Leitfaden für die IT-Sicherheit beim Umgang mit und bei der Beförderung von sonstigen radioaktiven Stoffen
basierend auf den IT-Sicherungsanforderungen der SEWD-Richtlinie sonstige radioaktive Stoffe Version 1.0

vom 8. Dezember 2021

Inhaltsverzeichnis

1 Einleitung

Informationen sind ein wesentlicher Wert für Unternehmen und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar. [1]

Die Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und bei der Beförderung von sonstigen radioaktiven Stoffen (SEWD-Richtlinie sonstige radioaktive Stoffe) [2] stellt unter anderem Anforderungen an den Einsatz von Informationstechnik, die Bestandteil von Sicherungsmaßnahmen ist oder anderweitig zu einer Schutzzielverletzung beitragen kann. Diese Anforderungen gelten für den Umgang mit und für die Beförderung von sonstigen radioaktiven Stoffen aller Sicherungsstufen. Zudem fordert auch die DIN 25422 (05-2021 – Norm zum Strahlen-, Brand- und Diebstahlschutz) [3] die Umsetzung der Standard-Sicherungsmaßnahmen des IT-Grundschutzes, weshalb dieser IT-Leitfaden auch unterstützend für die Umsetzung der DIN-Norm herangezogen werden kann.

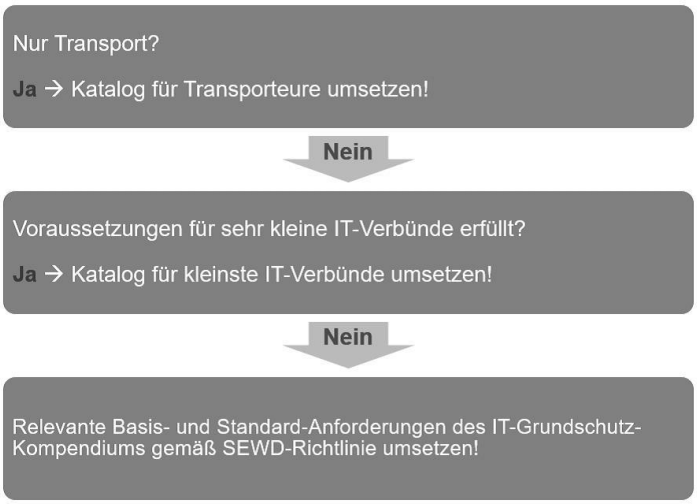
Der vorliegende Leitfaden enthält Anforderungen an den Einsatz von Informationstechnik, um ein Sicherungsniveau zu gewährleisten, das den Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums [4] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht. Der vor 25 Jahren eingeführte IT-Grundschutz des BSI bildet die konzeptionelle Grundlage zur systematischen Erstellung eines Informationssicherheits-Managementsystems (ISMS) und von IT-Sicherheitskonzepten. In diesem Sinne entwickelte das BSI das IT-Grundschutz-Kompendium sowie die BSI-Standards 200-1 bis 200-3. Darin wird erläutert, wie ein ISMS aufgebaut werden kann und welche Geschäftsprozesse bzw. Fachaufgaben wie abgesichert werden können. In diversen IT-Grundschutz-Bausteinen legt das IT-Grundschutz-Kompendium dar, welche Anforderungen bei den unterschiedlichen Themen der Informationssicherheit zu beachten sind. In rund 100 dieser IT-Grundschutz-Bausteine sind neben technischen auch infrastrukturelle, organisatorische und personelle Aspekte beschrieben.

Dieser Leitfaden dient als Hilfestellung zur Umsetzung der SEWD-Richtlinie sonstige radioaktive Stoffe. Er richtet sich an die für den Strahlenschutz zuständigen Genehmigungs- und Aufsichtsbehörden, die durch die Anwendung des Leitfadens die Umsetzung des IT-Grundschutzes zielgerichteter und daher schneller prüfen können. Mittelbar unterstützt er auch Genehmigungsinhaber und Antragsteller, die mit sonstigen radioaktiven Stoffen umgehen oder diese befördern, z. B. Strahlentherapieeinrichtungen, Großbestrahlungsanlagen, Betriebe der zerstörungsfreien Werkstoffprüfung oder Transportunternehmen.

Unternehmen mit großen Informationsverbünden werden i. d. R. eigene Organisationseinheiten vorhalten, die die IT-Sicherheitsanforderungen unter Anwendung des IT-Grundschutz-Kompendiums des BSI kompetent umsetzen können. Daher dient der Leitfaden insbesondere als Umsetzungshilfe für kleine Unternehmen mit kleinsten Informationsverbünden (IT-Anforderungen an kleinste Informationsverbünde) und für Unternehmen, die sonstige radioaktive Stoffe befördern (Anforderungskatalog zum Nachweis der IT-Sicherheit bei der Beförderung von sonstigen radioaktiven Stoffen).

Zu beachten ist, dass dieser Leitfaden lediglich solche Anforderungen an die Informationssicherheit behandelt, die aus dem Umgang mit oder der Beförderung von sonstigen radioaktiven Stoffen resultieren. Je nach Anwendungsfall können weitere rechtliche, externe oder interne Anforderungen bestehen, die zusätzliche oder höherwertigere Maßnahmen der Informationssicherheit notwendig machen.

Als Orientierungshilfe, welches Dokument zur Prüfung und Umsetzung des IT-Grundschutzes im Einzelfall geeignet ist, soll dieses Schaubild dienen:



2 IT-Sicherheitsanforderungen an kleinste Informationsverbünde

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Auftrag des BMU „ITSicherheitsanforderungen an kleinste Informationsverbünde zur Sicherung sonstiger radioaktiver Stoffe“ erstellt. Das Dokument erläutert die Anforderungen des IT-Grundschutz-Kompendiums des BSI in einer für kleinste Informationsverbünde angepassten Form und erleichtert einerseits Genehmigungsinhabern und Antragstellern die Umsetzung des IT-Grundschutzes und unterstützt andererseits die Genehmigungs- und Aufsichtsbehörden bei der Prüfung.

Auch in großen Unternehmensstrukturen können die IT-Sicherheitsanforderungen für kleinste Informationsverbünde Anwendung finden. Hierzu enthält das Dokument entsprechende Vorgaben, unter welchen Voraussetzungen es anwendbar ist und wann stattdessen die reguläre IT-Grundschutz-Methodik anzuwenden ist.

Die IT-Sicherheitsanforderungen an kleinste Informationsverbünde sind als Anhang A dieses Rahmendokumentes beigefügt und wird in regelmäßigen Abständen an den Stand der Technik angepasst.

3 Anforderungskatalog zum Nachweis der IT-Sicherheit bei der Beförderung von sonstigen radioaktiven Stoffen

Im Hinblick auf die Beförderung von Großquellen wurde durch das Bundesamt für die Sicherheit der nuklearen Entsorgung in Zusammenarbeit mit der Sachverständigenorganisation TÜV Süd Industrie Service GmbH eine Konkretisierung der Standardmaßnahmen des BSI-Grundschutzes erarbeitet. Die Ergebnisse dieser Arbeiten sind in einem „Anforderungskatalog zum Nachweis der IT-Sicherheit bei der Beförderung von Großquellen“ zusammenfassend dargestellt (s. hierzu unter *www.base.bund.de*)

Basierend darauf wurde übergreifend für die Beförderung von sonstigen radioaktiven Stoffen ein Anforderungskatalog entwickelt, der sich – wie auch die IT-Sicherheitsanforderungen an kleinste Informationsverbünde – an Genehmigungsinhaber und Antragsteller sowie an Genehmigungs- und Aufsichtsbehörden richtet, um die Anforderungen des ITGrundschutzes für die Beförderung von sonstigen radioaktiven Stoffen einfacher umsetzen und prüfen zu können.

Das Dokument ist als Anhang B dieses Rahmendokumentes beigefügt und wird in regelmäßigen Abständen durch das BMU an den Stand der Technik und Erkenntnis angepasst.

4 Weitere Informationen und Hinweise

Das BSI bietet auf seiner Internetseite verschiedene Möglichkeiten zur Unterstützung an. So gibt es z. B. eine Liste mit zertifizierten IT-Dienstleistern, die die Umsetzung der benötigten IT-Anforderungen begleiten und/oder begutachten können. Des Weiteren stehen ein Glossar mit den wichtigsten Fachbegriffen, verschiedene Bildungsangebote und Vorlagen für Sicherheitskonzepte zur Verfügung. In der nachfolgenden Tabelle werden hilfreiche Informationen und Hinweise aufgeführt:

Thema	**Internetlink**
Strahlenschutzgesetz	https://www.gesetze-im-internet.de/strlschg/
Glossar	https://www.bsi.bund.de/cyberglossar
IT-Grundschutz	https://www.bsi.bund.de/grundschutz
Zertifizierte ISO 27001-Auditoren für Audits auf der Basis von IT-Grundschutz	https://www.bsi.bund.de/auditoren
Zertifizierte IT-Grundschutz-Beratung	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Personen/GS-Berater/Liste-Grundschutzberater/liste-grundschutzberater_node.html
BSI-Standards	https://www.bsi.bund.de/gs-standards
IT-Grundschutz-Kompendium	https://www.bsi.bund.de/gs-kompendium
Online-Kurs – Informationssicherheit mit IT-Grundschutz	https://www.bsi.bund.de/grundschutzkurs
Arbeitsbeispiel RECPLAST GmbH	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/recplast_node.html

Referenzen

[1] Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Standard 200-2 „IT-Grundschutz-Methodik“.

https://www.bsi.bund.de/gs-standards

[2] Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (2020): Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und bei der Beförderung von sonstigen radioaktiven Stoffen (Revision 1.0). Bonn: 11.02.2020. VS – NUR FÜR DEN DIENSTGEBRAUCH.

[3] Beuth-Verlag (05/2021): DIN 25422. Aufbewahrung und Lagerung sonstiger radioaktiver Stoffe – Anforderungen an Aufbewahrungseinrichtungen und deren Aufstellungsräume zum Strahlen-, Brand- und Diebstahlschutz.

[4] Bundesamt für Sicherheit in der Informationstechnik (2021): IT-Grundschutz-Kompendium (Edition 2021). *https://www.bsi.bund.de/gs-kompendium*

Anhang A
IT-Sicherheitsanforderungen an kleinste Informationsverbünde zur Sicherung sonstiger radioaktiver Stoffe
Version 1.0

1 Vorbemerkungen

Die SEWD-Richtlinie für sonstige radioaktive Stoffe[1] fordert zu Erfüllung der Genehmigungsvoraussetzung nach StrlSchG die Sicherstellung des erforderlichen Schutzes gegen SEWD. In Bezug auf gefährdete IT-Systeme fordert sie den Nachweis der Informationssicherheit. Die SEWD-Richtlinie fordert hierzu die Einhaltung eines IT-Sicherheitsniveaus, das den Standard-Sicherheitsanforderungen des IT-Grundschutzes[2] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht. Anzuwenden ist dies auf die genutzte Informationstechnik, die Bestandteil von Sicherungsmaßnahmen ist oder anderweitig zu einer Schutzzielverletzung beitragen kann.

Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im Informationssicherheitsprozess zu reduzieren. Dazu werden bekannte Ansätze und Methoden zur Verbesserung und Aufrechterhaltung der Informationssicherheit gebündelt und kontinuierlich aktualisiert. Ergänzend veröffentlicht das BSI im IT-Grundschutz-Kompendium Bausteine mit konkreten Sicherheitsanforderungen für typische Prozesse, Anwendungen, Systeme, Kommunikationsverbindungen und Infrastruktur, die nach Bedarf in der eigenen Institution eingesetzt werden können. Im IT-Grundschutz werden alle Bereiche einer Institution betrachtet, dazu gehören Produktion und Fertigung mit Industrial Control Systems (ICS) ebenso wie Komponenten aus dem Bereich des Internet of Things (IoT).

Zwar bietet der IT-Grundschutz eine sehr effiziente Methode, um ein angemessenes IT-Sicherheitsniveau zu erreichen, dennoch ist dies für sehr kleine IT-Landschaften aufgrund der begrenzten Ressourcen oft eine Herausforderung. Dieses Dokument bietet daher für die in Kapitel 2 aufgeführten Spezialfälle eine vereinfachte Vorgehensweise. Hierzu richtet sich das vorliegende Dokument sowohl an die zuständigen Genehmigungs- und Aufsichtsbehörden als auch an Antragsteller bzw. Genehmigungsinhaber, die die SEWD-Richtlinie für sonstige radioaktive Stoffe umsetzen müssen und die in Kapitel 2 aufgeführten Voraussetzungen erfüllen.

2 Anwendungsweise

2.1 Methodik

Für die IT-Sicherheitskonzeption ist im BSI-Standard 200-2 mit der „Standard-Absicherung“ eine Vorgehensweise definiert. Ein wesentlicher Schritt ist dabei die Festlegung des Geltungsbereichs, für den das Sicherheitskonzept gelten soll. Dies wird beim IT-Grundschutz als „Informationsverbund“ bezeichnet.

Die Prozesse, Anwendungen, Systeme, Kommunikationsverbindungen und die baulich-physische Infrastruktur, die Bestandteile eines Informationsverbunds sind, heißen „Zielobjekte“.

Ausgehend vom Informationsverbund werden dann mittels Strukturanalyse, Schutzbedarfsfeststellung und Modellierung die notwendigen IT-Grundschutz-Bausteine und somit die notwendigen Sicherheitsanforderungen abgeleitet. Relevant für die Umsetzung der SEWD-Richtlinie sind die „Basis-Anforderungen“ und die „Standard-Anforderungen“ der jeweiligen IT-Grundschutz-Bausteine. Hinsichtlich der Modalverben MUSS, DARF NUR, DARF NICHT, DARF KEIN, SOLLTE, SOLLTE NICHT und SOLLTE KEIN in den IT-Grundschutz-Bausteinen gelten die entsprechenden Hinweise im IT-Grundschutz-Kompendium.

Um diese Vorgehensweise für sehr kleine Geltungsbereiche abzukürzen, wird im Folgenden ein minimaler Informationsverbund definiert, für den in Kapitel 3 ein Katalog mit vorgefertigten IT-Sicherheitsanforderungen aufgeführt ist. Die Anwendung des IT-Grundschutz wird auf diese Weise vereinfacht.

Für die Anforderungen aus dem Bereich der baulich-physischen Infrastruktur (Gebäude, Räume, Schränke, Verkabelung, etc.) wird auf die relevanten IT-Grundschutz-Bausteine verwiesen, da diese Anforderungen in geringerem Maße von der Größe des Informationsverbundes abhängen als die IT-bezogenen Bausteine.

2.2 Abgrenzung

Gemäß der SEWD-Richtlinie für sonstige radioaktive Stoffe muss der Informationsverbund die genutzte Informationstechnik, die Bestandteil von Sicherungsmaßnahmen ist oder anderweitig zu einer Schutzzielverletzung beitragen kann, abdecken.

[1] „Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und bei der Beförderung von sonstigen radioaktiven Stoffen“, Revision 1.0, 11.02.2020, Az. S II 3 – 13151/2 VS-NfD
[2] https://www.bsi.bund.de/grundschutz

Für Informationsverbünde, in denen die Anzahl von Zielobjekten die in Abschnitt 2.3 festgelegten Obergrenzen übersteigt oder die anderweitig von dem hier dargestellten Informationsverbund abweichen, sind die vorgefertigten IT-Sicherheitsanforderungen in Kapitel 3 nicht geeignet. Für solche Informationsverbünde muss die reguläre IT-Grundschutz-Methodik angewandt werden.

Wenn der hier betrachtete Informationsverbund ein Teil einer größeren IT-Landschaft ist[3], dann muss der Informationsverbund mindestens durch einen zustandsbehafteten Paketfilter von der restlichen IT-Landschaft abgetrennt werden. Es gelten die Anforderungen aus Abschnitt 3.13 zur Netztrennung.

