische Maßnahmen zur Sicherstellung der Verfügbarkeit und der Integrität
- Technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit

Einleitung

Daten sind die Grundlage verschiedener Entscheidungen und Anwendungen. Daher ist es für Digitalisateprovider von essenzieller Bedeutung, Daten zuverlässig zu schützen und gesetzliche Vorgaben zu erfüllen. Neben den Daten selbst sind weitere Informationen zu Prozessen, Arbeitsabläufen oder Infrastrukturen dafür relevant. Die Sicherstellung der Informationssicherheit umfasst insbesondere die Verfügbarkeit von Daten für berechtigte Nutzer zu gewährleisten, die Vertraulichkeit der Daten sicherzustellen und deren Integrität zu schützen. Eine effektive Sicherheitsstrategie trägt nicht nur dazu bei, die digitale Sammlung eines Unternehmens sicher aufzubewahren, sondern stellt auch die Nutzbarkeit des Digitalisateangebots für Nutzer und externe Plattformen sicher. Darüber hinaus schützt sie zentrale Geschäftsprozesse, wie Ticketverkauf, Webauftritt oder Gebäudetechnik, vor Störungen. Neben der Vermeidung von Reputationsschäden durch Cyberangriffe und Datenverluste ist die Einhaltung gesetzlicher Vorschriften wichtig.

Informationssicherheit ist eine kontinuierliche Herausforderung, die sowohl technische als auch organisatorische Maßnahmen erfordert. Digitalisateprovider sollten ihre IT-Sicherheitsstrategie und die daraus resultierenden IT-Sicherheitsmaßnahmen regelmäßig überprüfen und anpassen, um sich gegen die wachsende Bedrohungslage zu wappnen. Eine Kombination aus präventiven, detektiven und reaktiven Sicherheitsmaßnahmen sorgt für einen umfassenden Schutz der digitalen Infrastruktur und sichert langfristig die Integrität und Verfügbarkeit der digitalen Bestände.

Der hier vorliegende Leitfaden soll eine Planungs- und Entscheidungshilfe für die notwendigen Maßnahmen zur Informationssicherheit darstellen und wurde auf Basis aktueller Best Practices erstellt. Trotzdem enthält dieser Leitfaden keine abschließende Darstellung aller notwendiger Maßnahmen zur Informationssicherheit und ersetzt damit nicht eine finale Beurteilung / Entscheidung der umzusetzenden Maßnahmen.

Die Umsetzung der in diesem Leitfaden enthaltenen Maßnahmen ist entsprechend sehr zu empfehlen, aber keine Voraussetzung für die Anbindung von Digitalisateprovidern an den Kulturpool.

Überblick / Grundlagen

Im Rahmen dieses Leitfadens werden sinnvolle und bewährte technische und organisatorische Maßnahmen zur Sicherstellung der Informationssicherheit beschrieben, die den Empfehlungen des BSI-Grundschutzes (BSI - IT-Grundschutz-Kompendium) bzw. der ISO27001 (ISO/IEC 27001 - Anforderungen an Informationssicherheits-Managementsysteme) folgen. Die Maßnahmen sind dabei entsprechend den Grundsätzen der Informationssicherheit in folgende Bereiche gegliedert:

- Maßnahmen zur Sicherstellung der **Verfügbarkeit** von Daten
- Maßnahmen zur Sicherstellung der **Integrität** (Korrektheit) der Daten
- Maßnahmen zur Sicherstellung der **Vertraulichkeit** der Daten

Die Auswahl, Planung und Umsetzung der Maßnahmen zur Informationssicherheit sollte auf Basis einer strukturierten Risikobeurteilung erfolgen. Bewährte Methoden für die Durchführung derartiger Risikobeurteilungen sind der BSI-Standard 200-3 (BSI-Standard 200-3) oder eine Risikoanalyse gem. ISO27001.

Um eine sinnvolle Anwendung der Maßnahmen dieses Leitfadens auch zu ermöglichen, wenn eine strukturierte Risikobeurteilung z. B. aufgrund des hohen Aufwands noch nicht erfolgt ist, sind die in diesem Leitfaden dargestellten Maßnahmen nach Notwendigkeit bzw. nach Schutzwirkung auf Basis der allgemeinen Gefährdungslage gegliedert und bewertet:

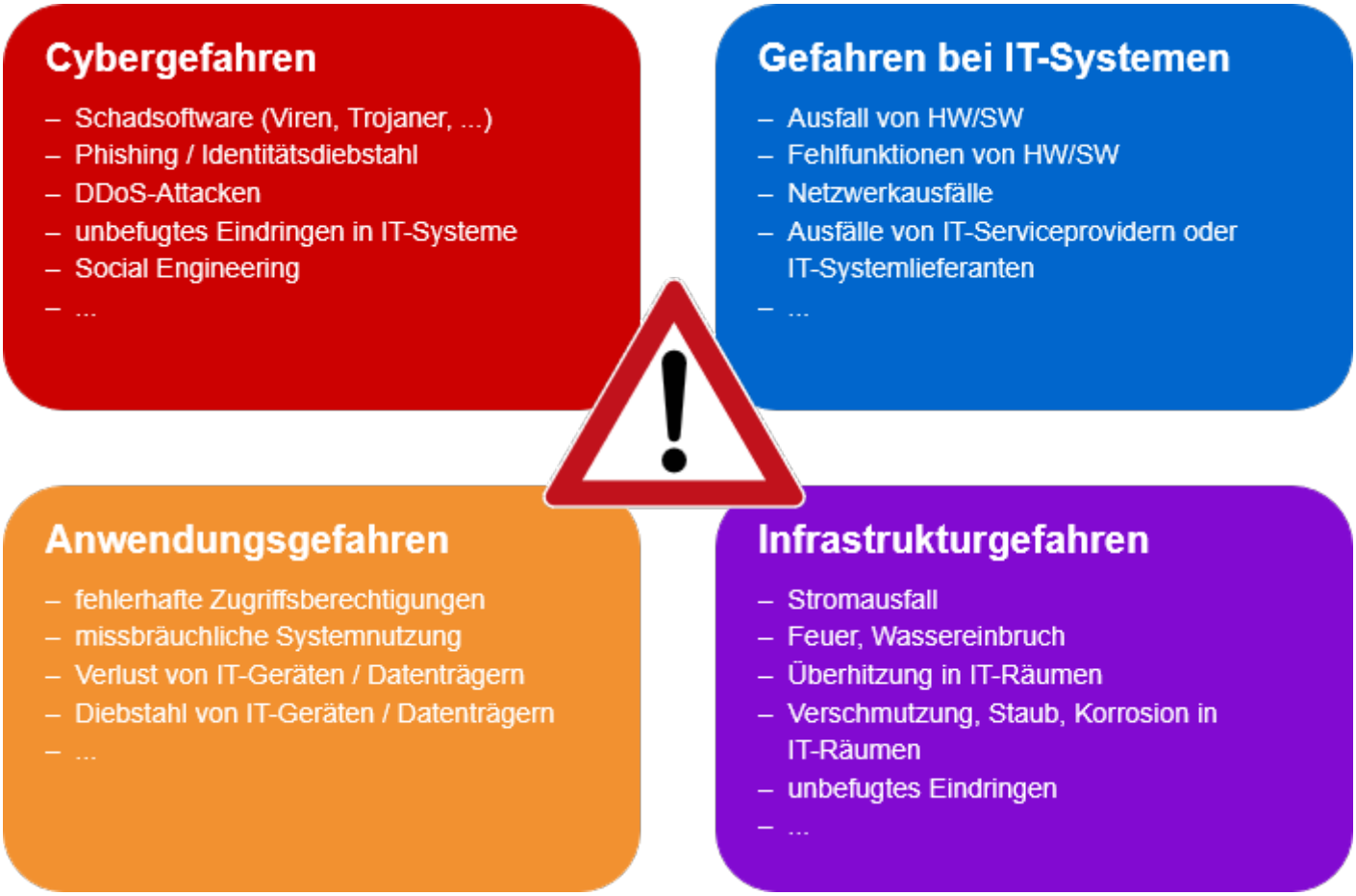
- **STARK EMPFOHLEN**: stark empfohlene Basis-Maßnahmen für alle Organisationsgrößen
- **EMPFOHLEN**: empfohlene Maßnahmen, sollten zumindest bei großen Organisationen umgesetzt werden
- **OPTIONAL**: sinnvolle, ergänzende Maßnahmen zur Sicherstellung eines hohen Niveaus der Informationssicherheit

Die Maßnahmen zur Informationssicherheit werden in diesem Leitfaden nicht im Detail beschrieben, sondern sollen internen IT-Abteilungen, IT-Securityabteilungen bzw. externen IT-Dienstleistern die notwendigen Handlungsbereiche klar aufzeigen. Eine Detaillierung der Maßnahmen zugeschnitten auf die genutzte IT-Umgebung muss dann durch die internen IT-Abteilungen, IT-Securityabteilungen bzw. den externen IT-Dienstleister erfolgen.
Anmerkung: In der Initialversion sind nur die „STARK EMPFOHLENEN“-Maßnahmen näher beschrieben.

Nach der Einführung von Maßnahmen zur Informationssicherheit ist eine kontinuierliche Kontrolle, Steuerung, Koordination und Verbesserung dieser Maßnahmen erforderlich. Das kann im Rahmen eines strukturierten ISMS (Informations-Sicherheits-Management-Systems) oder durch die Berücksichtigung im allgemeinen Vorhabens- und Aufgabenmanagement der IT oder IT-Security erfolgen.

Gefährdungs- und Problempotentiale

Sowohl die Entwicklung der letzten Jahre als auch alle Prognosen für die Zukunft zeigen ein exponentielles Wachstum von Cybergefahren und Cyberangriffen. Die Gefährdung der Informationssicherheit erfolgt aber nicht nur durch IT-Sicherheitsverletzungen und Cyberangriffe, sondern auch durch technische Gefahren, Gefahren bei der Anwendung von IT-Systemen und generellen Infrastrukturrisiken:



Im Rahmen der Maßnahmen zur Informationssicherheit müssen alle diese Gefahren und Risiken Berücksichtigung finden.

Maßnahmen zur Informationssicherheit

Als Grundvoraussetzung für die erfolgreiche Umsetzung von Maßnahmen zur Informationssicherheit sind folgende organisatorische Rahmenbedingungen unbedingt sicherzustellen:

- klares Bekenntnis des Unternehmens zur Bedeutung der Informationssicherheit beginnend mit der Unternehmensleitung (TopDown)
- klare Zuständigkeitsverteilung für die Aufgaben zur Informationssicherheit
- KnowHow-Aufbau und laufende Weiterbildung zur Informationssicherheit sowohl bei den IT-Verantwortlichen / IT-Mitarbeiter:innen als auch bei den IT-Anwender:innen
- Sicherstellung der notwendigen personellen Ressourcen / Budgetmittel für die Umsetzung von Maßnahmen zur Informationssicherheit

Besonderes Augenmerk ist bei der Umsetzung der Maßnahmen zur Informationssicherheit auf den Faktor „Mensch“ zu richten, da diesem bei allen angeführten Maßnahmen eine zentrale Bedeutung zukommt. Eine Involvierung aller betroffenen sozialen Umwelten und ein aktives Management der mit der Maßnahmenumsetzung einhergehenden Änderungen sind daher ein kritischer Erfolgsfaktor.

Sollten für die Umsetzung von Maßnahmen zur Informationssicherheit externe IT-Dienstleister erforderlich sein, so ist bei der Auswahl der Partner besondere Sorgfalt hinsichtlich der Verlässlichkeit, der wirtschaftlichen und fachlichen Leistungsfähigkeit, aber auch hinsichtlich relevanter gesetzlicher Vorgaben (z. B. DSGVO, …) anzuwenden.

Zur Absicherung von möglichen Schäden aufgrund von Informationssicherheitsvorfällen ist auf Basis einer Risikobeurteilung der Abschluss einer Cyberversicherung zu evaluieren.