Alternativ können auch andere Vorgehensweisen der Informationssicherheit – beispielsweise eine individuelle Risikoanalyse – angewandt werden, sofern sichergestellt ist, dass das gleiche Sicherheitsniveau erreicht wird, wie durch die Standard-Sicherheitsanforderungen des IT-Grundschutz-Kompendiums.

Aspekte des Datenschutzes und des Geheimschutzes (Schutz staatlicher Verschlusssachen) werden durch die vorgefertigten IT-Sicherheitsanforderungen in Kapitel 3 nicht abgedeckt und müssen separat betrachtet werden.

2.3 Zielobjekte

Die in Kapitel 3 aufgeführten IT-Sicherheitsanforderungen gelten für Informationsverbünde, die höchstens folgende Zielobjekte umfassen:

- Geschäftsprozesse:
  - Verwaltung von und Umgang mit sonstigen radioaktiven Stoffen
  - Schutz sonstiger radioaktiver Stoffe vor Entwendung und Freisetzung
- Anwendungen:
  - Anwendungen zur Unterstützung der vorgenannten Geschäftsprozesse
  - Webbrowser
- Netze:
  - Internes LAN
  - Internet-Zugang
- IT-Systeme/sonstigen Geräte:
  - Bis zu 5 allgemeine Clients
  - Bis zu 2 dedizierte Administrations-Clients
  - Bis zu 3 Gefahrenmeldeanlagen
  - Bis zu 2 Router
  - Bis zu 2 Firewalls
  - Bis zu 5 Drucker, Kopierer oder Multifunktionsgeräte
- Räume:
  - Bis zu 5 Büroarbeitsplätze
  - Bis zu 5 Räume oder Schränke für technische Infrastruktur

Darüber hinaus kann der Informationsverbund folgende zusätzliche Zielobjekte umfassen. In diesem Fall sind allerdings – ergänzend zu den vorgefertigten IT-Sicherheitsanforderungen in Kapitel 3 – weitere Bausteine aus dem IT-Grundschutz-Kompendium umzusetzen (Basis-Anforderungen und Standard-Anforderungen):

- Geschäftsprozess „Fernwartung“:
  Hierfür sind zusätzlich die Bausteine OPS.1.2.5 „Fernwartung“ und NET.3.3 „VPN“ umzusetzen.
- Geschäftsprozess „Nutzung von Outsourcing“:
  Hierfür ist zusätzlich der Baustein OPS.2.1 „Outsourcing für Kunden“ umzusetzen.

[3] Ein Beispiel hierfür ist ein größeres Unternehmen, in dem nur eine kleine Abteilung mit sonstigen radioaktiven Stoffen umgeht.

- Geschäftsprozess „Cloud-Nutzung“:
  Hierfür ist zusätzlich der Baustein OPS.2.2 „Cloud-Nutzung“ umzusetzen.

- Anwendungen „Office-Anwendungen“:
  Hierfür ist zusätzlich der Baustein APP.1.1 „Office-Produkte“ umzusetzen.

- IT-Systeme „Smartphones und Tablets“ (insgesamt höchstens 5 Geräte):
  Hierfür sind zusätzlich die Bausteine APP.1.4 „Mobile Anwendungen“ und SYS.3.2.1 „Allgemeine Smartphones und Tablets“ sowie – falls jeweils relevant – die Bausteine SYS.3.2.3 „iOS (for Enterprise)“ und SYS.3.2.4 „Android“ umzusetzen.

- Wenn die allgemeinen Clients vollständig oder teilweise als Laptops realisiert sind (insgesamt höchstens 5 allgemeine Clients, einschließlich Laptops):
  Hierfür ist zusätzlich der Baustein SYS.3.1 „Laptops“ umzusetzen.

- Netze „WLAN“:
  Hierfür sind zusätzlich die Bausteine NET.2.1 „WLAN-Betrieb“ und NET.2.2 „WLAN-Nutzung“ umzusetzen.

- Infrastruktur „Fahrzeuge“ (insgesamt höchstens 5 Fahrzeuge):
  Hierfür ist zusätzlich der Baustein INF.11 „Allgemeines Fahrzeug“ umzusetzen.

Bei allen anderen Erweiterungen des Informationsverbundes sind die vorgefertigten IT-Sicherheitsanforderungen in Kapitel 3 nicht geeignet. Es muss dann stattdessen die reguläre IT-Grundschutz-Methodik angewandt werden.

2.4 Umsetzung

Grundsätzlich sind alle Anforderungen aus Kapitel 3 – sowie ggf. die in Abschnitt 2.3 genannten zusätzlichen IT-Grundschutz-Bausteine – für die jeweils relevanten Zielobjekte des betrachteten Informationsverbundes umzusetzen. Folgende Gründe können jedoch dazu führen, dass Anforderungen (teilweise) nicht umgesetzt werden können oder nicht umgesetzt werden müssen:

- Eine IT-Sicherheitsanforderung ist unter Umständen entbehrlich, wenn die entsprechenden Prozesse oder Komponenten, von denen die Gefahr ausgeht, nicht eingesetzt werden. Beispielsweise müssen Wechseldatenträger nicht für den Versand gekennzeichnet werden, wenn sie nicht versandt werden.

- Eine IT-Sicherheitsanforderung ist unter Umständen entbehrlich, wenn alternative Maßnahmen umgesetzt sind, die mindestens die gleichen Sicherheitsziele erfüllen. Beispielsweise kann bei einem IT-System, das keine Authentisierung von Benutzern unterstützt, ersatzweise eine Zutrittskontrolle mit individuell dokumentierter und nachvollziehbarer Schlüsselausgabe erfolgen.

- Eine IT-Sicherheitsanforderung kann unter Umständen aufgrund übergeordneter Vorschriften (Gesetze, Verordnungen, etc.) nicht umgesetzt werden. Beispielsweise dürfen unter Umständen bestimmte Informationen aus Gründen des Datenschutzes nicht protokolliert werden.

- Eine IT-Sicherheitsanforderung kann unter Umständen aus zwingenden technischen Gründen nicht umgesetzt werden. Beispielsweise ist es nicht bei jedem IT-System technisch möglich, dass jeder Benutzer mit seiner eigenen individuellen Kennung arbeitet.

Wenn Anforderungen ganz oder teilweise entbehrlich sind, muss dies für jede Anforderung einzeln nachvollziehbar begründet werden.

Wenn Anforderungen ganz oder teilweise nicht umgesetzt werden können, müssen alternative Maßnahmen umgesetzt werden, die unter Einhaltung der jeweiligen Rahmenbedingungen ein möglichst vergleichbares IT-Sicherheitsniveau bieten. Dies muss für jede Anforderung einzeln nachvollziehbar begründet werden.

3 IT-Sicherheitsanforderungen

Die folgenden IT-Sicherheitsanforderungen gelten für die in den Kapiteln 1 und 2 dargestellten Anwendungsfälle.

Die jeweils in Klammern hinter den Anforderungen aufgeführten Kürzel verweisen auf Anforderungen im IT-Grundschutz-Kompendium, in denen vergleichbare Sicherheitsziele behandelt werden. Beispielsweise verweist „ORP.1.A1/A2“ auf die Anforderungen A1 und A2 im IT-Grundschutz-Baustein ORP.1 „Organisation“. Diese Verweise sind rein informativ und sollen als Nachschlagehilfe dienen, wenn weiterführende Informationen zu dem jeweiligen Thema gesucht werden. (Das Kürzel „SYS.4.X“ verweist auf den noch im Entwurf befindlichen Baustein zum Thema „Gefahrenmeldeanlagen“.)

Nicht alle Anforderungen aus dem IT-Grundschutz-Kompendium können unverändert auf sehr kleine Informationsverbünde angewandt werden. Im vorliegenden Dokument wurden daher zahlreiche Anpassungen an die in Kapitel 2 dargestellten Anwendungsfälle vorgenommen.

3.1 Management

Für den Themenbereich „Management der Informationssicherheit“ müssen folgende Anforderungen erfüllt werden:

- Die Geschäftsführung muss die Gesamtverantwortung für Informationssicherheit übernehmen und sicherstellen, dass das erforderliche Sicherheitsniveau erreicht und dauerhaft aufrechterhalten wird. (ISMS.1.A1)
- Die Geschäftsführung muss die notwendigen Ressourcen für die Informationssicherheit sowie für die Administration und den Betrieb der Informationstechnik bereitstellen. (ISMS.1.A1/A4/A6/A15, DER.1.A6, DER.3.1.A10, OPS.1.1.2.A9, OPS.1.1.5.A6)
- Die Geschäftsführung muss festlegen, wer welche Aufgaben im Bereich der Informationssicherheit hat. (ISMS.1.A1/A4/A6/A15, DER.3.1.A10)
- Die Geschäftsführung muss sich mindestens jährlich über den Stand der Informationssicherheit, mögliche Risiken und Konsequenzen von Mängeln informieren. (ISMS.1.A1/A12, DER.2.1.A17)
- Die Geschäftsführung muss für Fragen der Informationssicherheit sensibilisiert werden und mit gutem Beispiel vorangehen. (ISMS.1.A1, ORP.3.A1)
- Die Geschäftsführung muss ein Sicherheitskonzept festlegen, in dem alle Vorgaben und Maßnahmen beschrieben sind, um das erforderliche Sicherheitsniveau zu erreichen. (ISMS.1.A2/A3/A7/A10)
- Die Geschäftsführung muss den Stellenwert der Informationssicherheit und die Sicherheitsziele in einer Leitlinie zur Informationssicherheit dokumentieren. (ISMS.1.A3)
- Die Geschäftsführung muss festlegen, welche Regelungen die Mitarbeiter bei der Nutzung von Informationstechnik einhalten müssen. (SYS.4.1.A4/A5, SYS.4.5.A4/A5)
- Die Geschäftsführung muss die Einhaltung der Regelungen einfordern. Verstöße müssen kommuniziert werden. (ORP.3.A1/A3)
- Die Geschäftsführung muss sicherstellen, dass in allen Bereichen jederzeit ein aktueller Überblick über alle relevanten Vorgaben besteht, dass die Vorgaben dauerhaft umgesetzt werden und dass deren Einhaltung kontrolliert wird. (ORP.5.A4, APP.6.A2, SYS.2.1.A42)
- Die Geschäftsführung muss sicherstellen, dass alle relevanten gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG, LDSG) eingehalten werden. (CON.2.A1)
- Die Geschäftsführung muss die Ziele und Prioritäten von Überprüfungen festlegen. (DER.3.1.A2/A26)
- Die Geschäftsführung muss nachhalten, dass Abweichungen und Mängel, die bei Überprüfungen der Informationssicherheit festgestellt wurden, zeitnah behoben werden. Veraltete Konzepte, Regelungen und Entscheidungen müssen zeitnah auf den aktuellen Stand gebracht werden. (ISMS.1.A2/A7/A11, CON.6.A4/A8, ORP.4.A14, OPS.1.1.2.A7/A9, OPS.1.1.4.A1, OPS.1.1.5.A1/A3, DER.1.A1/A3/A13, DER.2.1.A2/A5/A7/A14, APP.6.A10, SYS.2.1.A9/A43, SYS.4.5.A4, NET.1.1.A13/A14/A15/A16/A17/A22/A25, NET.3.1.A10/A12/A23, NET.3.2.A1, DER.3.1.A3/A4/A5/A7/A8/A10/A19/A25/A26)
- In größeren Unternehmen hat es sich bewährt, die Koordinierung der Belange der Informationssicherheit einem Informationssicherheitsbeauftragten (ISB) zu übertragen. Wird ein ISB benannt, muss er bei allen relevanten Aktivitäten beteiligt werden und sich bei Mängeln direkt an die Geschäftsführung wenden können. Die Gesamtverantwortung für Informationssicherheit verbleibt in jedem Fall bei der Geschäftsführung. Wenn kein ISB benannt wird, muss die Geschäftsführung dessen Aufgaben übernehmen. (ISMS.1.A4)
- Die Geschäftsführung muss sicherstellen, dass Informationssicherheit bei allen geplanten und laufenden Aktivitäten berücksichtigt wird. (ISMS.1.A9)
- Die Geschäftsführung muss schriftlich festlegen, was im Fall eines Sicherheitsvorfalls durch wen zu tun ist und wie sich die Mitarbeiter und Administratoren zu verhalten haben. (DER.2.1.A2/A3/A9/A12/A13/A14)
- Die Geschäftsführung muss festlegen, wer im Fall eines Sicherheitsvorfalls durch wen in welcher Tiefe informiert wird. (DER.2.1.A9/A14)

3.2 Compliance und Datensparsamkeit

Für den Themenbereich „Compliance und Datensparsamkeit“ müssen folgende Anforderungen erfüllt werden:

- Alle gesetzlichen, behördlichen, vertraglichen und sonstigen Vorgaben mit Bezug zur Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) müssen identifiziert werden. (ORP.5.A1)

- Die Verantwortlichkeiten und Zuständigkeiten für die Einhaltung der identifizierten Vorgaben müssen eindeutig zugewiesen werden. (ORP.5.A2)
- Die identifizierten Vorgaben müssen in alle relevanten Planungen, Konzepte, Regelungen und Beschaffungen einfließen. (ORP.5.A2)
- Es müssen Maßnahmen umgesetzt werden, um Verstöße gegen Vorgaben zu vermeiden. Wenn Verstöße erkannt werden, müssen unverzüglich sachgerechte Korrekturmaßnahmen ergriffen werden. (ORP.5.A2)
- Wenn in Einzelfällen eine Abweichung von Vorgaben erforderlich ist, darf dies nur auf der Grundlage einer Ausnahmegenehmigung erfolgen. Ausnahmegenehmigungen müssen begründet und befristet sowie durch eine autorisierte Stelle aufgrund einer Risikoabschätzung geprüft und genehmigt sein. (ORP.5.A5)
- Es muss regelmäßig geprüft werden, ob alle relevanten Vorgaben erfasst sind und systematisch eingehalten werden. (ORP.5.A8)
- Informationstechnik muss so konfiguriert werden, dass die identifizierten internen und externen Vorgaben eingehalten werden, beispielsweise im Bereich des Datenschutzes. (OPS.1.1.4.A5)
- Bei der Erstellung, Sammlung und Auswertung von Protokollierungsdaten und von Meldungen sicherheitsrelevanter Ereignisse muss sichergestellt werden, dass alle internen und externen Vorgaben eingehalten werden. Hierbei müssen insbesondere die Datenschutzgesetze, das Telemediengesetz, das Telekommunikationsgesetz und das Betriebsverfassungsgesetz sowie die Persönlichkeits- und Mitbestimmungsrechte berücksichtigt werden. (OPS.1.1.5.A5/A9, DER.1.A2)
- Bei der Erfassung und Auswertung von Daten für forensische Untersuchungen müssen alle rechtlichen sowie sonstigen relevanten internen und externen Vorgaben eingehalten werden. (DER.2.2.A1/A5)
- Bei der Durchführung und Dokumentation von Überprüfungen müssen etwaige Aufbewahrungspflichten eingehalten werden. (DER.3.1.A24/A27)
- Wenn die von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) entwickelte Methode des Standard-Datenschutzmodells nicht angewandt wird, muss dies begründet und dokumentiert werden. (CON.2.A1)
- Personenbezogene und personenbeziehbare Daten dürfen nicht für Software-Tests verwendet werden. (OPS.1.1.6.A11)
- Software muss so installiert und konfiguriert werden, dass möglichst wenig personenbezogene Daten erfasst und verarbeitet werden. (APP.6.A4)
- Webbrowser müssen so konfiguriert werden, dass Benutzer ihre Nutzungsdaten (Cookies, Historie/Verlauf, Autovervollständigung, etc.) löschen können. (APP.1.2.A7)
- Webbrowser müssen so konfiguriert werden, dass so wenig Daten wie möglich an Dritte übertragen werden (Drittanbieter-Cookies, Cloud-Dienste, Telemetrie, etc.). (APP.1.2.A7)
- Nutz- und Metadaten, die bei Druckern, Kopierern und Multifunktionsgeräten anfallen, dürfen nur so kurz wie möglich auf den Geräten gespeichert werden und müssen nach einer festgelegten Zeit gelöscht werden. (SYS.4.1.A17)