Technische und organisatorische Maßnahmen zur Sicherstellung der Verfügbarkeit und der Integrität

Zur Sicherstellung der Verfügbarkeit und der Integrität (Korrektheit) von IT-Systemen sind folgende Maßnahmen erforderlich/sinnvoll:

Maßnahmen zur Absicherung	
Datensicherung	STARK EMPFOHLEN
Sicherstellung der Herstellerunterstützung	STARK EMPFOHLEN
Laufendes Einspielen von kritischen Software Patches / Updates	STARK EMPFOHLEN
Test neuer Software / Software-Versionen	STARK EMPFOHLEN
Migrationsplanung für Versionsumstellungen und Vorsorge durch Rollback-Szenarien	STARK EMPFOHLEN
Vereinbarung von Servicelevels (bei Systemoutsourcing / Cloudservices)	STARK EMPFOHLEN
DDoS-Schutz	STARK EMPFOHLEN
Dokumentation aller (wesentlichen) IT-Systeme	STARK EMPFOHLEN
Erstellung von Notfallplänen für den Ausfall von IT-Systemen	STARK EMPFOHLEN
Überwachung (Monitoring) aller (wesentlichen) IT-Systeme	EMPFOHLEN
Unterbrechungsfreie Stromversorgung (USV) / Notstromversorgung	EMPFOHLEN

Aufstellung der zentralen Hardwarekomponenten in geeigneten (Rechner) Räumen	EMPFOHLEN
redundante Gestaltung kritischer Hardwarekomponenten	EMPFOHLEN
örtlich getrennter Ausweich-Rechnerraum	OPTIONAL
redundante Netzwerkverbindungen	OPTIONAL
Vereinbarung einer (notariellen) System- / Sourcecodehinterlegung für wesentliche IT-Systeme	OPTIONAL

Datensicherung [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Die Sicherung von Daten und Programmen dient zur Vorsorge vor dem Verlust oder einer nicht gewollten Manipulation von Programmen oder Daten infolge von Hardware-, Software- oder Anwendungsfehlern oder von Cyberangriffen. Die Sicherung von Daten/Programmen und deren Wiederherstellung nach Daten/Programmverlusten ist damit wesentlich für die Sicherstellung der Systemverfügbarkeit. Bei Systemen, die von externen IT-Dienstleistern betrieben werden (Outsourcing, Cloudlösungen), dient eine zusätzliche lokale Datensicherung außerdem zur Vorsorge von Problemen, Ausfällen oder der Insolvenz des externen IT-Dienstleisters.

Umsetzung:

Die Realisierung der Datensicherung muss mit einer geeigneten Sicherheitssoftware auf Sicherungsmedien (SAN/NAS, Bandlaufwerke mit Magnetbändern, ...) erfolgen. Die Sicherungsmedien müssen dabei räumlich von den zu sichernden IT-Systemen getrennt aufgestellt werden (Vorsorge gegen Feuer u. ä.). Zur Vorsorge von nicht sofort erkannten Datenverlusten/-manipulationen sind mehrere Sicherungsgenerationen vorzusehen (Tages-, Wochen-, Monatssicherungen). Bei besonders kritischen Systemen muss eine Wiederherstellung bis zur letzten Speicherung/Transaktion realisiert werden.

Erfolgt die Datensicherung auf stationären Speichermedien (SAN, NAS), so ist eine automationsgestützte (physische) Trennung des Speichermediums nach dem Abschluss der Datensicherung erforderlich (AirGap). Diese Maßnahme dient der Vorsorge für eine Verschlüsselung des Sicherungsmediums bei Cyberangriffen mittels eines Kryptotrojaners.

Das Vorgehen für die Wiederherstellung von Datensicherungen muss dokumentiert und regelmäßig geprüft werden.

Bei IT-Systemen, die von externen IT-Dienstleistern betrieben werden (Outsourcing, Cloudlösungen), ist (neben der Sicherung des externen IT-Dienstleisters) auch eine zusätzliche lokale Sicherung auf eigenen Sicherungsmedien vorzusehen, um im Fall von Problemen/Ausfall/Insolvenz des externen IT-Dienstleisters zumindest auf die eigenen Daten weiter zugreifen zu können.

Sicherstellung der Herstellerunterstützung [STARK EMPFOHLEN]

>

> **Ziele/Nutzen**: Durch die Herstellerunterstützung (Wartung) von IT-Systemen wird u. a. die Behebung von Fehlern, Problemen und Sicherheitslücken sowie die Versorgung mit Ersatzteilen (bei Hardwarekomponenten) gewährleistet. Üblicherweise umfasst die Herstellerunterstützung (Wartung) auch die Anpassung von IT-Systemen an geänderte Rahmenbedingungen (z. B. geänderte gesetzliche Regelungen) sowie die Weiterentwicklung der IT-Systeme. Eine aufrechte Herstellerunterstützung ist daher wesentlich für die Sicherstellung der Systemverfügbarkeit und der IT-Sicherheit.

Umsetzung:

Es muss zumindest für alle wesentlichen IT-Systeme eine Wartungsvereinbarung, die zumindest die Behebung von Fehlern, Problemen und Sicherheitslücken (u. a. im Rahmen von Software-Patches und Updates) sowie die Versorgung mit Ersatzteilen (bei Hardwarekomponenten) umfasst, mit dem Hersteller/Lieferanten abgeschlossen werden. Darüber hinaus ist regelmäßig zu prüfen, ob die Herstellerunterstützung von eingesetzten IT-Systemen oder von einzelnen Systemversionen in Zukunft eingestellt werden soll (End of Life). Sollte dies der Fall sein, so sind rechtzeitig Maßnahmen zur Ablöse der betroffenen IT-Systeme oder für Systemupdates vorzusehen.

Laufendes Einspielen von kritischen Software-Patches / Updates [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Das Einspielen von kritischen Software-Patches oder Updates dient zur Behebung von kritischen Fehlern oder Sicherheitslücken und ist damit sowohl für das Funktionieren als auch für die Sicherstellung der Verfügbarkeit von IT-Systemen wesentlich.

Umsetzung:

Das Einspielen von Software-Patches oder Updates, die kritische Fehler oder Sicherheitslücken beheben, ist unverzüglich/zeitnah nach deren Veröffentlichung sicherzustellen. Dazu ist es auch erforderlich, sicherzustellen, dass eine Benachrichtigung des Herstellers über kritische Software-Patches oder Updates erfolgt (Notification der Hersteller, ...).

Test neuer Software / Software-Versionen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Durch die Überprüfung neuer Softwarekomponenten oder neuer Software-Versionen vor deren produktiver Nutzung werden die Funktionalitäten der Software, die korrekte Verarbeitung der Daten und das fehlerfreie Zusammenwirken mit verbundenen IT-Systemen geprüft. Diese Maßnahme ist wesentlich, um das anforderungsgerechte Funktionieren von IT-Systemen und deren Verfügbarkeit nach der Produktivsetzung zu gewährleisten.

Umsetzung:

Zumindest für wesentliche IT-Systeme sind vor deren produktiver Nutzung entsprechende Funktionalitäts- und Integrationstests auf Basis von vorher erstellten Testplänen vorzusehen. Zur Durchführung der Tests sind sowohl eine eigene Testinfrastruktur als auch die entsprechenden Personalressourcen notwendig.

Bei kritischen Software-Patches oder Updates kann aufgrund der zeitlichen Kritikalität die Testung entfallen.

Migrationsplanung für Versionsumstellungen und Vorsorge durch Rollback-Szenarien [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Ziel der Migrationsplanung ist die Sicherstellung einer erfolgreichen Versionsumstellung (Patch, Update) von IT-Systemen auf Basis einer getesteten Software-Version und die Minimierung der Auswirkungen der Downtime des IT-Systems auf den Geschäftsbetrieb.

Umsetzung:

Im Rahmen der Migrationsplanung ist der Ablauf der Versionsumstellung (Patch, Update) mit den entsprechenden Zuständigkeiten festzulegen und der Zeitpunkt der Migration so zu wählen, dass die Auswirkungen auf den Geschäftsbetrieb so gering wie möglich sind. Vor der Inbetriebnahme einer neuen Version des IT-Systems ist u. a. die erfolgreiche Datenübernahme aus der Vorversion zu prüfen.

Als Vorsorge für eine fehlerhafte Datenübernahme oder sonstige Mängel, die erst nach der Versionsumstellung erkennbar sind, ist zumindest für wesentliche IT-Systeme ein Rollback-Szenario vorzusehen, mit dem wieder auf die Vorversion zurückgewechselt werden kann. Bei kritischen Software-Patches oder Updates kann aufgrund der zeitlichen Kritikalität das Rollback-Szenario entfallen.

Vereinbarung von Servicelevels (bei Systemoutsourcing / Cloudservices) [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Bei IT-Systemen, die von externen IT-Dienstleistern betrieben werden (Outsourcing, Cloudlösungen) besteht kein direkter Einfluss auf den internen Systembetrieb. Zur Sicherstellung der erforderlichen Verfügbarkeit und Nutzbarkeit ist daher eine entsprechende vertragliche Absicherung der einzuhaltenden Servicelevels erforderlich.

Umsetzung:

Die Vereinbarung der erforderlichen Servicelevels ist in den vertraglichen Vereinbarungen mit dem externen IT-Dienstleister entsprechend zu berücksichtigen. Die Vereinbarung von Servicelevels erfolgt im Rahmen eines Service-Level-Agreements (SLA) und sollte dabei u. a. garantierte Mindestwerte für die grundsätzliche Verfügbarkeit des IT-Systems, die Systemperformance, die Reaktionszeiten bei Fehlern / Problemen / Sicherheitsverletzungen sowie für die max. Systemwiederherstellungsdauer nach Ausfällen beinhalten. Bei dem SLA ist auch die Erbringung des Nachweises der Einhaltung der vereinbarten Servicelevels durch den externen IT-Dienstleister festzulegen. Bei der Überschreitung von Servicelevels sind entsprechende Korrekturmaßnahmen und/oder Pönalzahlungen vorzusehen.

Bei besonders kritischen IT-Systemen kann auch eine regelmäßige Auditierung der Maßnahmen zur Erreichung der Servicelevels beim externen IT-Dienstleister vorgesehen werden.

Die Vereinbarung eines SLA kann auch mit einer internen IT-Abteilung oder einem internen IT-Dienstleister zur Sicherstellung der notwendigen Servicequalität sinnvoll sein.

DDoS-Schutz [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Der Schutz vor Distributed Denial of Service-Attacken (DDoS) dient der Abwehr von Überlastungsangriffen, deren Ziel es ist, die Verfügbarkeit von IT-Systemen zu beeinträchtigen oder zu unterbrechen.

Umsetzung:

Zumindest für wesentliche IT-Systeme, die aus dem Internet erreichbar sind, sind entsprechende Schutzdienste gegen DDoS-Attacken einzurichten (Load Balancer, DDoS-Schutzdienste, ...). Das kann in der eigenen IT-Infrastruktur erfolgen oder durch vorgelagerte Sicherheitsdienstleister.

Dokumentation aller (wesentlichen) IT-Systeme [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Sowohl zur Planung und Umsetzung von Maßnahmen zur Informationssicherheit als auch zur Bewältigung von Fehlern und Problemen (inkl. Cybergefahren und Cyberangriffe) sind relevante Informationen über die genutzten IT-Systeme und deren Zusammenwirken notwendig.

Umsetzung:

Zumindest wesentliche IT-Systeme (Hardware und Software!) sind ausreichend zu dokumentieren. Dazu zählen neben allgemeinen Angaben (Bezeichnung, Hersteller, Version, ...) auch Informationen über Abhängigkeiten zu anderen IT-Systemen und wesentliche Prozesse zur Systemadministration.

Erstellung von Notfallplänen für den Ausfall von IT-Systemen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Für wesentliche IT-Systeme sind als Vorsorge für einen Totalausfall entsprechende Notfallpläne notwendig. Ziel dieser Notfallpläne ist eine möglichst rasche Wiederherstellung der betroffenen IT-Systeme sowie Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs während des Ausfalls.

Umsetzung:

Für alle wesentlichen IT-Systeme sind Notfallpläne zu erstellen, die

- die Wiederherstellung und den Wiederanlauf des betroffenen IT-Systems unter Berücksichtigung aller technischen Abhängigkeiten beschreiben,
- etwaige notwendige, organisatorische Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs während des Ausfalls beschreiben,
- die notwendige Kommunikation im Rahmen der Notfallbewältigung definieren und
- die Zuständigkeiten und Entscheidungsstrukturen im Rahmen der Notfallbewältigung festlegen.

Ist im Rahmen eines Notfalls die Wiederherstellung mehrerer IT-Systeme erforderlich, so ist eine Reihenfolge der Wiederherstellung auf Basis der Kritikalität der IT-Systeme für die Organisation sowie auf Basis der Abhängigkeiten zwischen den IT-Systemen festzulegen.

Technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit

Zur Sicherstellung der Vertraulichkeit bei IT-Systemen sind folgende Maßnahmen aufbauend auf den Maßnahmen zur Verfügbarkeit und Integrität von IT-Systemen erforderlich / sinnvoll:

Maßnahmen zur Absicherung	
Schutz vor Viren	STARK EMPFOHLEN
Schutz vor der Installation unerwünschter Software oder unzulässiger Veränderung von Systemeinstellungen	STARK EMPFOHLEN
Schutz vor schädlichen Mails	STARK EMPFOHLEN
Schutz vor unerwünschten Netzwerkzugriffen (Firewall)	STARK EMPFOHLEN
Sicherstellung einer verschlüsselten Datenübertragung mit externen Stellen	STARK EMPFOHLEN
Sicherstellung einer abgesicherten Fernwartung von Dritten	STARK EMPFOHLEN
WLAN-Verschlüsselung	STARK EMPFOHLEN
Trennung in internes WLAN und Gäste-WLAN	STARK EMPFOHLEN
Hardening von IT-Systemen	STARK EMPFOHLEN
Berücksichtigung der IT-Sicherheit bei der Entwicklung von IT-Systemen (Security by Design)	STARK EMPFOHLEN
Verschlüsselung von gespeicherten Daten	STARK EMPFOHLEN

Schutz vor der Schadwirkung von Cyberangriffen wie z. B. Verschlüsselung durch Kryptotrojaner (u. a. durch EDR/XDR-Systeme)	EMPFOHLEN
Einrichtung einer DMZ (demilitarisierten Zone) für IT-Systeme, die aus dem Internet erreichbar sind	EMPFOHLEN
Network Access Control (NAC) zum Schutz von unautorisierten Endgeräten	EMPFOHLEN
Einschränkung der Endgerätekonnektivität auf vertrauenswürdige Geräte (Wechseldatenträger, Peripheriegeräte, ...)	EMPFOHLEN
Deaktivierung von Endgeräten im Verlustfall / bei Diebstahl	EMPFOHLEN
erweiterter physischer Zutrittsschutz zu wesentlichen Hardwarekomponenten / Rechnerräumen	EMPFOHLEN
Netzwerksegmentierung / Netzwerktrennung IT/OT	OPTIONAL
DataLeak-Prevention (DLP) für sensible Daten	OPTIONAL

Maßnahmen zum Zugriffsschutz	
Benutzer:innenauthentifizierung und rollenbasierte Berechtigungssysteme/-Vergabe	STARK EMPFOHLEN
Passwort-Policy zur Sicherstellung "sicherer" Passwörter	STARK EMPFOHLEN
Multifaktorauthentifizierung für Zugriffe von externen Netzwerken	STARK EMPFOHLEN
Sicherstellen von Bildschirmsperren	STARK EMPFOHLEN
Festlegung und Umsetzung notwendiger IT-Maßnahmen bei Onboarding / Offboarding / Funktionswechsel	STARK EMPFOHLEN
besonderer Schutz privilegierter User-Accounts / Systemadministrator:innen	EMPFOHLEN
erweiterte Überwachung von Logins	EMPFOHLEN
Überwachung/Logging von Systemadministrationsaktivitäten	EMPFOHLEN
Logging von Benutzer:innenaktivitäten	OPTIONAL
zentrales Identity-Management / Berechtigungssystem	OPTIONAL

ergänzende organisatorische Maßnahmen	
Festlegung und Umsetzung eines Vorgehens bei IT-Sicherheitsverletzungen	STARK EMPFOHLEN
Festlegung und Umsetzung eines Verfahrens für die Meldung von Geräteverlusten / Diebstahl	STARK EMPFOHLEN

Vereinbarung der notwendigen IT-Sicherheitsmaßnahmen (bei Systemoutsourcing / Cloudservices)	STARK EMPFOHLEN
IT-Security-Awareness-Ausbildung für Benutzer:innen	STARK EMPFOHLEN
IT-Sicherheitsrichtlinien für IT-Mitarbeiter:innen und Benutzer:innen	EMPFOHLEN
regelmäßige Security-Überprüfungen / Audits (Pentesting, Blackbox-Tests, Gesamtaudits, ...)	EMPFOHLEN
regelmäßige Audits / Prüfung aller Zugriffsberechtigungen	EMPFOHLEN

Schutz vor Viren [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Der Schutz vor Viren dient der Abwehr von sich selbst verbreitenden Schadprogrammen, die Veränderungen an der Systemsoftware (Betriebssystem, ...), an sonstiger Software, an Daten oder mittelbar auch Schäden an der Hardware verursachen können.

Umsetzung:

Es müssen auf allen IT-Endgeräten (PCs, Notebooks, ...) sowie auf allen Servern geeignete Virenschutzprogramme installiert werden, die sowohl Viren erkennen als auch entfernen können. Die Virenschutzprogramme müssen regelmäßig (automatisch) aktualisiert werden und sind so zu konfigurieren, dass sie die zu schützenden IT-Geräte regelmäßig überprüfen. Daten-Downloads / Uploads aus ungeschützten / unbekannten Quellen (Internet) müssen vor dem Speichern gescannt werden.

Schutz vor der Installation unerwünschter Software oder unzulässiger Veränderung von Systemeinstellungen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Um die Installation von Software, die unerwünscht, gefährlich oder nicht lizenziert ist, zu unterbinden, darf die Installation von Software nur durch Systemadministrator:innen oder im Rahmen einer zentralen Softwareverteilung erfolgen. Auch die Durchführung von zentralen Systemeinstellungen / -Konfigurationen darf zur Prävention vor einer missbräuchlichen Systemnutzung nur durch Systemadministrator:innen oder zentrale Konfigurationsmechanismen erfolgen.

Umsetzung:

Die Benutzer:innen-Accounts auf allen IT-Endgeräten (PCs, Notebooks, ...) sowie auf allen Servern sind so zu konfigurieren, dass die Installation von Software, der Start von ausführbaren Programmen und die Veränderung wesentlicher Systemeinstellungen / -Konfigurationen nicht möglich ist. Administrationsrechte auf IT-Endgeräten, Servern, aber auch auf Druckern und Multifunktionsgeräten müssen IT-Systemadministrator:innen vorbehalten sein.