3.3 Organisation

Für den Themenbereich „Organisation“ müssen folgende Anforderungen erfüllt werden:

- Der Einsatz von Informationstechnik muss hinsichtlich seiner betrieblichen und sicherheitstechnischen Aspekte geplant werden. (SYS.2.1.A10, SYS.4.1.A1/A4, NET.1.1.A13/A16/A17/A22/A25)
- Alle wesentlichen Prozesse, die die Informationstechnik und/oder die Informationssicherheit betreffen, müssen geregelt werden. (ORP.4.A1/A15)
- Alle Aufgaben und Zuständigkeiten in Bezug auf die Informationstechnik und Informationssicherheit müssen eindeutig geregelt und aktuell gehalten werden. (ORP.1.A1/A2, APP.6.A1)
- Notwendige Geräte und Betriebsmittel, die Einfluss auf die Informationssicherheit haben, müssen bereitgestellt und verwaltet werden. (ORP.1.A8)
- Bei Umzügen muss die Informationssicherheit vor, während und nach dem Umzug gewährleistet sein. (ORP.1.A13)

- Bei Personaländerungen müssen die notwendigen Änderungen in der Organisation sowie in den Plänen und Konzepten vorgenommen werden. Alle anderen betroffenen Mitarbeiter müssen über die Änderungen informiert werden. (ORP.2.A1/A2)

- Es muss gewährleistet sein, dass kritische Geschäftsprozesse und die Informationssicherheit auch bei Ausfall/Abwesenheit einzelner Mitarbeiter aufrechterhalten werden. (ORP.2.A3, OPS.1.1.2.A2)

- Gefahrenmeldeanlagen müssen unter Berücksichtigung des Einsatzzwecks und der individuellen Verhältnisse am Einsatzort geplant werden. (SYS.4.X.A2)

- Wenn ein oder mehrere Anlagenbestandteile für verschiedene Gefahrenmeldeanlagen genutzt werden sollen, müssen diese unterschiedlichen Aufgaben aufeinander abgestimmt werden. (SYS.4.X.A6)

3.4 Personal

Für den Themenbereich „Personal“ müssen folgende Anforderungen erfüllt werden:

- Die Mitarbeiter müssen in die Festlegung und Umsetzung der sie betreffenden Sicherheitsmaßnahmen einbezogen und mit allen notwendigen Informationen zur Informationssicherheit versorgt werden. (ISMS.1.A8, CON.3.A6, CON.6.A8, CON.9.A1/A3, DER.1.A1/A3, DER.2.1.A1/A2/A12/A14, DER.3.1.A12/A16/A17/A20/A22, DER.4.A2)

- Die Mitarbeiter müssen darüber aufgeklärt werden, welche Konsequenzen eine Verletzung von Sicherheitsvorgaben haben kann. (ISMS.1.A8)

- Alle Mitarbeiter müssen darüber informiert sein, wofür sie zuständig sind und was ihre Aufgaben und Pflichten sind. (ORP.1.A1/A2, CON.3.A10, CON.6.A2/A4, NET.1.1.A26, NET.3.2.A2)

- Alle Mitarbeiter müssen darüber informiert sein, an wen sie sich wenden sollen, wenn sie Fragen zur Informationssicherheit haben. (ORP.1.A15)

- Alle Mitarbeiter müssen schriftlich bestätigen, dass sie die für sie geltenden Regelungen zur Informationssicherheit zur Kenntnis genommen haben. (ORP.1.A16, OPS.1.1.2.A3, OPS.1.1.4.A7, DER.2.1.A1/A2/A12/A14)

- Beim Ausscheiden von Mitarbeitern muss sichergestellt werden, dass alle überlassenen Unterlagen, Schlüssel, Ausweise und andere Betriebsmittel zurückgegeben werden. (ORP.2.A2)

- Beim Ausscheiden von Mitarbeitern müssen alle Zutritts-, Zugangs- und Zugriffsberechtigungen entzogen werden. Ihre persönlichen Kennungen müssen gesperrt werden. Wenn die ausscheidenden Mitarbeiter weitere Passwörter kennen, müssen diese Passwörter geändert werden. (ORP.2.A2, OPS.1.1.2.A4)

- Beim Ausscheiden von Mitarbeitern muss erneut auf Verschwiegenheitsverpflichtungen hingewiesen werden. (ORP.2.A2)

- Alle Mitarbeiter müssen mit den relevanten Gesetzen, Vorschriften, internen Regelungen und Entscheidungen vertraut gemacht und dazu verpflichtet werden, diese einzuhalten. (ORP.2.A1/A14, CON.3.A10, OPS.1.1.2.A3, OPS.1.1.4.A7, DER.1.A1/A3, DER.2.1.A1/A2/A12/A14, DER.4.A2, APP.6.A2, APP.6.A10, SYS.2.1.A9, SYS.4.1.A4/A5, SYS.4.5.A1, NET.3.1.A10, NET.3.2.A1)

- Alle Mitarbeiter müssen dazu verpflichtet werden, dienstliche Informationen zu schützen, auch außerhalb der Arbeitszeit und außerhalb des Betriebsgeländes. (ORP.2.A14)

- Neue Mitarbeiter müssen auf ihre Vertrauenswürdigkeit hin überprüft werden, bevor sie eingestellt werden. (ORP.2.A7)

- Alle Mitarbeiter müssen verpflichtet werden, Auffälligkeiten, den Verdacht auf Sicherheitsprobleme und tatsächliche Sicherheitsprobleme unverzüglich zu melden. Hierzu müssen ihnen die jeweiligen Ansprechpartner mitgeteilt werden. (OPS.1.1.4.A7, DER.1.A4, DER.2.1.A3/A8/A9/A14, SYS.4.5.A2)

- Alle Mitarbeiter müssen darauf hingewiesen werden, dass sicherheitsrelevante Einstellungen nur von den hierzu befugten Personen geändert werden dürfen. (APP.1.2.A3):

- Alle Mitarbeiter müssen darauf hingewiesen werden, dass sie den Zugriff auf lokale Informationen, Peripheriegeräte und Standortdaten im Webbrowser nur für Seiten aktivieren dürfen, bei denen sie unbedingt benötigt werden. (APP.1.2.A7)

3.5 Schulung und Sensibilisierung

Für den Themenbereich „Schulung und Sensibilisierung“ müssen folgende Anforderungen erfüllt werden:

- Bei Neueinstellungen und wenn Mitarbeitern neue Aufgaben zugewiesen werden, muss eine geregelte Einarbeitung erfolgen. (ORP.2.A1, OPS.1.1.2.A3, OPS.1.1.6.A6)
- Es muss dauerhaft sichergestellt sein, dass alle Mitarbeiter die für ihre jeweiligen Tätigkeiten notwendigen Kenntnisse und Qualifikationen haben. (ORP.2.A15, OPS.1.1.2.A10, OPS.1.1.6.A7, DER.1.A7, DER.2.2.A6/A10, DER.3.1.A9, APP.6.A1, SYS.2.1.A23)
- Administratoren müssen sich regelmäßig über die Sicherheit der von ihnen betreuten Informationstechnik informieren. (OPS.1.1.2.A10)
- Die für die Detektion sicherheitsrelevanter Ereignisse zuständigen Mitarbeiter müssen regelmäßig externe Quellen nach relevanten neuen Erkenntnissen durchsuchen. (DER.1.A12)
- Alle Mitarbeiter müssen regelmäßig für die Bedeutung der Informationssicherheit sensibilisiert und über aktuelle Gefahren informiert werden. (ORP.3.A1/A3/A4, CON.9.A5, OPS.1.1.4.A7, DER.1.A4, DER.2.1.A12)
- Alle Mitarbeiter müssen in den sicheren Umgang mit der für sie jeweils relevanten Informationstechnik eingewiesen werden. (ORP.3.A1/A3, ORP.4. A5/A6/A7/A19, CON.9.A5, DER.2.1.A15, DER.3.1.A12/A16/A17/A20/A22, SYS.2.1.A9)
- Alle Mitarbeiter müssen in den Themen der Informationssicherheit geschult werden, die für sie jeweils relevant sind. (ORP.3.A6/A7, DER.2.1.A15, DER.3.1.A12/A16/A17/A20/A22)
- Die Erfolge der Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit müssen bewertet werden. Die Ergebnisse müssen in die Fortschreibung der Maßnahmen einfließen. (ORP.3.A8)

3.6 Dienstleister und externe Personen

Für den Themenbereich „Dienstleister und externe Personen“ müssen folgende Anforderungen erfüllt werden:

- Mit externen Personen, denen vertrauliche Informationen zur Verfügung gestellt werden sollen, und mit externen Dienstleistern, die sich vertrauliche Informationen verschaffen können, müssen vorher schriftliche Vertraulichkeitsvereinbarungen geschlossen werden. (ORP.2.A5, SYS.4.1.A2)
- Falls ein externer Informationssicherheitsbeauftragter bestellt wird, müssen die Rechte und Pflichten, die Vertraulichkeit und die geregelte Beendigung des Vertragsverhältnisses im Vertrag geregelt sein. (ISMS.1.A5)
- Wenn ein externer Dienstleister mit der Löschung bzw. Vernichtung von Informationen, Datenträgern, Geräten oder Betriebsmitteln beauftragt wird, muss sichergestellt werden, dass die Verfahrensweisen des Dienstleisters die festgelegten Anforderungen erfüllen. Dies muss regelmäßig kontrolliert werden. (CON.6.A11)
- Es muss eine Liste mit geeigneten Dienstleistern erstellt und aktuell gehalten werden, die bei der Behandlung von Sicherheitsvorfällen und bei der Durchführung forensischer Untersuchung hinzugezogen werden können. (DER.2.1.A5, DER.2.2.A3)
- Wenn externe Dienstleister mit Audits, Revisionen oder anderen Überprüfungen beauftragt werden, müssen diese Dienstleister auf Unabhängigkeit überprüft und zur Verschwiegenheit verpflichtet werden. (DER.3.1.A9/A24)
- Die Regelungen zur Sensibilisierung, zur Einweisung in neue Aufgaben, zur Verpflichtung auf die geltenden Vorschriften und zum Ausscheiden von Mitarbeitern müssen auch auf externes Personal angewandt werden. (ORP.2.A4)
- Externes Personal und Fremdpersonen müssen in sicherheitsrelevanten Räumlichkeiten beaufsichtigt werden. (ORP.1.A3, ORP.2.A4)

3.7 Beschaffung

Für den Themenbereich „Beschaffung“ müssen folgende Anforderungen erfüllt werden:

- Es muss sichergestellt sein, dass nur Informationstechnik beschafft wird, die die jeweils erforderlichen Funktionen und Sicherheitseigenschaften aufweist. Hierzu muss jeweils eine Anforderungsliste erstellt werden. (ORP.4.A17/A18, CON.3.A7, OPS.1.1.3.A8, DER.2.2.A7, APP.6.A1/A2/A3/A7, SYS.2.1.A11, NET.3.1.A11, NET.3.2.A15)
- Informationstechnik, bei der absehbar ist, dass Fehler und Sicherheitslücken nicht mehr behoben werden, darf nicht beschafft werden. (APP.6.A3, SYS.2.1.A11)

- Es darf nur Informationstechnik beschafft und eingesetzt werden, deren Sicherheitseigenschaften dem Stand der Technik entsprechen. (APP.1.2.A1/A2/A3/A13, APP.6.A6, NET.3.2.A15)
- Bei der Beschaffung von Software muss sichergestellt werden, dass die Software kompatibel mit der bestehenden IT-Landschaft ist und in die organisatorischen und administrativen Abläufe integriert werden kann. (APP.6.A1)
- Software und Patches/Updates dürfen nur aus vertrauenswürdigen Quellen bezogen werden. (OPS.1.1.3.A10, DER.2.2.A7, APP.6.A3/A4)
- Soweit dies möglich ist, muss die Integrität von Software und von Patches/Updates überprüft werden, bevor sie installiert werden. (OPS.1.1.3.A10, DER.2.2.A7, APP.6.A3/A4)
- Sofern Clients beschafft werden, die über die Funktion UEFI SecureBoot oder über ein TPM verfügen, müssen diese Funktionalitäten durch den Eigentümer selbst verwaltet werden können. (SYS.2.1.A11)
- Es dürfen nur Gefahrenmeldeanlagen beschafft werden, die alle internen und externen Vorgaben erfüllen, insbesondere die Vorgaben der EU in Bezug auf elektrische Anlagen. (SYS.4.X.A1)
- Bei der Beschaffung von Gefahrenmeldeanlagen müssen alle funktionalen, nicht-funktionalen und sicherheitstechnischen Anforderungen berücksichtigt werden. Es muss auf die Dimensionierung und auf Reserven für mögliche Erweiterungen geachtet werden. (SYS.4.X.A5)
- Fachunternehmen, die mit der Planung oder Errichtung von Gefahrenmeldeanlagen beauftragt werden, müssen die Anforderungen des Einsatzzwecks kennen und entsprechend qualifiziert sein. (SYS.4.X.A5)
- Gefahrenmeldeanlagen müssen nach anerkannten Regeln der Technik sowie den Vorgaben der VdS installiert werden. (SYS.4.X.A1)

3.8 Identitäten und Berechtigungen

Für den Themenbereich „Identitäten und Berechtigungen“ müssen folgende Anforderungen erfüllt werden:

- Alle Administratoren und Benutzer müssen eindeutige Kennungen für die Administration bzw. Nutzung von Informationstechnik erhalten. (ORP.4.A1)
- Soweit dies technisch möglich ist, muss jeder Administrator und jeder Benutzer unter seiner eigenen Kennung arbeiten. (ORP.4.A14, OPS.1.1.2.A5)
- Administrative Tätigkeiten müssen über administrative Kennungen durchgeführt werden. Normale Nutzung darf nicht über administrative Kennungen erfolgen. (ORP.4.A1/A2, OPS.1.1.2.A6)
- Der Zugang und Zugriff auf Informationstechnik und Dienste für Administratoren und Benutzer muss durch eine jeweils angemessene Identifikation und Authentisierung geschützt sein. (ORP.4.A9/A12/A23, OPS.1.1.2.A6, SYS.2.1.A1, NET.3.1.A21)
- Vorkonfigurierte Authentisierungsmittel (z. B. Passwörter) müssen vor dem produktiven Einsatz geändert werden. (ORP.4.A9/A12/A23)
- Kennungen müssen nach einer vorgegebenen Anzahl von fehlerhaften Anmeldeversuchen gesperrt werden. (ORP.4.A13)
- Administratoren und Benutzer müssen sich nach Aufgabenerfüllung von den IT-Systemen bzw. IT-Anwendungen abmelden. (ORP.4.A14, SYS.2.1.A1)
- Anmeldevorgänge von Administratoren müssen protokolliert werden. (OPS.1.1.2.A5)
- Kennungen und Berechtigungen dürfen nur aufgrund des tatsächlichen Bedarfs und der Notwendigkeit für die Aufgabenerfüllung vergeben werden. (ORP.4.A2, ORP.4.A5/A6/A7/A16, NET.3.1.A21)
- Miteinander unvereinbare Tätigkeiten müssen bei der Vergabe von Kennungen und Berechtigungen getrennt werden. (ORP.4.A4)
- Zutritts-, Zugangs- und Zugriffsrechte müssen nachvollziehbar und sicher verwaltet werden. (ORP.4.A5/A6/A7/A16, NET.3.1.A21)
- Bei administrativen Kennungen und anderen Kennungen mit weitreichenden Berechtigungen muss mindestens eine der folgenden Anforderungen erfüllt werden:
  - Aktivierung von Funktionen oder Dienstleistungen zur Erkennung kompromittierter Passwörter.
  - Aktivierung von Mehr-Faktor-Authentisierung, beispielsweise mittels Chipkarten oder Tokens.