Schutz vor schädlichen Mails [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Der Schutz vor schädlichen Mails dient zum Erkennen und der Abwehr von Mails, die Schadsoftware beinhalten (in Anhängen) oder schädliche Inhalte aufweisen (Links auf schädliche

> Internetinhalte, Phishing-Mails, Spam-Mails, ...).

Umsetzung:

Es muss am Mailserver ein geeigneter Schutzdienst installiert werden, der alle eingehenden Mails auf schädliche Inhalte überprüft, Anhänge in einer abgetrennten Umgebung (Sandbox) auf Schadwirkung testet und so erkannte schädliche Mails blockiert. Die Sicherheitssoftware für den Mailschutz muss regelmäßig (automatisch) aktualisiert werden.

Schutz vor unerwünschten Netzwerkzugriffen (Firewall) [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Firewalls dienen dem Schutz vor gefährlichen oder unerwünschten Netzwerkzugriffen und damit zum Schutz vor Cyberangriffen und/oder Datendiebstahl.

Umsetzung:

Es muss zumindest zwischen dem Internet und dem internen LAN eine geeignete Firewall installiert werden (Netzwerk-Firewall). Die Firewall muss so konfiguriert werden, dass unerwünschter Datenverkehr blockiert wird und erlaubter Datenverkehr passieren kann. Ist das LAN in mehrere Netzwerksegmente gegliedert, so sollten zwischen den Netzwerksegmenten ebenfalls Firewalls installiert werden.

Ergänzend zu den Netzwerk-Firewalls muss auch auf jedem IT-Endgerät eine Personal-Firewall installiert werden.

Sicherstellung einer verschlüsselten Datenübertragung mit externen Stellen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Die sichere Verschlüsselung der Datenübertragung an Dritte oder bei externen Zugriffen dient zur Prävention vor dem Ausspähen oder der ungewollten Manipulation von Daten am Übertragungsweg zu externen Stellen.

Umsetzung:

Es müssen sämtliche Datenverbindungen für Zugriffe von externen Stellen oder zu externen Stellen mit geeigneten Verschlüsselungsmechanismen geschützt werden. Das können z. B. VPN-Lösungen für Netzwerkverbindungen zwischen Rechnersystemen (Server, Homeoffice) oder die zwingende Nutzung von HTTPS bzw. HSTS bei Internetdiensten sein.

Bei Mails an externe Stellen ist zumindest für Mails mit vertraulichen, sensiblen oder geheimen Inhalten eine Mailverschlüsselung vorzusehen.

Sicherstellung einer abgesicherten Fernwartung von Dritten [STARK EMPFOHLEN]

>

> **Ziele/Nutzen**: Die Absicherung der Fernwartung von Dritten dient zum Schutz gegen unerwünschte Wartungs- oder Administrationszugriffe bei IT-Systemen, für die Wartungs- oder Administrationsaktivitäten durch externe IT-Dienstleister erforderlich sind.

Umsetzung:

Für die Wartungs- oder Administrationsaktivitäten durch externe IT-Dienstleister ist eine geeignete Fernwartungssoftware einzusetzen, die Fernzugriffe erst nach einer entsprechenden Freigabe erlaubt und die Beobachtung bzw. das Aufzeichnen aller Fernzugriffe ermöglicht.

WLAN-Verschlüsselung [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Die sichere Verschlüsselung von WLANs dient zur Prävention vor dem Ausspähen oder der ungewollten Manipulation während der Datenübertragung in eigenen Funknetzen (WLANs).

Umsetzung:

Sowohl interne als auch Gäste-WLANs müssen mit aktuellen, dem Stand der Technik entsprechenden Verschlüsselungsmechanismen geschützt werden.

Trennung in internes WLAN und Gäste-WLAN [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Die Trennung in das interne WLAN und das Gäste-WLAN dient dem Schutz des internen LANs (inkl. des internen WLANs) und der internen IT-Systeme vor potenziell ungeschützten oder gefährlichen IT-Endgeräten, die mit dem Gäste-WLAN verbunden sind.

Umsetzung:

Das interne WLAN und das Gäste-WLAN sind strikt zu trennen, sodass das Gäste-WLAN aus Sicht des internen LANs ein externes Netzwerk darstellt. Direkte Zugriffe aus dem Gäste-WLAN auf interne IT-Systeme dürfen nicht möglich sein.

Darüber hinaus sollte aber auch beim Gäste-WLAN sichergestellt werden, dass sich nur autorisierte Geräte mit dem WLAN verbinden dürfen (Gäste-WLAN-Passwort, Geräte-Accounts, ...).

Hardening von IT-Systemem [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Durch das Hardening von IT-Systemen sollen potenzielle Angriffspunkte oder mögliche Schwachstellen von IT-Systemen minimiert werden.

Umsetzung:

Das Hardening von IT-Systemen umfasst die Deaktivierung aller nicht erforderlichen Dienste, Schnittstellen (auch z. B. Bluetooth o. Ä.) und Zugriffs-Accounts sowie das Setzen von sicherheitsrelevanten

Konfigurationseinstellungen gemäß entsprechender (Hersteller-) Empfehlungen. Auch der Startvorgang von Hardware ist durch sichere Boot-Mechanismen abzusichern (z. B. Aktivierung von SecureBoot bei der UEFI-Firmware).

Diese Maßnahmen sind sowohl auf IT-Endgeräten, Druckern, Multifunktionsgeräten, Servern als auch bei allen Softwarekomponenten erforderlich.

Berücksichtigung der IT-Sicherheit bei der Entwicklung von IT-Systemen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Durch die Berücksichtigung von Sicherheitsaspekten in allen Phasen der Entwicklung von IT-Systemen (Planung, Konzeption, Implementierung, Einführung) können potenzielle Sicherheitslücken und Angriffspunkte bereits vor der Produktivsetzung verhindert werden (Security by Design). Das ist sowohl bei Eigenentwicklungen als auch bei Auftragsentwicklungen oder zugekauften IT-Systemen zu berücksichtigen. Bei Auftragsentwicklungen oder zugekauften IT-Systemen ist eine vertragliche Vereinbarung dazu sinnvoll.

Umsetzung:

Die erforderlichen Absicherungsmaßnahmen für IT-Systeme müssen bereits in der Planungs- und Konzeptionsphase analysiert und spezifiziert werden. Die Umsetzung der notwendigen Absicherungsmaßnahmen muss dann vor der Einführung bzw. Produktivsetzung im Rahmen der Qualitätssicherung noch entsprechend geprüft werden.