  - Regelmäßiger Wechsel der Passwörter. (ORP.4.A10/A23)

- Authentisierungsdaten (z. B. Passwörter), private kryptografische Schlüssel und andere schützenswerte Administrationsdaten müssen bei der Verarbeitung, Speicherung und Übertragung vor unbefugtem Zugriff geschützt werden. (ORP.4.A12/A13/A23, NET.3.1.A1, NET.3.2.A4)
- Informationen, Datenträger und Geräte müssen vor unbefugtem Zugriff geschützt werden. (CON.6.A2, SYS.4.1.A2, SYS.4.5.A4)
- Benannte Vertreter müssen mit den notwendigen Zutritts-, Zugangs- und Zugriffsrechten ausgestattet sein. (OPS.1.1.2.A2)
- Soweit dies technisch möglich ist, dürfen nur Administratoren Zugriff auf administrative Schnittstellen und Funktionen erhalten. (OPS.1.1.2.A6, NET.3.2.A4)
- Soweit dies technisch möglich ist, muss sichergestellt werden, dass sicherheitsrelevante Änderungen an Informationstechnik nur durch Administratoren vorgenommen werden können. (OPS.1.1.2.A6, OPS.1.1.4.A5, APP.1.2.A3, SYS.2.1.A6/A8/A13, SYS.4.1.A2/A18, NET.3.2.A4)
- Wenn Benutzer bzw. Administratoren eine festgelegte Zeit keine Aktion durchgeführt haben, muss das IT-System bzw. die IT-Anwendung automatisch gesperrt werden. Die Sperre darf nur durch eine erfolgreiche Authentisierung deaktiviert werden können. (SYS.2.1.A1)
- Der Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (z. B. durch das Betriebssystem speziell abgesicherte Speicherbereiche, Firmwarebereiche etc.) darf nur durch Administratoren möglich sein. (SYS.2.1.A13)
- Clients müssen so konfiguriert werden, dass nur der lokal aktive Benutzer die Kameras und Mikrofone am System aktivieren kann. Kameras und Mikrofone müssen deaktiviert oder deinstalliert werden, wenn sie nicht benutzt werden. (SYS.2.1.A21)
- Es muss verhindert werden, dass von Clients aus auf nicht freigegebene Geräte oder Datenträger zugegriffen wird. (SYS.2.1.A24)
- Es muss verhindert werden, dass Benutzer von externen Datenträgern Programme ausführen können. (SYS.2.1.A24)
- Informationstechnik muss vor unberechtigtem physischen Zugriff geschützt werden. (SYS.4.1.A2, NET.3.1.19)
- Kennungen und Berechtigungen müssen regelmäßig daraufhin überprüft werden, ob sie noch korrekt und auf dem aktuellen Stand sind. Abweichungen müssen zeitnah korrigiert werden. (ORP.4.A3)
- Nicht (mehr) benötigte Kennungen und Berechtigungen müssen deaktiviert oder gelöscht werden. (ORP.4.A1/A2)
- Nicht (mehr) benötigte Zutritts-, Zugangs- und Zugriffsrechte müssen entzogen werden. (ORP.4.A5/A6/A7/A16)
- Chipkarten und andere Betriebsmittel für Zutritt, Zugang oder Zugriff müssen ausgewechselt werden, wenn sie kompromittiert wurden. (ORP.4.A5/A6/A7)
- Nutz- und Metadaten, die bei Druckern, Kopierern und Multifunktionsgeräten anfallen, müssen vor unbefugtem Zugriff geschützt werden. (SYS.4.1.A17)

3.9 Passwörter

Für den Themenbereich „Passwörter“ müssen folgende Anforderungen erfüllt werden:

- Die Verwendung von Passwörtern muss verbindlich geregelt werden. Dabei muss gewährleistet werden, dass Passwörter geheim gehalten, sicher verwaltet und sicher benutzt werden. (ORP.4.A8)
- Für unterschiedliche Systeme, Anwendungen und Dienste dürfen nicht die gleichen Passwörter verwendet werden. (ORP.4.A8)
- Es müssen Mindestanforderungen für Passwörter hinsichtlich Länge und Komplexität festgelegt werden. Passwörter, die leicht zu erraten oder in gängigen Passwortlisten enthalten sind, dürfen nicht verwendet werden. (ORP.4.A8/A22)
- Mitarbeiter müssen wissen, an welchen Ansprechpartner sie sich wenden sollen, wenn sie ihr Passwort zurücksetzen lassen möchten. (ORP.4.A11)

- Wenn Passwortmanager genutzt werden, müssen die Passwörter darin verschlüsselt gespeichert werden. (APP.1.2.A6)
- Wenn Passwortmanager genutzt werden, muss sichergestellt sein, dass auf die gespeicherten Passwörter nur nach Eingabe eines Master-Passworts zugegriffen werden kann. (APP.1.2.A6)
- Wenn Passwortmanager genutzt werden, muss sichergestellt sein, dass Benutzer ihre Passwörter ändern und löschen können. (APP.1.2.A6)
- Wenn ein im Webbrowser integrierter Passwortmanager genutzt wird, muss der Webbrowser eine eindeutige Beziehung zwischen Webseite und hierfür gespeichertem Passwort herstellen. (APP.1.2.A6)
- Wenn ein im Webbrowser integrierter Passwortmanager genutzt wird, darf das Master-Passwort den Passwortmanager nur für die aktuelle Browser-Sitzung freischalten. Wird die aktuelle Browser-Sitzung beendet, muss der Passwortmanager wieder gesperrt werden. (APP.1.2.A6)
- Wenn der Verdacht besteht, dass ein Passwort kompromittiert wurde, muss es gewechselt werden. (ORP.4.A8)

3.10 Härtung

Für den Themenbereich „Härtung“[4] müssen folgende Anforderungen erfüllt werden:

- Nicht benötigte informationstechnische Komponenten, Funktionen, Schnittstellen, Dienste, Protokolle und Konten müssen deaktiviert oder deinstalliert werden. (SYS.2.1.A16, SYS.4.1.A18, NET.3.1.A1, NET.3.2.A4/A17)
- Funktionen für die Fernadministration und Fernwartung von Informationstechnik sowie für den sonstigen Fernzugriff auf Informationstechnik müssen deaktiviert werden. (SYS.4.1.A18)
- Software muss so installiert und konfiguriert werden, dass möglichst nur der benötigte Funktionsumfang installiert und ausgeführt wird und dass die Software mit den geringsten möglichen Berechtigungen ausgeführt wird. (APP.6.A4/A11)
- Alle Clients müssen so konfiguriert werden, dass Benutzer das System nur von einem fest eingestellten internen Laufwerk starten („booten“) können. Nur Administratoren dürfen Clients von anderen (internen oder externen) Laufwerken booten können. (SYS.2.1.A8)
- Nicht benötigte Funktionen in der Firmware von Clients müssen deaktiviert werden. (SYS.2.1.A8)
- Nicht benötigte Cloud- und Online-Funktionen von Clients müssen deaktiviert werden. (SYS.2.1.A42)
- Auf Firewalls und Paketfiltern müssen vorkonfigurierte Zertifikate entfernt werden, wenn sie nicht benötigt werden. (NET.3.2.A21)
- Vorhandene Sicherheitseigenschaften und Sicherheitsfunktionen von Informationstechnik müssen aktiviert und genutzt werden. (APP.1.2.A1/A2/A3/A13, APP.6.A6, SYS.2.1.A26, SYS.4.1.A15/A18)
- Bei der Konfiguration von Informationstechnik müssen die Sicherheitsempfehlungen des jeweiligen Herstellers/Anbieters berücksichtigt werden, sofern diese Sicherheitsempfehlungen nicht den internen und externen Vorgaben widersprechen. (SYS.2.1.A43)

3.11 Schutz vor Schadprogrammen

Für den Themenbereich „Schutz vor Schadprogrammen“ müssen folgende Anforderungen erfüllt werden:

- Es muss festgelegt werden, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Neben der Büro-IT müssen dabei auch spezielle und eingebettete IT-Systeme berücksichtigt werden, beispielsweise Internet-of-Things-Systeme. (OPS.1.1.4.A1)
- Funktionen in Betriebssystemen und Anwendungsprogrammen zum Schutz vor Schadprogrammen müssen genutzt werden, sofern kein mindestens gleichwertiger Ersatz in Betrieb ist oder besondere Gründe dagegensprechen. (OPS.1.1.4.A2)
- Alle Arten des internen und externen Informationsaustauschs (Netzwerk, E-Mail, Dateiablagen, Datenträger, etc.) müssen durch ein dem Stand der Technik entsprechendes Virenschutzprogramm geschützt werden. (OPS.1.1.4.A3, SYS.2.1.A6, NET.3.2.A20/A21)

[4] Der Begriff „Härtung“ steht hier allgemein für Aktivitäten, die die Angriffsfläche der Informationstechnik reduzieren und die Widerstandsfähigkeit erhöhen.

- Virenschutzprogramme für reine Heimanwender oder ohne Hersteller-Support dürfen nicht eingesetzt werden. (OPS.1.1.4.A3)
- Virenschutzprogramme müssen Funktionen zum Echtzeit- und On-Demand-Scan sowie zum Durchsuchen komprimierter Daten bieten. (OPS.1.1.4.A3)
- Virenschutzprogramme müssen so konfiguriert werden, dass sie einen dem Stand der Technik entsprechenden Schutz vor Schadprogrammen bieten. (OPS.1.1.4.A5)
- Virenschutzprogramme müssen so konfiguriert werden, dass die zu prüfenden Daten von ihnen durchsucht werden. (OPS.1.1.4.A5)
- Virenschutzprogramme müssen Infektionen mit Schadprogrammen automatisch blockieren und melden. (OPS.1.1.4.A9)
- Es muss festgelegt werden, wer Meldungen und Alarme der Virenschutzprogramme entgegennimmt und wie auf solche Meldungen bzw. Alarme reagiert wird. (OPS.1.1.4.A9)
- Es müssen Verhaltensregeln für alle Mitarbeiter zum Schutz vor Schadprogrammen festgelegt werden. Dateien, E-Mails, Webseiten, Datenträger usw. aus nicht vertrauenswürdigen Quellen dürfen nur dann geöffnet werden, wenn dies für die Aufgabenerfüllung unvermeidlich ist. (OPS.1.1.4.A7)
- Bei Windows-Clients muss entweder das integrierte Schutzprogramm gegen Schadsoftware oder ein Schutz-programm von einem Drittanbieter eingesetzt werden. (SYS.2.1.A6, SYS.2.2.3.A5)
- Bei Windows-Clients muss regelmäßig der gesamte Datenbestand auf dem Client auf Schadsoftware geprüft werden. (SYS.2.1.A6)
- Die Scan-Engines der Virenschutzprogramme und die Signaturen für die Schadprogramme müssen regelmäßig und zeitnah aktualisiert werden. (OPS.1.1.4.A6)

3.12 Informationsaustausch

Für den Themenbereich „Informationsaustausch“ müssen folgende Anforderungen erfüllt werden:

- Auf der Grundlage der internen und externen Vorgaben muss festgelegt werden, welche Informationen auf welchen Wegen mit welchen Kommunikationspartnern ausgetauscht werden dürfen. (CON.9.A1, SYS.2.1.A23/A24, SYS.4.1.A17)
- Alle Mitarbeiter müssen vor dem Austausch von Informationen sicherstellen, dass der Empfänger die jeweiligen Informationen erhalten und weiterverarbeiten darf. (CON.9.A1)
- Auf der Grundlage der internen und externen Vorgaben muss festgelegt werden, welche Informationen welchen Schutzbedarf haben und welche Sicherheitsmaßnahmen dafür jeweils erforderlich sind. (CON.9.A2)
- Beim Austausch schutzbedürftiger Informationen müssen die Empfänger auf den Schutzbedarf der Informationen, die notwendigen Sicherheitsmaßnahmen und auf die Zweckbindung der Informationen hingewiesen werden. (CON.9.A2)
- Wenn regelmäßig schutzbedürftige Informationen mit Dritten ausgetauscht werden, müssen die Rahmenbedingungen und Sicherheitsmaßnahmen zwischen den Kommunikationspartnern nachvollziehbar vereinbart werden. (CON.9.A4)
- Bevor Dateien oder Dokumente weitergegeben werden, müssen unerwünschte Restinformationen daraus entfernt werden. (CON.9.A5)
- Für den Informationsaustausch müssen Datenformate verwendet werden, die auf Empfängerseite verarbeitet werden können. (CON.9.A6)

3.13 Netzsicherheit

Für den Themenbereich „Netzsicherheit“ müssen folgende Anforderungen erfüllt werden:

- Es muss festgelegt werden, wofür das interne Netz, das Internet und ggf. weitere Netze genutzt werden und welche grundsätzlichen Sicherheitsanforderungen dafür gelten. (NET.1.1.A1/A3, NET.3.2.A1)
- Die Internet-Zone und das interne Netz müssen physisch durch eine Firewall separiert werden. Für die Absicherung des internen Netzes muss mindestens eine professionelle restriktiv eingerichtete Firewall-Lösung (mindestens zustandsbehafteter Paketfilter) mit Support für Hardware, Software und Konfiguration eingesetzt werden. (NET.1.1.A4/A12/A18, NET.3.2.A16)

- Der Internet-Datenverkehr muss durch die Firewall-Struktur geführt werden. Das Firewall-Regelwerk muss nach dem Whitelisting-Prinzip aufgebaut werden. Die Datenflüsse müssen dabei auf die benötigten Protokolle und Kommunikationsbeziehungen eingeschränkt werden (NET.1.1.A4/A8)

- Für jedes Netz muss festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die nicht vertrauenswürdig sind, werden als Fremdnetze bezeichnet. Fremdnetze müssen wie das Internet behandelt und entsprechend abgesichert werden. (NET.1.1.A9)

- IT-Systeme mit unterschiedlichem Sicherheitsniveau müssen in verschiedenen Netzsegmenten platziert werden. Netzsegmente müssen durch einen zustandsbehafteten Paketfilter getrennt werden. Paketfilter dürfen nicht überbrückt oder umgangen werden. (NET.1.1.A5/A6/A19/A22/A23)

- Schützenswerte Informationen müssen über sichere Protokolle übertragen werden, wenn sie über das Internet oder über andere Fremdnetze transportiert werden. (NET.1.1.A7/A9)

- Die IT-Systeme des Informationsverbunds dürfen nicht aus dem Internet und nicht aus anderen Fremdnetzen erreichbar sein. Es dürfen keine Dienste ins Internet oder in andere Fremdnetze angeboten werden. (NET.1.1.A9/A10/A11, SYS.4.1.A11)

- Soweit dies technisch möglich ist, müssen unterschiedliche Arten von Endgeräten (Clients, Drucker, etc.) im Netz unterschiedlichen IPv4-/IPv6-Subnetzen zugeordnet werden. (NET.1.1.A20)

- Die Trennung von Netzen von anderen Unternehmen/Institutionen muss durch physische Trennung oder durch den Einsatz von kryptografischen Verfahren, die dem Stand der Technik entsprechen, erfolgen. (NET.1.1.A23)

- Falls virtuelle LANs (VLANs) eingesetzt werden, dürfen damit keine Firewalls oder Paketfilter überbrückt werden. (NET.1.1.A24)

- Router, Paketfilter und Firewalls müssen so konfiguriert werden, dass Zugriffe vom Internet aus in das interne Netz blockiert werden. (NET.3.1.A1/A18)

- Die Funktionen der Router, Paketfilter und Firewalls zum Schutz vor netzbasierten Angriffen müssen aktiviert sein. (NET.3.1.A5/A14/A15/A16/A17/A20, NET.3.2.A3/A10/ A19)

- Paketfilter und Firewalls müssen so konfiguriert sein, dass nur die benötigten Protokolle, Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen müssen unterbunden werden („default deny“). Für die Internet-Web-Nutzung bedeutet dies insbesondere, dass nur die benötigten Ports und nur die IP-Adressen der Clients, die dies benötigen, freigeschaltet werden dürfen. (NET.3.2.A2/A3, NET.1.1.A8)

- Neue oder geänderte Firewall-Regeln müssen getestet werden. (NET.3.2.A2)

- Die gesamte Kommunikation mit dem Internet sowie mit nicht vertrauenswürdigen anderen Netzen muss über eine Firewall geleitet werden. (NET.3.2.A2)