Mögliche Absicherungsmaßnahmen für IT-Systeme sind beispielsweise:

- Verschlüsselte Speicherung der Passwörter aller Zugriffs-Accounts
- Absicherung von Schnittstellen und APIs durch z. B. erforderliche Verbindungsautorisierung oder Web-Application-Firewalls
- Schutz von Web-Applikationen vor SQL-Injection durch z. B. Prepared Statements
- Schutz vor Web-Applikationen vor Cross-Site Scripting (XSS) durch z. B. HTML-Escaping aller Benutzereingaben oder durch sichere Input-Validierung
- Schutz von Web-Applikationen vor Cross-Site Request Forgery (CSRF) durch z. B. CSRF-Tokens oder durch Same-Site-Cookies
- Schutz von Verbindungssitzungen gegen Hijacking und Fixation durch z. B. Secure & HttpOnly-Cookies oder durch automatischen Session-Timeout
- Schutz vor unerlaubtem Upload von Daten oder Inhalten

Verschlüsselung von gespeicherten Daten [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Die sichere Verschlüsselung von gespeicherten Daten soll das Ausspähen bzw. den Diebstahl von Daten bei einem ungewollten direkten Zugriff auf das Speicherungsmedium verhindern (SSD, HDD, USB-Stick, ...). Unter direktem Zugriff wird dabei ein technischer Datenzugriff auf das Speichermedium unter Umgehung von Autorisierungs- und Berechtigungssystemen verstanden.

Umsetzung:

Die Speicherung von Daten auf mobilen IT-Endgeräten (Notebooks, Smartphones), auf extern betriebenen Servern und Datenspeichern (Cloud, Outsourcing, ...) oder auf Wechseldatenträgern (USB-Sticks, ...) muss verschlüsselt unter Nutzung geeigneter und transparenter Verschlüsselungsmethoden erfolgen. Dabei ist auch ein geeignetes Schlüssel- und Zertifikatsmanagement zu berücksichtigen.

Benutzer:innenauthentifizierung und rollenbasierte Berechtigungssysteme / -Vergabe [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Der Zugriff auf IT-Systeme darf nur autorisierten Benutzer:innen mit einem persönlichen, der Benutzer:in direkt zuordenbaren Login erfolgen. Um sicherzustellen, dass autorisierte Benutzer:innen nur auf Funktionalitäten und Daten zugreifen können, die sie zur Ausübung ihrer beruflichen Tätigkeiten benötigen ("need-to-know"), muss der Zugriff auf Funktionalitäten und Daten über ein rollenbasiertes Berechtigungssystem gesteuert werden.

Umsetzung:

Es dürfen sowohl auf Infrastrukturebene (IT-Endgeräte, Server, Drucker, Multifunktionsgeräte, ...) als auch auf Fachanwendungsebene nur IT-Systeme eingesetzt werden, bei denen der Zugang nur nach einer personenbezogenen Benutzer:innenauthentifizierung möglich ist und bei denen die Zugriffssteuerung erfolgt (sofern diese Differenzierung notwendig ist). Zum Identitätsnachweis bei der Benutzer:innenauthentifizierung sind ein sicheres Passwort und/oder sichere biometrische Merkmale erforderlich (Fingerabdruck, Gesichtserkennung, ...).

Passwort-Policy zur Sicherstellung "sicherer" Passwörter [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Die Vorgabe und Sicherstellung "sicherer" Passwörter für die Benutzer:innenauthentifizierung in IT-Systemen sind erforderlich, um das Hacken des Logins zu IT-Systemen mit dem Ziel des unautorisierten Zugriffs zu verhindern oder erheblich zu erschweren.

Umsetzung:

Die Vorgabe von "sicheren" Passwörtern und eines "sicheren" Authentifizierungsvorgangs muss in einer Passwort-Policy festgeschrieben und aufgrund laufend weiterentwickelter Angriffsmethoden kontinuierlich angepasst werden. Aktuelle Best-Practices für die Gestaltung "sicherer" Passwörter sind verlässlichen Quellen zu entnehmen (z. B. Empfehlung des BSI: BSI – Sichere Passwörter erstellen).

Die Umsetzung der Passwort-Policy und von Änderungen in der Passwort-Policy ist in allen IT-Systemen verbindlich durchzuführen. Dabei sind die IT-Systeme so zu konfigurieren, dass nur der Passwort-Policy entsprechende Passwörter vergeben werden können.

Multifaktorauthentifizierung für Zugriffe von externen Netzwerken [STARK EMPFOHLEN]

>

> **Ziele/Nutzen**: Ist der Zugriff auf IT-Systeme auch von externen Netzwerken erlaubt (z. B. im Rahmen von Home-Office), so ist zur Absicherung des Zugriffs von unerwünschten Personen (die z. B. Username + Passwort regulärer User:innen ausgespäht haben) eine Absicherung mittels einer Multifaktorauthentifizierung erforderlich.

Umsetzung:

Für Zugriffe auf IT-Systeme von externen Netzwerken ist die Einrichtung einer zusätzlichen Bestätigung einer Systemanmeldung über einen getrennten, nur der autorisierten User:in zugänglichen Kommunikationskanal erforderlich (=Multifaktorauthentifizierung). Diese zusätzliche Bestätigung kann z. B. über eine Authentifizierungs-App auf einem persönlichen Smartphone oder über eine SMS oder einen Telefonanruf erfolgen.

Sicherstellung von Bildschirmsperren [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Um die ungewollte Nutzung von unbeaufsichtigten IT-Endgeräten durch nicht berechtigte Personen zu verhindern, ist es notwendig, die Benutzer:innen im Rahmen einer Regelung zu verpflichten, beim Verlassen des Arbeitsplatzes das IT-Endgerät zu sperren. Als weitere Vorsorge ist die Einrichtung einer automatischen Bildschirmsperre nach kurzer Inaktivität notwendig.

Umsetzung:

Es ist eine Verbindliche, allen Benutzer:innen zur Kenntnis zu bringende Regelung zu erstellen, die die Benutzer:innen verpflichtet, beim Verlassen des Arbeitsplatzes das eigene IT-Endgerät zu sperren. Außerdem sind alle IT-Geräte so zu konfigurieren, dass nach einer definierten Zeit (aktuelle Empfehlung des BSI: 5 Minuten) ab der letzten Benutzer:innen-Aktivität das IT-Endgerät automatisch gesperrt wird (Aktivierung der Bildschirmsperre).