- Router, Paketfilter und Firewalls müssen so konfiguriert werden, dass sie möglichst wenig Informationen über ihren internen Konfigurations- und Betriebszustand nach außen preisgeben. (NET.3.2.A4)

- Soweit dies technisch möglich ist, müssen Routen auf Firewalls und Paketfiltern statisch konfiguriert werden. (NET.3.2.A8)

- Wenn Multifunktionsgeräte an das Telefonnetz angeschlossen werden, muss sichergestellt werden, dass keine unkontrollierten Datenverbindungen zwischen dem Datennetz und dem Telefonnetz aufgebaut werden können. (SYS.4.1.A11)

3.14 Wechseldatenträger

Für den Themenbereich „Wechseldatenträger“ müssen folgende Anforderungen erfüllt werden:

- Das Anschließen von Wechseldatenträgern aus unbekannten Quellen muss den Mitarbeitern untersagt werden. (SYS.4.5.A1)

- Nur auf Schadsoftware überprüfte Daten dürfen auf Wechseldatenträger übertragen werden. Bevor Daten von Wechseldatenträgern verarbeitet werden, müssen sie auf Schadsoftware überprüft werden. (SYS.4.5.A12)

- Mitarbeiter müssen umgehend melden, wenn ein Wechseldatenträger gestohlen wurde oder der Verdacht einer Manipulation besteht. (SYS.4.5.A2)

- Die Herstellerangaben zum Umgang mit Wechseldatenträgern müssen berücksichtigt werden. (SYS.4.5.A4)

- Es muss geregelt werden, wer welche Wechseldatenträger zu welchen Anlässen außer Haus transportieren darf und welche Sicherheitsmaßnahmen dabei zu beachten sind. (SYS.4.5.A5)
- Wenn Wechseldatenträger mit vertraulichen Daten außerhalb eines sicheren Bereiches verwendet oder transportiert werden, müssen sie mit einem sicheren Verfahren verschlüsselt werden. (SYS.4.5.A10)
- Wechseldatenträger müssen verwaltet und gekennzeichnet werden. (SYS.4.5.A6)
- Wechseldatenträger, die versendet werden sollen, müssen so gekennzeichnet werden, dass Absender und Empfänger sie eindeutig identifizieren können. (SYS.4.5.A13)
- Wenn Wechseldatenträger mit schützenswerten Informationen versendet werden, darf die Kennzeichnung keine Rückschlüsse auf Art und Inhalte der Informationen zulassen. (SYS.4.5.A13)

3.15 Tests und Freigabe

Für den Themenbereich „Tests und Freigabe“ müssen folgende Anforderungen erfüllt werden:

- Neue Informationstechnik muss getestet und freigegeben werden, bevor sie produktiv eingesetzt wird. Dabei muss auch die Kompatibilität mit der bestehenden Informationstechnik berücksichtigt werden. (OPS.1.1.3.A9, OPS.1.1.2.A20, APP.6.A5)
- Wesentliche Änderungen an Informationstechnik oder Konfigurationen müssen getestet und freigegeben werden, bevor sie umgesetzt werden. (OPS.1.1.3.A1, APP.6.A5, SYS.4.X.A12)
- Es muss festgelegt werden, wie und anhand welcher Kriterien Software vor dem produktiven Einsatz getestet wird. Vorhandene Anforderungskataloge und Pflichtenhefte müssen dabei berücksichtigt werden. (OPS.1.1.6.A1)
- Es muss getestet werden, ob die Software vollständig und ordnungsgemäß funktioniert, ob die Software mit den vorgesehenen Einsatzumgebungen kompatibel ist, ob die Software die notwendigen Sicherheitseigenschaften aufweist und ob die übrigen nicht-funktionalen Anforderungen erfüllt sind. (OPS.1.1.6.A1/A2/A5)
- Software-Tests dürfen den Produktivbetrieb nicht beeinträchtigen und müssen auf einem separaten Testsystem stattfinden, soweit dies möglich ist. (OPS.1.1.6.A2/A13)
- Software darf nur für den Produktivbetrieb freigegeben werden, wenn die Software-Tests erfolgreich durchgeführt wurden und die internen/externen Vorgaben erfüllt sind. (OPS.1.1.6.A4/A15)
- Wenn Produktivdaten für Software-Test verwendet werden, die schützenswerte Informationen enthalten, dann müssen diese Daten angemessen während der Software-Tests geschützt werden. (OPS.1.1.6.A11)
- Es muss festgelegt werden, welche Kriterien für die Freigabe von Software erfüllt sein müssen. (OPS.1.1.6.A10)
- Bevor Informationstechnik in den Produktivbetrieb überführt wird, muss sichergestellt werden, dass alle sicherheitsrelevanten Updates/Patches eingespielt sind und dass die Konfiguration den internen/externen Vorgaben entspricht. (APP.6.A4, SYS.2.1.A15, NET.1.1.A14)
- Firmware, Betriebssysteme und Software, für die keine Updates/Patches angeboten werden, um Sicherheitslücken zu schließen, dürfen nicht eingesetzt werden. (SYS.2.1.A11/A14)
- Das Anschließen nicht-freigegebener Informationstechnik an freigegebene Informationstechnik ist ausschließlich im Rahmen von Test- und Freigabeprozessen zulässig. (SYS.2.1.A24)

3.16 Überprüfungen

Für den Themenbereich „Überprüfungen“ müssen folgende Anforderungen erfüllt werden:

- Es muss regelmäßig überprüft werden, ob alle internen und externen Vorgaben an die Informationssicherheit vollständig, korrekt, angemessen und aktuell umgesetzt sind. (DER.3.1.A3/A19, DER.3.1.A4, DER.3.1.A5/A7/A8/A10)
- Es muss anlassbezogen und mindestens jährlich überprüft werden, dass das Sicherheitskonzept noch auf dem aktuellen Stand ist. (ISMS.1.A2/A7/A11)
- Es muss anlassbezogen und mindestens jährlich überprüft werden, dass die im Sicherheitskonzept vorgesehenen Maßnahmen umgesetzt und wirksam sind. (ISMS.1.A11, DER.1.A13)
- Konzepte, Regelungen und Entscheidungen zur Informationssicherheit müssen regelmäßig daraufhin überprüft werden, ob sie noch dem Stand der Technik entsprechen und ausreichend sind. (CON.6.A4/A8, OPS.1.1.2.A7/A9, OPS.1.1.4.A1, DER.1.A1/A3/A13, DER.2.1.A2/A5/A7/A14, DER.3.1.A26, APP.6.A10, SYS.2.1.A9, SYS.4.5.A4, NET.1.1.A13/A16/A17/A22/A25, NET.3.2.A1)

- Konzepte, Regelungen und Entscheidungen zur Informationssicherheit müssen regelmäßig daraufhin überprüft werden, ob sie korrekt umgesetzt sind. (CON.6.A4/A8, OPS.1.1.2.A7/A9, OPS.1.1.4.A1, DER.1.A1/A3/A13, DER.2.1.A2/A5/A7/A14, NET.1.1.A15/A25, NET.3.2.A1)
- Sicherheitsrelevante Konfigurationseinstellungen müssen regelmäßig daraufhin überprüft werden, ob sie den internen und externen Vorgaben entsprechen. (OPS.1.1.5.A1/A3, OPS.1.1.4.A1, SYS.2.1.A43, NET.3.1.A10/A12/A23, NET.3.2.A1)
- Es muss regelmäßig überprüft werden, ob alle Regelungen zur Informationssicherheit eingehalten werden. (CON.6.A8, NET.3.2.A1, ORP.4.A14, APP.6.A10)
- Die regelmäßige Überprüfung der Informationssicherheit muss anhand von Dokumentenprüfungen, Interviews und Stichprobenprüfungen vor Ort durchgeführt werden. (DER.3.1.A3/A13/A14/A17/A18/A21)
- Alle betroffenen Mitarbeiter und die Personalvertretung müssen über geplante Überprüfungen informiert werden. (DER.3.1.A2)
- Überprüfungen können durch interne oder externe Prüfer durchgeführt werden. Überprüfungen müssen möglichst so durchgeführt werden, dass Mitarbeiter nicht ihre eigene Arbeit überprüfen. (ORP.1.A4, DER.3.1.A1/A9)
- Bei Überprüfungen dürfen die Prüfer nicht selbst in Systeme eingreifen und keine Anweisungen zu Änderungen an den Prüfgegenständen erteilen. (DER.3.1.A3)
- Die Ergebnisse von Überprüfungen müssen der Geschäftsführung zeitnah vorgelegt werden. (DER.3.1.A3/A5/A22)
- Für Überprüfungen muss ein einheitliches, geeignetes und angemessenes Verfahren sowie ein einheitliches Bewertungsschema festgelegt werden. (DER.3.1.A6/A15)
- Informationen, die bei Überprüfungen erhoben, ausgetauscht oder dokumentiert werden, müssen vertraulich behandelt und dürfen nicht verfälscht werden. (DER.3.1.A11/A24/A27)
- Anhand der Ergebnisse der Überprüfungen muss bewertet werden, ob die verbleibenden Restrisiken angemessen und tragbar sind und ob sie von der Geschäftsführung getragen werden. (DER.3.1.A19)
- Nach einer Überprüfung müssen alle dafür entliehenen Dokumente, Datenträger und Systeme wieder an die jeweils verantwortlichen Personen zurückgegeben oder in Abstimmung mit den verantwortlichen Personen sicher vernichtet werden. (DER.3.1.A24)
- Nach einer Überprüfung müssen alle dafür erstellten Zutritts-, Zugangs- und Zugriffsrechte gelöscht werden. (DER.3.1.A24)
- Die Ergebnisse von Überprüfungen müssen ausgewertet und zur Verbesserung der Informationssicherheit herangezogen werden. (DER.3.1.A1/A5/A21)
- Nach Ablauf der Aufbewahrungsfristen müssen Unterlagen zu Überprüfungen sicher gelöscht oder vernichtet werden. (DER.3.1.A27)
- Gefahrenmeldeanlagen einschließlich der Übertragungswege zu den hilfeleistenden Stellen müssen regelmäßig getestet werden. (SYS.4.X.A4/A11)

3.17 Aufrechterhaltung

Für den Themenbereich „Aufrechterhaltung“ müssen folgende Anforderungen erfüllt werden:

- Wenn sich die interne Aufgabenverteilung ändert, müssen die davon betroffenen internen und externen Ansprechpartner über die Änderung informiert werden. (OPS.1.1.2.A4)
- Es muss sichergestellt werden, dass alle notwendigen Wartungs- und Reparaturarbeiten an IT-Systemen und sonstigen IT-Geräten durchgeführt werden. (OPS.1.1.2.A12, SYS.4.X.A4)
- Melder und Sensoren von Gefahrenmeldeanlagen müssen regelmäßig auf Verschmutzung und Korrosion geprüft werden. Wenn nötig, müssen sie gesäubert und neu kalibriert werden. (SYS.4.X.A4)
- Es muss ein Zeitraum festgelegt werden, innerhalb dessen Störungen und Fehlfunktionen von Gefahrenmeldeanlagen behoben werden müssen. Es muss sichergestellt werden, dass dieser Zeitraum eingehalten wird. (SYS.4.X.A8)
- Änderungen sowie Administrations-, Wartungs- und Reparaturarbeiten müssen so durchgeführt werden, dass die Sicherheit der Informationstechnik aufrechterhalten wird. (OPS.1.1.2.A12, OPS.1.1.3.A1/A5)

- Alle sicherheitsrelevanten Patches und Updates müssen zeitnah nach deren Veröffentlichung mittels Auto-Up-date oder manuell eingespielt werden. Wenn für Auto-Updates ein Zeitintervall vorgegeben werden kann, muss mindestens täglich automatisch nach Updates gesucht und diese installiert werden. (OPS.1.1.3.A3/A15/A16, SYS.2.1.A3, SYS.4.X.A12, NET.3.2.A24)
- Es müssen regelmäßig Informationen über Sicherheitslücken in den genutzten Produkten und Dienstleistungen eingeholt werden, beispielsweise über Newsletter. (OPS.1.1.2.A10, OPS.1.1.3.A16, NET.3.2.A24)
- Wenn für eine Sicherheitslücke kein Patch verfügbar ist oder ein Patch aus betrieblichen Gründen nicht eingespielt werden kann, muss geprüft werden, ob Ersatzmaßnahmen („Workarounds“) notwendig sind. Ersatzmaßnahmen müssen zeitnah umgesetzt werden. (OPS.1.1.3.A3/A15/A16, NET.3.2.A24)
- Bei größeren Updates, beispielsweise beim Wechsel auf eine neuere Hauptversion, muss die Software erneut getestet und freigegeben werden. (OPS.1.1.6.A12)
- Sicherheitsvorfälle müssen nachbereitet werden, um etwaige Mängel zeitnah zu erkennen und zu beseitigen und um Verbesserungen umsetzen zu können. (DER.2.1.A17/A18)
- Während Änderungen an der Software oder Konfiguration von Gefahrenmeldeanlagen müssen die überwachten Objekte weiterhin geschützt sein. (SYS.4.X.A12)

3.18 Notfallplanung und Notfallhandbuch

Für den Themenbereich „Notfallplanung und Notfallhandbuch“ müssen folgende Anforderungen erfüllt werden:

- Es muss ein Notfallhandbuch erstellt und aktuell gehalten werden, das auch im Notfall und bei Ausfall der Informationstechnik verfügbar ist. (DER.4.A1, NET.3.1.A22)
- Im Notfallhandbuch muss festgehalten werden, wer in welchen Fällen wen informiert und wer dann welche Aktivitäten durchführt. (DER.4.A1)
- Im Notfallhandbuch müssen die wichtigsten für das Unternehmen relevanten Notfälle behandelt werden. (DER.4.A1)
- Im Notfallhandbuch muss beschrieben werden, wie bei Störungen und Ausfällen vorzugehen ist, um die Geschäftsprozesse aufrecht zu erhalten. (NET.3.1.A22)
- Die im Notfallhandbuch beschriebenen Abläufe müssen regelmäßig geübt und überprüft werden. (NET.3.1.A22, DER.4.A1)
- Für Notfälle müssen auf sicherheitsrelevanten und geschäftskritischen IT-Systemen Notfall-Kennungen mit Administrationsrechten eingerichtet werden. (OPS.1.1.2.A2)
- Bei Änderungen an Informationstechnik oder Konfigurationen muss sichergestellt sein, dass dies notfalls wieder rückgängig gemacht werden kann. (OPS.1.1.3.A1, SYS.4.X.A12)
- Bei der Notfallplanung muss berücksichtigt werden, dass Netzwerke oder Netzwerkgeräte gestört sein können ausfallen können oder kompromittiert werden können. (NET.1.1.A27, NET.3.2.A32)
- Sicherungskopien müssen so abgelegt werden, dass im Notfall darauf zugegriffen werden kann. (NET.3.1.A8)

3.19 Backup

Für den Themenbereich „Backup“ müssen folgende Anforderungen erfüllt werden:

- Auf der Grundlage der identifizierten internen und externen Vorgaben muss festgelegt werden, für welche Daten auf welche Weise und wie häufig eine Datensicherung durchgeführt wird. (CON.3.A1/A2/A4/A6/A11)
- Die festgelegten Datensicherungen müssen regelmäßig durchgeführt werden. (CON.3.A5)
- Es muss regelmäßig getestet werden, ob die Datensicherungen den Festlegungen entsprechen und ob sie problemlos und in angemessener Zeit zurückgespielt werden können. (CON.3.A5/A6)
- Datensicherungen müssen vor unbefugtem Zugriff geschützt werden. (CON.3.A5)
- Wenn für die Datensicherung ein Online-Speicher genutzt wird, müssen folgende Punkte im Vertrag geregelt sein: Ort der Speicherung, Dienstgüte (SLA), Authentisierung, Verschlüsselung der gespeicherten Daten und Verschlüsselung auf dem Übertragungsweg. (CON.3.A9)

- Datenträger von Datensicherungen müssen so aufbewahrt werden, dass sie vor unbefugtem Zugriff geschützt sind, von den gesicherten IT-Systemen räumlich getrennt sind und dass die Vorgaben des Herstellers zur Lagerung (z. B. Temperatur, Klima) erfüllt sind. (CON.3.A12)
- Informationen, die aufgrund externer oder interner Vorgaben aufbewahrt werden müssen, müssen in die Datensicherung einbezogen werden. (CON.9.A7)
- Wichtige Konfigurationsdaten von Informationstechnik müssen in die Datensicherung einbezogen werden. (NET.3.1.A8)
- Die Festlegungen zur Datensicherung müssen regelmäßig aktualisiert werden. (CON3.A1)

3.20 IT-Administration

Für den Themenbereich „IT-Administration“ müssen folgende Anforderungen erfüllt werden:

- Es muss festgelegt werden, welche Personen administrative Tätigkeiten übernehmen und somit die Rolle von Administratoren haben. Diese Festlegung muss allen Mitarbeitern bekannt gegeben werden. (OPS.1.1.2.A7/A12, NET.3.1.A10)
- Die Aufgaben, Befugnisse und Pflichten von Administratoren müssen schriftlich festgelegt werden. (OPS.1.1.2.A7/A12, NET.3.1.A10)
- Nur Administratoren dürfen Informationstechnik installieren, deinstallieren, ändern, konfigurieren und warten. (OPS.1.1.3.A2, SYS.2.1.A15)
- Bei administrativen Arbeiten muss sichergestellt werden, dass alle betroffenen Personen vorab beteiligt bzw. informiert werden. (OPS.1.1.2.A8, OPS.1.1.3.A6/A7)
- Es muss eine Übersicht erstellt und aktuell gehalten werden über alle vorhandenen Geräte, die einen Einfluss auf die Informationssicherheit haben können. Neben IT-Systemen der Büro-IT gehören dazu beispielsweise auch Internet-of-Things-Geräte. (OPS.1.1.2.A20)
- Es muss ein Verzeichnis der eingesetzten Software einschließlich der jeweiligen Lizenzen geführt und aktuell gehalten werden. (APP.6.A9)
- Informationstechnik darf nur lokal am jeweiligen Gerät oder mittels eines dedizierten internen Administrations-Clients administriert werden. (OPS.1.1.2.A6, SYS.2.1.A20/A44, SYS.4.1.A7/A18, NET.1.1.A21, NET.3.1.A4/A6/A13, NET.3.2.A6/A7/A18)
- Administrationsschnittstellen müssen netzwerktechnisch und zeitlich reglementiert werden. Es müssen sichere Protokolle und Verschlüsselung nach dem Stand der Technik für die Administration verwendet werden. Nicht verwendete Administrationsschnittstellen müssen deaktiviert werden. (OPS.1.1.2.A6, SYS.2.1.A20/A44, SYS.4.1.A7/A18, NET.1.1.A21, NET.3.1.A4/A6/A13, NET.3.2.A6/A7/A18)
- Administrations-Clients müssen in das Sicherheitskonzept integriert sein und entsprechend abgesichert werden. (OPS.1.1.2.A6, SYS.2.1.A20/A44, SYS.4.1.A7/A18, NET.1.1.A21, NET.3.1.A4/A6/A13, NET.3.2.A6/A7/A18)
- Es muss sichergestellt werden, dass Software bei Bedarf neu installiert werden kann. (APP.6.A8)

3.21 Dokumentation

Für den Themenbereich „Dokumentation“ müssen folgende Anforderungen erfüllt werden:

- Alle wesentlichen Prozesse, Pläne, Konzepte, Vorgaben, Regelungen, Entscheidungen, Aktivitäten, Arbeitsergebnisse, Einstellungen und Änderungen, die die Informationstechnik und/oder die Informationssicherheit betreffen, müssen dokumentiert und archiviert werden. (ISMS.1.A12/A13, ORP.4.A1/A3/A15/A16, ORP.5.A1, CON.6.A8, OPS.1.1.2.A11/A12, OPS.1.1.3.A1/A5/A11, OPS.1.1.4.A1/A2/A5/A9, OPS.1.1.5.A1, OPS.1.1.6.A1/A3/A4, DER.1.A1/A3/A13, DER.2.1.A7/A16, DER.2.2.A11, DER.3.1.A3/A5/A6/A7/A8/A10/A13/A14/A16/A22/A23/A25, APP.6.A1/A4/A8, SYS.2.1.A42/A9/A10/A15/A16/A43/A44, SYS.4.X.A3/A6/A7/A12, NET.1.1.A2/A16/A17/A22/A25/A26, NET.3.1.A1/A9/A10/A12/A23, NET.3.2.A1/A2/A4/A14)
- Die Dokumentation muss auf dem aktuellen Stand gehalten werden. (ORP.5.A1, OPS.1.1.5.A1, NET.1.1.A2/A16/A17/A22/A25)
- Die Dokumentation muss vor unberechtigten Zugriffen geschützt werden. (NET.3.2.A1/A2/A4/A14, ORP.4.A3/A16)
- Die Dokumentation muss in die Datensicherung einbezogen werden, falls sie digital erfolgt. (ORP.4.A3/A16)

3.22 Einsatz kryptografischer Verfahren

Für den Themenbereich „Einsatz kryptografischer Verfahren“ müssen folgende Anforderungen erfüllt werden:

- Die Informationstechnik muss so konfiguriert werden, dass die eingesetzten kryptografischen Verfahren, Algorithmen und die Schlüssellängen der Technischen Richtlinie BSI TR-02102 (Teile 1 bis 4) entsprechen. (CON.1.A1, CON.9.A8, SYS.2.1.A18)
- Unsichere kryptographische Verfahren müssen in den eingesetzten Webbrowsern deaktiviert werden.(APP.1.2.A2, NET.3.2.A21)
- Webbrowser müssen die Gültigkeit der Server-Zertifikate mithilfe der öffentlichen Schlüssel und unter Berücksichtigung der Gültigkeitszeiträume vollständig prüfen. Auch der Sperrstatus der Server-Zertifikate muss von den Webbrowsern geprüft werden. Die Zertifikatskette einschließlich der Wurzelzertifikate muss verifiziert werden. (APP.1.2.A3, NET.3.2.A21)
- Webbrowser müssen den Benutzer informieren und die Verbindung abbrechen, wenn Zertifikate fehlen, ungültig sind oder widerrufen wurden. Die Kommunikation darf erst fortgesetzt werden, wenn der Benutzer dies ausdrücklich bestätigt hat. (APP.1.2.A3, NET.3.2.A21)
- Webbrowser müssen dem Benutzer eindeutig und gut sichtbar darstellen, ob die Kommunikation verschlüsselt erfolgt. (APP.1.2.A3)
- Kryptografische Schlüssel müssen so gespeichert bzw. aufbewahrt werden, dass Unbefugte nicht darauf zugreifen können. Dies gilt auch für Datensicherungen. Langlebige kryptografische Schlüssel müssen außerhalb der eingesetzten IT-Systeme aufbewahrt werden. (CON.1.A2)
- Bei einer Langzeitspeicherung verschlüsselter Daten muss sichergestellt werden, dass auf die Daten auch nach längeren Zeiträumen noch zugegriffen werden kann. Außerdem muss regelmäßig geprüft werden, ob die verwendeten kryptografischen Verfahren, Algorithmen und Schlüssellängen noch dem Stand der Technik entsprechen. (CON.1.A2)
- Kryptografische Schlüssel müssen mit geeigneten Schlüsselgeneratoren und in einer sicheren Umgebung erzeugt werden. (CON.1.A4)
- Kryptografische Schlüssel dürfen immer nur einem Einsatzzweck dienen. Für Verschlüsselung und digitale Signatur müssen unterschiedliche Schlüssel verwendet werden. (CON.1.A4)
- Beim Austausch von kryptografischen Schlüsseln muss hierfür ein sicheres Verfahren verwendet werden. (CON.1.A4)
- Beim Einsatz kryptografischer Schlüssel oder Zertifikate muss die authentische Herkunft, Integrität und Korrekt-heit überprüft werden. (CON.1.A4, SYS.2.1.A18)
- Kryptografische Schlüssel müssen sicher aufbewahrt und verwaltet werden. (CON.1.A4)
- Es muss festgelegt werden, für welche Prozesse, Anwendungen, Systeme und Kommunikationsverbindungen kryptografische Verfahren eingesetzt werden sollen. Diese Festlegungen müssen zeitnah umgesetzt werden. (CON.1.A6)
- Sensitive Informationen müssen verschlüsselt werden, wenn sie über das Internet oder andere ungesicherte Netze übertragen werden. (CON.1.A3, CON.9.A8, SYS.2.1.A18)
- Es müssen Vorgehensweisen festgelegt werden für den regelmäßigen Wechsel von kryptografischen Schlüsseln und für den Fall, dass ein kryptografischer Schlüssel offengelegt wird. (CON.1.A4)
- Nicht mehr benötigte kryptografische Schlüssel und Zertifikate müssen sicher gelöscht bzw. vernichtet werden. (CON.1.A5)

3.23 Protokollierung und Detektion

Für den Themenbereich „Protokollierung und Detektion“ müssen folgende Anforderungen erfüllt werden:

- Informationstechnik muss so konfiguriert werden, dass alle sicherheitsrelevanten Ereignisse protokolliert werden. Dabei müssen die Herstellervorgaben für die jeweiligen IT-Systeme und Anwendungen beachtet werden. (OPS.1.1.5.A2, NET.3.1.A7, NET.3.2.A9)
- Soweit dies technisch möglich ist, müssen auch solche Ereignisse protokolliert werden, die auf Programmabstürze oder ähnliche Fehler hindeuten. (OPS.1.1.5.A6)

- Es muss sichergestellt werden, dass sich der jeweilige Zeitpunkt der protokollierten Ereignisse eindeutig feststellen lässt. (OPS.1.1.5.A4, NET.3.2.A22)
- Protokollierungsdaten müssen technisch vor unkontrollierter Löschung oder Veränderung geschützt werden. (OPS.1.1.5.A5)
- Protokollierungsdaten müssen bis zur festgelegten Löschfrist aufbewahrt und vor unberechtigtem Zugriff geschützt werden. Insbesondere müssen die Protokollierungsdaten bei einem Neustart der jeweiligen IT-Systeme erhalten bleiben. (OPS.1.1.5.A8)
- Soweit dies technisch möglich ist, dürfen Administratoren keine Berechtigung haben, aufgezeichnete Protokollierungsdaten zu verändern. (OPS.1.1.5.A10)
- Soweit dies technisch möglich ist, dürfen nur wenige, explizit benannte Personen die Berechtigung haben, aufgezeichnete Protokollierungsdaten zu löschen. (OPS.1.1.5.A10)
- Protokollierungsdaten müssen nach einer vorgegebenen Frist und nach einem vorgegebenen Verfahren gelöscht werden. (OPS.1.1.5.A5)
- Auf der Grundlage der internen und externen Vorgaben muss festgelegt werden, wie sicherheitsrelevante Ereignisse erkannt werden. (DER.1.A1)
- Es muss festgelegt werden, wer unter welchen Voraussetzungen über erkannte sicherheitsrelevante Ereignisse informiert werden muss und wer für die Auswertung dieser Ereignisse zuständig ist. (DER.1.A3/A6)
- Vorhandene Funktionen von Anwendungen und IT-Systemen zur Erkennung sicherheitsrelevanter Ereignisse müssen aktiviert und benutzt werden. (DER.1.A5)
- Erkannte sicherheitsrelevante Ereignisse müssen auf den festgelegten Wegen gemeldet, mit den vorliegenden Protokollierungsdaten korreliert und ausgewertet werden. (DER.1.A5)
- Gesammelte Meldungen sicherheitsrelevanter Ereignisse müssen regelmäßig strichprobenartig kontrolliert werden. (DER.1.A5)
- Protokollierungsdaten müssen regelmäßig auf der Grundlage eines festgelegten Verfahrens ausgewertet werden. (DER.1.A6)
- Auf Routern, Paketfiltern und Firewalls zum Internet und zu anderen Fremdnetzen müssen die vorhandenen Funktionen zur Erkennung sicherheitsrelevanter Ereignisse aktiviert werden. (DER.1.A9)
- Funktionen auf zentralen Systemen oder auf Endsystemen zur Erkennung von Schadprogrammen oder anderen sicherheitsrelevanten Ereignissen müssen möglichst so konfiguriert werden, dass auch Daten erfasst werden, die verschlüsselt übertragen werden. (DER.1.A10, NET.3.2.A20/A21)
- Wenn Detektionssysteme zur automatischen Erkennung sicherheitsrelevanter Ereignisse eingesetzt werden, müssen die Detektionssignaturen dieser Systeme auf dem aktuellen Stand gehalten werden. (DER.1.A11)
- Meldungen von Gefahrenmeldeanlagen müssen unter Beachtung der dafür geltenden technischen Anschlussbedingungen (TAB) auf eine Alarmempfangsstelle der hilfeleistenden Stellen aufgeschaltet werden. Die ausgewählte Alarmempfangsstelle muss jederzeit erreichbar und technisch sowie personell in der Lage sein, geeignet auf die gemeldete Gefährdung zu reagieren. (SYS.4.X.A11)
- Die Firewall muss bei Fehlern und bei Überschreitung von Grenzwerten eine Alarmmeldung an festgelegte Ansprechpersonen senden. (NET.3.2.A23)

3.24 Behandlung von Sicherheitsvorfällen

Für den Themenbereich „Behandlung von Sicherheitsvorfällen“ müssen folgende Anforderungen erfüllt werden:

- Die Geschäftsführung muss definieren, was ein Sicherheitsvorfall ist und wie sich ein Sicherheitsvorfall von einer Störung im Normelbetrieb abgrenzt. (DER.2.1.A1)
- Die Geschäftsführung muss schriftlich festlegen, was im Fall eines Sicherheitsvorfalls durch wen zu tun ist, welche Ziele Priorität haben und wie sich die Mitarbeiter und Administratoren zu verhalten haben. (DER.2.1.A2/A10/A11, DER.2.2.A4)
- Bei einem Sicherheitsvorfall muss die Geschäftsführung entscheiden, ob der Vorfall durch einen Forensik-Dienstleister untersucht werden soll. In diesem Fall muss der Dienstleister auf die Einhaltung der relevanten IT-Grundschutz-Anforderungen, insbesondere den Baustein DER.2.2, verpflichtet werden. (DER.2.2, SYS.2.1.A6)

- Bei einem Sicherheitsvorfall müssen alle betroffenen internen und externen Stellen zeitnah über den Vorfall und über die ggf. erforderlichen Maßnahmen informiert werden. (DER.2.1.A4/A14)
- Bei einem Sicherheitsvorfall muss geprüft werden, welche internen und externen Stellen bei der Behandlung des Vorfalls einbezogen werden müssen. Dabei muss insbesondere geprüft werden, ob und ggf. welche Meldepflichten bestehen. (DER.2.1.A4)
- Bei einem Sicherheitsvorfall müssen die betroffenen Komponenten vom Netzwerk getrennt werden. (DER.2.1.A6, SYS.2.1.A6)
- Bei einem Sicherheitsvorfall müssen alle erforderlichen Daten gesichert werden, die Aufschluss über Art und Ursache des Problems geben könnten. (DER.2.1.A6)
- Bei einem Sicherheitsvorfall müssen zunächst die Ursachen ermittelt und anschließend Maßnahmen erarbeitet werden, um das Problem zu beheben. Die Geschäftsführung muss die Maßnahmen freigeben, bevor sie umgesetzt werden. Schließlich müssen die Ursachen beseitigt und ein sicherer Zustand hergestellt werden. (DER.2.1.A5/A7, SYS.2.1.A6)
- Wenn Software oder Daten nach einem Sicherheitsvorfall von Datenträgern wiederhergestellt werden, muss gewährleistet sein, dass die Datenträger nicht von dem Vorfall betroffen waren. (DER.2.1.A6)
- Nach einem Sicherheitsvorfall müssen alle Zugangsdaten auf den betroffenen Komponenten geändert werden, bevor sie wieder in Betrieb genommen werden. (DER.2.1.A6)
- Bevor Komponenten nach einem Sicherheitsvorfall wieder in Betrieb genommen werden, muss sichergestellt werden, dass alle sicherheitsrelevanten Updates/Patches eingespielt sind, dass die Konfiguration den internen/ex-ternen Vorgaben entspricht und dass keine unerlaubten Veränderungen an den Komponenten vorgenommen wurden. (DER.2.1.A6, SYS.2.1.A6)
- Nach einem Sicherheitsvorfall muss eine engmaschige Kontrolle auf weitere sicherheitsrelevante Ereignisse er-folgen. (DER.2.1.A6)
- Für besonders schwerwiegende Szenarien, die durch Sicherheitsvorfälle verursacht werden können, müssen vorab Handlungsanweisungen festgelegt werden. (DER.2.1.A10)
- Die festgelegten Vorgehensweisen zur Behandlung von Sicherheitsvorfällen müssen regelmäßig geübt werden. (DER.2.1.A14)