Festlegung und Umsetzung notwendiger IT-Maßnahmen bei Onboarding / Offboarding / Stellenwechsel [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Um beim Onboarding und bei einem Stellenwechsel von Mitarbeiter:innen die Zuweisung / Bereitstellungen der notwendigen IT-Systeme und die Vergabe der notwendigen Zugriffsberechtigungen sicherzustellen, sind entsprechende Regelungen und Prozesse notwendig. Beim Offboarding sowie beim Stellenwechsel sind zusätzlich Regelungen und Prozesse zum Entzug der bisherigen Zugriffsberechtigungen bzw. die Rückgabe von IT-Endgeräten vorzusehen, um so nicht mehr erforderliche und ungewollte Datenzugriffe zu verhindern.

Umsetzung:

Die erforderlichen Prozesse für Onboarding, Offboarding und einen Stellenwechsel sind zu definieren und in der Organisation einzuführen. Beim Entzug bisheriger Zugriffsberechtigungen bzw. bei der Rückgabe von IT-Geräten im Rahmen des Offboardings oder bei einem Stellenwechsel ist auch der Umgang mit Daten, die aus etwaiger Privatnutzung dienstlicher IT-Geräte stammen sowie die Übergabe der dienstlichen Daten an eine Nachfolger:in zu regeln.

Festlegung und Umsetzung eines Vorgehens bei IT-Sicherheitsverletzungen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Um bei IT-Sicherheitsverletzungen (Cyberangriffe, unberechtigte Zugriffe, ...) eine möglichst rasche Reaktion zur Durchführung notwendiger Abwehrmaßnahmen und von Maßnahmen zur Minimierung negativer Auswirkungen sicherzustellen, ist eine detaillierte Festlegung des Vorgehens bei IT-Sicherheitsverletzungen inkl. aller relevanter Zuständigkeiten erforderlich.

Umsetzung:

Ausgangspunkt für das Vorgehen zur Reaktion auf IT-Sicherheitsverletzungen ist das Erkennen der IT-Sicherheitsverletzung aufgrund entsprechender Alarme von IT-Schutzdiensten, einer manuellen Erkennung oder aufgrund von externen Meldungen. Im Rahmen des zu definierenden Vorgehens sind zumindest folgende Maßnahmen vorzusehen:

- Erstanalyse der IT-Sicherheitsverletzung und etwaige Durchführung von Sofortmaßnahmen zur Schadensabwehr
- Kommunikation / Meldung der Sicherheitsverletzung an relevante Stellen (Management, Fachabteilungen, Cyber-Versicherung, Datenschutzbehörde, ...)
- Umfassende Analyse der IT-Sicherheitsverletzung, Umsetzung nachhaltiger Maßnahmen zur Problemlösung und (sofern erforderlich) zur Behebung / Minimierung von etwaigen Schäden
- Dokumentation der IT-Sicherheitsverletzung

Zur Umsetzung dieses Vorgehens sind die notwendigen organisatorischen Maßnahmen inkl. Verfügbarkeit und Erreichbarkeit von qualifiziertem Personal zu setzen.

Festlegung und Umsetzung eines Verfahrens für die Meldung von Geräteverlusten / Diebstahl [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Um im Fall des Verlusts oder des Diebstahls von IT-Endgeräten mögliche negative Auswirkungen zu vermeiden, ist ein entsprechendes Meldeverfahren inkl. der Erreichbarkeit von zuständigen IT-Mitarbeiter:innen erforderlich.

Umsetzung:

Es ist ein Meldeverfahren für den Verlust oder Diebstahl von IT-Endgeräten festzulegen und die notwendigen organisatorischen Maßnahmen zur Umsetzung inkl. Verfügbarkeit und Erreichbarkeit von qualifiziertem Personal zu setzen.

Vereinbarung der notwendigen IT-Sicherheitsmaßnahmen (bei Systemoutsourcing / Cloudservices) [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Bei IT-Systemen, die von externen IT-Dienstleistern betrieben werden (Outsourcing, Cloudlösungen) besteht kein direkter Einfluss auf die Umsetzung der erforderlichen Maßnahmen zur

> Informationssicherheit. Zur Sicherstellung der erforderlichen Maßnahmen zur Informationssicherheit ist daher eine entsprechende vertragliche Absicherung erforderlich.

Umsetzung:

Die durch den externen IT-Dienstleister sicherzustellenden Maßnahmen zur Informationssicherheit sind in den vertraglichen Vereinbarungen mit dem externen IT-Dienstleister entsprechend zu berücksichtigen. Dabei muss auch festgelegt werden, wie der externe IT-Dienstleister die Umsetzung der erforderlichen Maßnahmen zur Informationssicherheit nachzuweisen hat. Bei fehlender oder mangelhafter Umsetzung von Maßnahmen zur Informationssicherheit sind entsprechende Korrekturmaßnahmen und/oder Pönalzahlungen vorzusehen.

Bei besonders kritischen IT-Systemen kann auch eine regelmäßige Auditierung der Maßnahmen zur Informationssicherheit beim externen IT-Dienstleister vorgesehen werden.

IT-Security-Awareness-Ausbildung für Benutzer:innen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Ziel einer IT-Security-Awareness-Ausbildung ist die Sensibilisierung der IT-Benutzer:innen hinsichtlich möglicher Cybergefahren und die Ausbildung der IT-Benutzer:innen im Umgang mit diesen Cybergefahren u. a. zur Vermeidung möglicher Schäden.

Umsetzung:

Es sind geeignete Kurse zur IT-Security-Awareness auszuwählen und zu beschaffen (eLearnings, Klassenraumkurse, ...), die dann alle Benutzer:innen absolvieren müssen. Geeignete Kurse zur IT-Security-Awareness müssen zumindest die häufigsten Cybergefahren (bei Mails, im Internet, ...), Methoden des Social Engineerings und die notwendigen Maßnahmen bei erkannten Cybergefahren beinhalten.

Nach der Erstausbildung sollte die IT-Security-Awareness-Ausbildung regelmäßig aktualisiert und durch die Benutzer:innen auch wiederholt absolviert werden.