3.25 Außerbetriebnahme, Aussonderung, Löschung und Vernichtung

Für den Themenbereich „Außerbetriebnahme, Aussonderung, Löschung und Vernichtung“ müssen folgende Anforderungen erfüllt werden:

- Es muss festgelegt werden, welche Informationen, Datenträger, Geräte und Betriebsmittel unter welchen Voraussetzungen gelöscht bzw. vernichtet werden. Dabei müssen alle internen und externen Vorgaben, insbesondere zum Datenschutz und zu Aufbewahrungsfristen, eingehalten werden. (CON.6.A1)
- Bevor schützenswerte Informationen, Datenträger, Geräte und Betriebsmittel entsorgt werden, müssen sie sicher gelöscht oder vernichtet werden. Dabei müssen auch Datenträger für Backups berücksichtigt werden. (CON.6.A2, ORP.1.A8, SYS.2.1.A27)
- In Abhängigkeit vom Schutzbedarf der jeweils verarbeiteten Daten und von den internen/externen Vorgaben müssen angemessene Verfahren zum Löschen bzw. Vernichten von Informationen, Datenträgern, Geräten und Betriebsmitteln festgelegt werden. Hierbei müssen die jeweils relevanten Normen und ggf. die Vorgaben der Hersteller berücksichtigt werden. (CON.6.A4/A12)
- In Abhängigkeit vom Schutzbedarf der jeweils verarbeiteten Daten müssen Informationen, Datenträger, Geräte und Betriebsmittel entsprechend der festgelegten Anforderungen sicher vernichtet werden, wenn eine sichere Löschung zwar erforderlich, aber nicht möglich ist. (CON.6.A13)
- Bei Außerbetriebnahme von Software muss sichergestellt werden, dass alle betroffenen Personen beteiligt bzw. informiert werden. (APP.6.A12)
- Bei der Deinstallation von Software müssen möglichst alle für das Produkt angelegten und nicht mehr benötigten Dateien entfernt werden. Außerdem müssen möglichst alle Einträge in Systemdateien, die für das Produkt vorgenommen wurden und nicht länger benötigt werden, rückgängig gemacht werden. (APP.6.A13)
- Bei der Außerbetriebnahme von Informationstechnik muss ein Backup der weiterhin benötigten Daten erstellt werden. (SYS.2.1.A27)

- Ausgedruckte Dokumente mit vertraulichen Informationen müssen geeignet vernichtet werden, wenn sie nicht (mehr) benötigt werden. (SYS.4.1.A22)
- Bevor wiederbeschreibbare Datenträger weitergegeben, wiederverwendet oder ausgesondert werden, müssen sie in geeigneter Weise gelöscht werden. (SYS.4.5.A7)

3.26 Baulich-physische Infrastruktur

Für den Themenbereich „baulich-physische Infrastruktur“ müssen folgende Bausteine und Anforderungen erfüllt werden:

- Der Baustein INF.1 *Allgemeines Gebäude* des IT-Grundschutz-Kompendiums ist für jedes Gebäude einmal anzuwenden.
- Der Baustein INF.5 *Raum sowie Schrank für technische Infrastruktur* des IT-Grundschutz-Kompendiums ist für Räume anzuwenden, in denen technische Infrastruktur betrieben wird. Der Baustein ist ebenfalls anzuwenden, wenn stationäre Container, im Sinne eines großen Schrankes, betrieben werden.
- Der Baustein INF.7 *Büroarbeitsplatz* des IT-Grundschutz-Kompendiums ist auf jeden Raum im Informationsverbund anzuwenden, der als Büroarbeitsplatz genutzt wird.
- Der Baustein INF.12 *Verkabelung* des IT-Grundschutz-Kompendiums ist einmal auf die Verkabelung in Gebäuden und Räumen anzuwenden, zusätzlich zum Baustein INF.1 *Allgemeines Gebäude*. Die Anforderungen des Bausteins sind immer sowohl auf die IT- als auch auf die elektronische Verkabelung anzuwenden.
- Gefahrenmeldeanlagen müssen an eine stabile, unterbrechungsfreie und ausreichend dimensionierte Stromversorgung angeschlossen werden. Die Stromversorgung muss entsprechend der anlagenspezifischen Anforderungen ausgelegt sein. (SYS.4.X.A9)
- Wichtige Bestandteile von Gefahrenmeldeanlagen müssen vor Brandeinwirkung und eindringendem Wasser geschützt werden. (SYS.4.X.A10)

4 Glossar

Es wird auf das Cyber-Glossar des BSI verwiesen:

https://www.bsi.bund.de/cyberglossar

Anhang B
Anforderungskatalog zum Nachweisder IT-Sicherheit bei der Beförderungvon sonstigen radioaktiven Stoffen basierend auf den IT-Sicherungsanforderungen der SEWD-Richtlinie sonstige radioaktive Stoffe
Version 1.0

1 Einleitung

Der vorliegende Anforderungskatalog legt eine auf die Situation von Inhabern einer Genehmigung nach dem Strahlenschutzgesetz (StrlSchG) angepasste Vorgehensweise dar, mit der für die Beförderung von sonstigen radioaktiven Stoffen zu betrachtenden IT-Systeme ein Sicherungsniveau gewährleistet werden kann, das den Standardsicherungsmaßnahmen des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht.

Durch die besonderen Rahmenbedingungen bei der Beförderung von sonstigen radioaktiven Stoffen sowie die spezifischen Festlegungen im Rahmen der SEWD-Richtlinie sonstige radioaktive Stoffe ist es nicht erforderlich, alle im Rahmen des BSI-Grundschutzes (IT-Grundschutzkompendium /1/) zu behandelnden Themen im Rahmen dieses Anforderungskatalogs abzudecken. Der vorliegende Anforderungskatalog ist daher nur in Verbindung mit den weiteren regulatorischen Vorgaben für Genehmigungen nach §§ 27 und 29 StrlSchG und der „Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und bei der Beförderung von sonstigen radioaktiven Stoffen (SEWD-Richtlinie sonstige radioaktive Stoffe)“ /2/ zur Anwendung zu bringen.

Die Umsetzung des vorliegenden Anforderungskatalogs stellt dabei eine Möglichkeit dar, wie durch den Antragsteller in Genehmigungsverfahren nach den §§ 27 und 29 StrlSchG der IT-spezifische Nachweis erbracht werden kann. Eine anderweitige Ausgestaltung dieser Nachweisführung, z. B. in Form einer Dokumentation, die u. a. den ausschließlichen Einsatz von BSI-zertifizierten informationstechnischen Produkten und Managementsystemen bei der Beförderung von sonstigen radioaktiven Stoffen belegt, bleibt dem Antragsteller unbenommen.

2 Informationssicherheitsmanagement

Es ist vom Antragsteller/Genehmigungsinhaber ein dem Stand der Technik entsprechendes Informationssicherheitsmanagement (ISM) zu etablieren und in die Gesamtorganisation einzubinden.

Sofern kein ISM vorhanden ist, sind für die Festlegung und Umsetzung geeigneter IT-Sicherheitsmaßnahmen mindestens die nachfolgend genannten Managementprozesse (MP) und die damit verbundenen Verantwortlichkeiten zu etablieren.

Zu jedem Managementprozess sind entsprechende Regelungen zu treffen und schriftlich zu dokumentieren. Die Ergebnisse der Umsetzung der Managementprozesse sind in geeigneter Form aufzuzeichnen.

MP1: Festlegung der Verantwortlichkeit für Informationssicherheit

Die verantwortlichen Personen (und gegebenenfalls ihre Vertreter) mit den ihnen zugeordneten Funktionen/Aufgaben sind zu benennen. Für das eingesetzte Personal sind die für die Ausübung ihrer Tätigkeiten erforderlichen Qualifikationen sicherzustellen und nachzuweisen.

MP2: Festlegung der erforderlichen Maßnahmen der IT-Sicherheit

- Ermittlung und detaillierte Erfassung der sogenannten „genutzten Informationstechnik“, die Bestandteil von Sicherungsmaßnahmen ist oder anderweitig zu einer Verletzung der Schutzziele der SEWD-Richtlinie sonstige radioaktive Stoffe beitragen kann (vgl. /2/), samt ihrer Schnittstellen (genutzt und ungenutzt)
- Festlegung, Auslegung und Umsetzung erforderlicher Sicherungsmaßnahmen

Bei der Festlegung und Auslegung der erforderlichen IT-Sicherungsmaßnahmen sind die Schutzthemen und Schutzaspekte gemäß Kap. 3 dieses Anforderungskatalogs zu berücksichtigen.

Hierbei sind alle relevanten IT-Szenarien zu betrachten, incl. Angreifer mit privilegierten Zugriffsmöglichkeiten.

Die für die einzelnen IT-Systeme festgelegten und umgesetzten Sicherungsmaßnahmen sind in IT-Security-Handbüchern (s. Kap. 12) zusammenfassend darzustellen.

MP3: IT-Sicherheit in der Lieferantenbeziehung

Für IT-Systeme, die von Dritten (Hardware- und Softwarelieferanten und Systemintegratoren) bezogen werden, ist ein Vorgehen zu etablieren, durch das sichergestellt werden kann, dass ein möglichst großer Teil erforderlicher IT-Sicherheitsmaßnahmen bereits durch den Lieferanten abgedeckt wird.

- Lieferantenunabhängige Festlegung der IT-Sicherheitsanforderungen für Hardware- und Softwarelieferanten sowie für Systemintegratoren

- Berücksichtigung von IT-Sicherheitsaspekten in der Vertragsgestaltung mit den Hardware- und Softwarelieferanten sowie mit Systemintegratoren
- Test- und Freigabeverfahren für Hardware- und Softwarelieferanten sowie für Systemintegratoren
- Vereinbarung über Datenaustausch

Für bereits bestehende IT-Systeme, für die die IT-Sicherheit in der Lieferantenbeziehung nicht in der zuvor beschriebenen Weise gewährleistet werden kann, sind erforderliche IT-Sicherheitsmaßnahmen durch den Antragsteller/Genehmigungsinhaber sicherzustellen, ggf. unter Einbeziehung kompensatorischer Maßnahmen wie z. B. Nachweise zur Betriebsbewährung, regelmäßige Prüfungen, Systemüberwachung und physische und logische Absicherung.

MP4 IT-Sicherheitsmaßnahmen überprüfen und anpassen

IT-Sicherheitsmaßnahmen sind zu überprüfen:

- Regelmäßig auf Wirksamkeit
- Bei sich ändernden Gegebenheiten, z. B. bei Änderungen an IT-Systemen, der Umgebungsbedingungen oder der allgemeinen IT-Sicherheitslage

Informationen zur IT-Sicherheitslage und zu bekannten Schwachstellen können z. B. auf verschiedenen kommerziellen oder nicht kommerziellen Plattformen sowie bei Herstellern abgerufen werden.

Wenn hierbei Erkenntnisse über Unzulänglichkeiten der etablierten IT-Sicherheitsmaßnahmen offenkundig werden, sind geeignete Anpassungen zur Wiederherstellung des erforderlichen Sicherungsniveaus vorzunehmen.

3 Vorgehensweise zur systemspezifischen Ermittlung der erforderlichen Standard-Sicherungsmaßnahmen

Die Standard-Sicherungsmaßnahmen des BSI sind im IT-Grundschutz-Kompendium (ITGSK) in den IT-Grundschutzbausteinen (ITGSB) zusammengestellt. Diese Maßnahmensammlung werden nachfolgend zur Vereinfachung des Vorgehens im Rahmen von Genehmigungsverfahren für die Beförderung von sonstigen radioaktiven Stoffen in Schutzthemen (ST) und ihnen zugeordnete Schutzaspekte (SA) strukturiert. Im Einzelnen bestehen folgende Schutzthemen:

ST1: Sichere Installation und Modifikation

ST2: Funktionsreduktion auf das Erforderliche

ST3: Härtung

ST4: Überwachung des IT-Systems und seiner Datenkommunikation

ST5: Regelmäßige Prüfungen

ST6: Notfallvorsorge

ST7: Systemadministration und Dokumentation

ST8: Kryptografie

In den folgenden Kapiteln ist zu den einzelnen Schutzthemen dargelegt, welche Schutzaspekte bei der Behandlung des jeweiligen Schutzthemas mindestens zu betrachten sind.

Da die in den Kapiteln 4–11 aufgeführten Schutzthemen und Schutzaspekte aus den im ITGSK angesprochenen Schutzaspekten abgeleitet wurden, ist es grundsätzlich hinreichend, bei der Festlegung der Standard-Sicherungsmaßnahmen die zu den einzelnen Schutzthemen aufgeführten Schutzaspekte zu behandeln. Hierbei sind für die Umsetzung in konkrete Standard-Sicherungsmaßnahmen das jeweilige Erfordernis und gegebenenfalls die relevanten IT-Szenarien für die jeweiligen IT-Systeme zu ermitteln und zu berücksichtigen.

Können einzelne Schutzaspekte zur Sicherstellung des anforderungsgerechten Schutzniveaus nicht im erforderlichen Umfang behandelt werden, ist die Gleichwertigkeit kompensatorischer Maßnahmen im Einzelfall nachzuweisen.

Zur nachvollziehbaren Dokumentation der Umsetzung der Schutzaspekte sind für jedes IT-System in einem sogenannten IT-Security-Handbuch, gegliedert nach den Schutzthemen und -aspekten, die spezifizierten Standard-Sicherungsmaßnahmen sowie die zugrunde gelegten Randbedingungen aufzuführen und zu beschreiben.

4 Schutzthema ST1: Sichere Installation und Modifikation

Die Installation eines IT-Systems ist von integritätsgesicherten Quellen nach einem geplanten Installationsprocedere durchzuführen. Gleiches gilt auch für Modifikationen am IT-System.

Zu diesem Schutzthema gehören im Einzelnen folgende Aspekte:

- SA1.1: Betriebssystem-Installation aus nachvollziehbar korrekten Quellen
- SA1.2: Applikations-Installation aus nachvollziehbar korrekten Quellen
- SA1.3: Erstellung von integritätsgesicherten Images des geprüften IT-Systems
- SA1.4: Modifikation ausschließlich aus nachvollziehbaren und integritätsgesicherten Codequellen

Nachvollziehbare integritätsgesicherte Quellen sind z. B. Codes, deren Authentizität und Integrität durch deren Beschaffungsvorgang oder bei Datenfiles über kryptografische Hashfunktionen sichergestellt sind. Beispiele sind Original-CDs/DVDs des Herstellers oder Installationsfiles mit vom Hersteller veröffentlichten Hashwerten.

Für bestehende Installationen, bei denen die Installationsmedien nicht mehr verfügbar sind, aber die Korrektheit der bestehenden Installation des IT-Systems anderweitig nachgewiesen (z. B. durch Betriebsbewährung oder langjährig positive Ergebnisse bei Funktionsprüfungen) und deren Schadsoftwarefreiheit plausibel dargelegt werden kann, kann ersatzweise ein sog. Image, d. h. ein Abzug der Software und der Konfiguration des IT-Systems ohne variable Daten, erstellt und als Referenz für den weiteren Betrieb, insbesondere zur Integritätssicherung, verwendet werden.

5 Schutzthema ST2: Funktionsreduktion auf das Erforderliche

Die IT-Systeme sind nach den Grundsätzen

- Verzicht auf unnötige Funktionen
- Verzicht auf unnötigen Komfort

auszulegen, da Funktionsvielfalt und Komfortfunktionen Angreifern ihr Vorgehen erleichtern.

Zu diesem Schutzthema gehören im Einzelnen folgende Aspekte:

- SA2.1: Verzicht auf nicht für die sicherungstechnische Aufgabe des Systems erforderliche Komponenten in der Hardware-Konfiguration des IT-Systems (z. B: WLAN-Module, Baseboard Management Controller (BMC) mit remote Intelligent Platform Management Interface (IPMI))
- SA2.2: Tailoring des Betriebssystems auf die funktionalen Anforderungen
- SA2.3: Kein Vorhalten von nicht für Kernaufgaben erforderlichen Anwendungsprogrammen
- SA2.4: Kein Vorhalten von Treibern für nicht erforderliche Hardware-Komponenten
- SA2.5: Kein Vorhalten von Development Tools auf IT-Systemen im Produktionsbetrieb (Wirksysteme in Abgrenzung z. B. zu Wartungs- und Servicesystemen)
- SA2.6: Restriktion auf unbedingt erforderliche Tools zum System Management

Development Tools und Tools zum komfortablen System Management bzw. zur Fehlersuche (Debugging) sind Werkzeuge, die für einen Angriff auf ein IT-System sehr vorteil-haft genutzt werden können und stellen deshalb auf IT-Systemen im Produktionsbetrieb ein hohes Risiko dar. Sind solche Tools erforderlich, so sind sie auf getrennten Rechnern einzusetzen und es ist sicherzustellen, dass von diesen aus nicht auf IT-Systeme im Betrieb schädlich eingewirkt werden kann.

6 Schutzthema ST3: Härtung

Härtung bedeutet, ein IT-System so zu installieren und zu konfigurieren, dass Störmaßnahmen oder sonstige Einwirkungen Dritter erschwert werden. Standardprodukte unterstützen dies auch durch spezielle Security Funktionen, die entsprechend zu konfigurieren sind.

Wirksame Härtung bedeutet, alle relevanten Aspekte der missbräuchlichen Nutzung in Betracht zu ziehen und auch zu berücksichtigen, dass andere Schutzmaßnahmen, wie z. B. der physische Schutz, Schwächen aufweisen können. Insbesondere dann fällt der Härtung eine wichtige Rolle zu, um im Sinne eines Defense-in-Depth-Konzepts Angriffswege zu erschweren oder Schadensauswirkungen einzugrenzen.

Je nach Technologie und Funktionalität der IT-Systeme gibt es vielfache Ausprägungen der Härtung. Es werden deshalb nachfolgend als Schutzaspekte Härtungsprinzipien aufgeführt, und dazu teilweise spezifische Ausprägungen bzw. konkrete Umsetzungen als Beispiele aufgeführt.

Zu diesem Schutzthema gehören im Einzelnen folgende Aspekte:

- SA3.1: Es ist sicherzustellen, dass das IT-System aus einer genau festgelegten Quelle bootet, die nicht ohne privilegierten Administrationszugriff auf das System verändert werden kann.
- SA3.2: Die Nutzung aller nicht für die Aufgabenerfüllung erforderlichen Schnittstellen des IT-Systems ist zu verhindern, z. B. durch:
  - Entfernung von Schnittstellen
  - Dauerhafte physische/logische Blockade von Schnittstellen
  - Absicherung der Schnittstellen zu sowie durch BIOS, Hardware-Konfiguration, System Management Tools
- SA3.3: Deaktivierung aller nicht erforderlichen Dienste[5], z. B.:
  - im Betriebssystem
  - in der Konfiguration von Netzwerkinfrastruktur-Komponenten
- SA3.4: Die Filterfunktionen des IT-Systems zur Einschränkung der Kommunikation über die Schnittstellen des IT-Systems sind zu aktivieren und restriktiv zu konfigurieren, z. B. durch:
  - Filterung der zugelassenen Protokolle über Firewall-Funktionen
  - Filterung der zugelassenen Kommunikationspartner über Firewall-Funktionen
  - Filterung der zugelassenen TCP/UDP-Ports über Firewall-Funktionen
  - Filterung der zur Kommunikation zugelassenen Programme über Firewall-Funktionen
- SA3.5: Die Vergabe von Zugriffsrechten ist so vorzunehmen, dass einerseits nur die erforderlichen Benutzerrollen eingerichtet werden und andererseits diese nur mit den jeweils erforderlichen Rechten ausgestattet werden, z. B. durch:
  - Definition von Benutzerrollen und Vergabe von aufgabenspezifischen Benutzeraccounts
  - Vergabe von Zugriffsrechten auf System-Ressourcen (z. B. auf Speichermedien)
  - Rechtevergabe nach dem „Nur-Soweit-Erforderlich“ Prinzip angepasst an die Aufgabenstellung der jeweiligen Benutzerrolle
- SA3.6: Die Funktionen des IT-Systems, die dessen Betrieb automatisch dokumentieren, sind gegen Veränderung zu schützen, z. B. durch:
  - Absicherung der Logging-Funktionen und der Systemlogs gegen unzulässige Veränderung
- SA3.7: Die Authentisierung der Benutzer ist so vorzunehmen, dass die Qualität der Methodik der Rolle des Benutzers angemessen ist. Dies bedeutet, dass die Sicherheit der Authentisierungsmechanismen für Benutzer der Gefährdung angepasst werden sollte. Beispielsweise ist für privilegierte Benutzer eine höhere Sicherheit des Authentisierungsmechanismus vorzusehen. Eine höhere Sicherheit kann z. B. durch stärkere Passwörter und mehr Authentifikations-Faktoren (z. B. 2-Faktor-Authentifikation) erreicht werden.
- SA3.8: Verzicht auf Komfortfunktionen bei der Administration mit hohem Potential für eine missbräuchliche Nutzung für Angriffe, z. B. durch:
  - Verzicht auf eine zentrale Systemadministration über Netzwerkkommunikation, stattdessen dezentrale Administration direkt am IT-System (Systemkonsole)
- SA3.9: Verzicht auf Automatismen und Dynamische Funktionen, stattdessen z. B.:
  - Statische Vergabe von Netzwerkadressen
  - Verzicht auf Namensauflösungsprotokolle (DNS, WINS) via Nameserver

7 Schutzthema ST4: Überwachung des IT-Systems und seiner Datenkommunikation

Die IT-Systeme besitzen überwiegend Funktionen zur Selbstüberwachung und vielfach auch zur Protokollierung dieser Überwachung. Damit durch Eingriffe verursachte inkorrekte Abläufe innerhalb eines IT-Systems erkannt werden können,

[5] In einem IT-System ablaufende Programme, die parallel zu den Anwendungsprogrammen Funktionen im Hintergrund bereitstellen oder auto-matisch ausführen, insbesondere solche, die über das Netzwerk ansprech-bar sind. Betriebssysteme beinhalten in der Regel viele solcher Dienste standardmäßig.

sind diese Funktionen durch entsprechende Konfiguration zu nutzen und deren Meldungen auszuwerten. Zur Auswertung der Meldungen stehen durch die von Inhabern einer Genehmigung für die Beförderung von sonstigen radioaktiven Stoffen etablierten Überwachungsverfahren die Möglichkeiten

- Regelmäßige visuelle Inspektion durch ausreichend fachkundiges Personal am IT-System vor Ort
- Einbindung, ggfs. über Sammelmeldungen, in Meldeanlagen (KMA, GMA, RMA etc.)
- Überwachung mobiler IT-Systeme durch Positionsortung

zur Verfügung.

Zu diesem Schutzthema gehören im Einzelnen folgende Aspekte:

- SA4.1: Angemessene Konfiguration der System-Selbstüberwachungsfunktionen
- SA4.2: Überwachung der Schnittstellennutzung
- SA4.3: Einbindung der Überwachung des IT-Systems in Meldeanlagen
- SA4.4: Regelmäßige Inspektion der Systemüberwachungslogs auf Auffälligkeiten
- SA4.5: Permanenter Schutz vor schädlichem Programmcode durch detektierende Schadsoftwarescanner. Hierzu gehören z. B. Virenscanner mit nur lesendem Zugriff auf IT-Systemen, Servicegeräten und Netzwerk-Gateways, Intrusion Detection Systems (IDS) oder Intrusion Prevention Systems (IPS).

8 Schutzthema ST5: Regelmäßige Prüfungen

Die Sicherstellung der Funktionalität eines IT-Systems hängt davon ab, dass sich die Programme, Konfigurationsparameter und Daten in einem korrekten, d. h. unverfälschten, Zustand befinden. Sind die Programme und Konfiguration unverändert, kann für funktionsgeprüfte IT-Systeme angenommen werden, dass auch die Funktionalität korrekt ist.

Bei IT-Systemen sind Veränderungen an Programmen und Konfigurationsparametern, insbesondere solche, die gezielt herbeigeführt und verschleiert werden, nur schwer zu detektieren, da sie nicht unmittelbar zu einer sich im Betrieb des IT-Systems offenbarenden Fehlfunktion des IT-Systems führen müssen. Es sind daher Maßnahmen festzulegen, um regelmäßig die Integrität des IT-Systems zu verifizieren.

Zu diesem Schutzthema gehören im Einzelnen folgende Aspekte:

- SA5.1: Integritätsprüfung von statischen Teilen von Betriebssystemen, Programmen und Konfigurationsdateien, sowie der Systemhärtung
- SA5.2: Regelmäßige Funktionsprüfungen
- SA5.3: Regelmäßige Überprüfung von detektierenden Schadsoftwarescannern auf Aktualität der Signaturen und Überprüfung der Scanergebnisse
  - Bei kontinuierlich genutzten Systemen: alle ein bis zwei Wochen
  - Bei Systemen mit ereignisbezogenem Einsatz: jeweils innerhalb einer Woche vor und nach einem Einsatz

9 Schutzthema ST6: Notfallvorsorge

Erhöhungen des Risikos von zu erwartenden Störmaßnahmen oder sonstigen Einwirkungen Dritter auf IT-Systeme von Inhabern einer Genehmigung für die Beförderung von sonstigen radioaktiven Stoffen können über IT-Sicherheitswarnungen erkannt und bereits eingetretene IT-Sicherheits-auffälligkeiten oder IT-Sicherheitsvorfälle durch Überwachung gem. ST4 und regelmäßige Prüfungen gem. ST5 detektiert werden. Je nach Schwere des Vorfalls sind ggfs. kurzfristig die Auswirkungen zu analysieren und schadensbegrenzende Maßnahmen festzulegen. Diese können auf Grund der Komplexität der IT-Systeme nicht erst nach Eintreten eines Vorfalls erarbeitet werden, sondern es sind im Sinne der Vorsorge geeignete Maßnahmen vorzuplanen.

Zu diesem Schutzthema gehören im Einzelnen folgende Aspekte:

- SA6.1: Festlegungen, wie bei erkannten IT-Security Auf-fälligkeitenIVorfällen spezifisch für das IT-System generell vorzugehen ist (z. B. Vollständige/Teilweise Trennung des IT-Systems von Kommunikationssystemen, schnellstmöglicher Ersatz des IT-Systems durch ein integritätsgesichertes Ersatzgerät, Abschalten von Teilfunktionen des IT-Systems, z. B. Sperrung bestimmter privilegierter Accounts etc.)

- SA6.2: Festlegung einer Ersatzgerätestrategie für das IT-System
- SA6.3: Festlegungen für den Notbetrieb eines IT-Systems auch im Verbund mit anderen IT-Systemen
- SA6.4: Festlegung von Maßnahmen zur Beweissicherung

10 Schutzthema ST7: Systemadministration und Dokumentation

Für den sicheren Betrieb von IT-Systemen ist eine sorgfältige Planung und Durchführung der Administrationstätigkeiten erforderlich. Sowohl Planung als auch Durchführung sind zu dokumentieren, um unabhängig von den Personen, die als Administratoren tätig werden, eine geregelte und konsistente Umsetzung aller Anforderungen an den sicheren Betrieb eines IT-Systems sicherzustellen und nachweisen zu können.

Die schriftlichen Vorgaben (Planungsdokumentation) müssen gewährleisten, dass bei der Installation und Wartung die Integrität der IT-Systeme sichergestellt wird und die vorgesehenen Aufgaben erfüllt werden. Die Betriebsdokumentation stellt sicher, dass die Kontinuität in der Arbeit unterschiedlicher Administratoren gegeben ist und ist wichtig, damit Störungsursachen zielgerichtet analysiert und erforderliche Routinemaßnahmen belegt werden können.

Die Dokumentation soll so beschaffen sein, dass sie nicht nur von Administratoren des IT-Systems, sondern auch von fachkundigen Dritten nachvollzogen werden kann. Zur Reduktion des Aufwandes empfiehlt sich die Erstellung von Referenzinstallationen für IT-Systeme vergleichbarer Technologie und Aufgabenstellung und eine Standardisierung von administrativen Vorgehensweisen.

Zu diesem Schutzthema gehören im Einzelnen folgende Aspekte:

- SA7.1: Schriftliche Vorgaben für die Installation des Systems
- SA7.2: Schriftliche Vorgaben für die Konfiguration des Systems
- SA7.3: Schriftliche Vorgaben zur Durchführung von Änderungen an Parametern
- SA7.4: Schriftliche Vorgaben zur Durchführung von Änderungen an Programmen
- SA7.5: Schriftliche Vorgaben für die Durchführung von Backup und Restore
- SA7.6: Schriftliche Vorgaben für die Konfiguration und Durchführung des Benutzermanagements
- SA7.7: Schriftliche Vorgaben für die Konfiguration und Durchführung der Systemüberwachung
- SA7.8: Führung von Aufzeichnungen über Betriebsvorkommnisse und durchgeführte Tätigkeiten am IT-System (Betriebsdokumentation)

11 Schutzthema ST8: Kryptografie

Bei der Speicherung von Daten (data at rest) und der vernetzten Kommunikation zwischen informationstechnischen Systemen (data at transit) sind diese Daten vor unzulässigem Zugriff zu schützen. Dies ist durch dem Stand der Technik entsprechende anwendungsspezifische kryptografische Verfahren sicherzustellen.

- SA8.1: Verschlüsselung von Datenspeichern mobiler Systeme
- SA8.2: Aufbau einer Kommunikationsverbindung ausschließlich mit den vorgesehenen Kommunikationspartnern
- SA8.3: Verschlüsselung von Kommunikationsverbindungen

12 Dokumentation

Zur nachvollziehbaren Dokumentation der Umsetzung der Schutzaspekte sowie zur Sicherstellung der Aufrechterhaltung der IT-Security bei späteren Änderungen sind für jedes IT-System in einem IT-Security-Handbuch die spezifizierten Standard-Sicherungsmaßnahmen sowie die zugrunde gelegten Randbedingungen aufzuführen und zu beschreiben.

In den systemspezifischen IT-Security-Handbüchern sind die zugrunde gelegten Randbedingungen sowie, gegliedert nach den Schutzthemen und -aspekten,

- die für das IT-System spezifischen Vorgaben,
- die Einstellungen und Konfigurationsparameter und
- die IT-Security relevante System- und Betriebsdokumentation

aufzuführen bzw. als Anhang beizufügen.

Die Randbedingungen, die bei der Festlegung der Sicherungsmaßnahmen berücksichtigt wurden, sind z. B. spezifische Gegebenheiten des IT-Systems selbst oder dessen Betriebsweise oder übergreifende Regelungen zur IT-Security.

Referenzen

[1] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium; Stand Februar 2020, ISBN (Print): 978-3-8462-0906-6

[2] Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit, Richtlinie für den Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter beim Umgang mit und bei der Beförderung von sonstigen radioaktiven Stoffen, Revision 1.0, 11.02.2020, VS-NfD