Neuerungen im IT-Grundschutz-Kompendium 2021

Delta-Präsentation

verinice.XP

Deniz Desti, Consultant

Deniz Desti

HiSolutions AG | Security Consulting

Fachliche Schwerpunkte

- Informationssicherheit & Datenschutz, GRC-Tools

Qualifikationen

- Zertifizierte IT-Grundschutz Praktikerin (HiSolutions AG)
- Zertifizierte Datenschutzbeauftragte (TÜV Süd)

Ausgewählte Projektreferenzen

- Softwareentwickler: Entwicklung und Unterstützung bei der Einführung einer individuellen Informationssicherheitsstrategie auf Basis des Reifegrads mit Hilfe von Best Practices und Standards zur Aufrechterhaltung der Sicherheit im Wandel der Digitalisierung
- IT-Dienstleister: Erstellung von diversen Datenschutzkonzepten nach DSGVO und BDSG als Voraussetzung zur Freigabe von Berlin-weiten Anwendungen für Bürger und Bürgerämter
- Öffentlicher Sektor: Erhebung des Reifegrads der Informationssicherheit und Erstellung eines übergreifenden Sicherheitskonzeptes, Migration von Basis-Sicherheitschecks in IT-Grundschutz Checks zur zeitlichen Optimierung

Agenda

1. Warum ins neue IT-Grundschutz-Kompendium 2021 migrieren?
2. Überblick und Vergleich mit Edition 2020
3. Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020
4. Änderungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020
5. Methoden zur schnellen, effizienten Migration in das neue IT-Grundschutz-Kompendium
6. Fragen

1. Warum ins neue IT-Grundschutz-Kompendium 2021 migrieren?

Warum ins neue IT-Grundschutz-Kompendium 2021 migrieren?

Schwerpunkte der Edition 2021: Entfernung von Redundanzen und Kumulation von gleichen Inhalten zu einem IT-Grundschutz Baustein oder einer Anforderung zur Aufwandsreduzierung; Erschließung neuer IT-Grundschutz Bausteine.

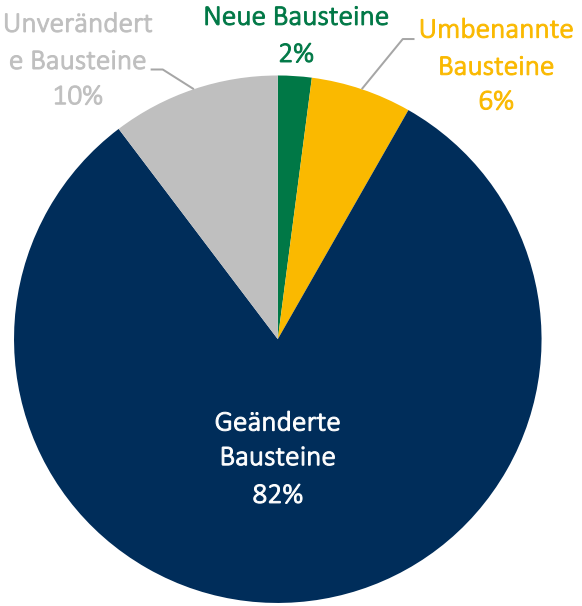
Das neue IT-Grundschutz-Kompendium ist seit dem 1. Februar 2021 veröffentlicht und zertifizierungsrelevant.

Edition 2020 des IT-Grundschutz-Kompendiums ist für aktuelle Zertifizierungsprozesse noch bis zum 30. September 2021 gültig.

2. Überblick und Vergleich mit Edition 2020

Was hat sich zur vorherigen Edition geändert?

- 97 IT-Grundschutz Bausteine insgesamt (+1)
- 2 davon sind neue IT-Grundschutz Bausteine
- 6 IT-Grundschutz Bausteine wurden umbenannt und überarbeitet (davon wurde einer aus 2 IT-Grundschutz Bausteinen zusammengefasst)
- 79 sind geänderte IT-Grundschutz Bausteine



Veränderte Bausteine: Klassifizierung der Änderungen

Umfangreiche Änderungen

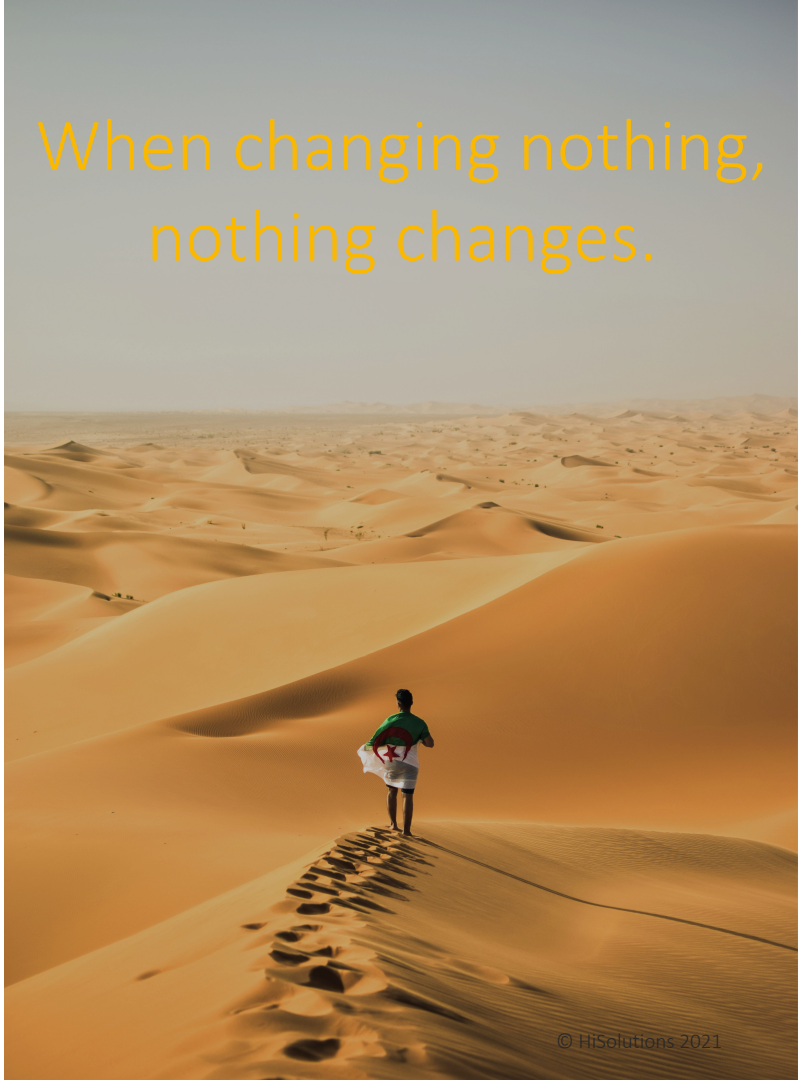
- Ggf. Auswirkungen auf Zertifizierungsverfahren oder bestehende Sicherheitskonzepte
- Im separaten Änderungsdokument aufgeführt
- Betrifft 85 Bausteine aus der Edition 2020

Geringfügige Änderungen

- Sprachliche und redaktionelle Änderungen
- Sind nicht in einem separaten Änderungsdokument aufgeführt
- Änderungsdatum in Fußzeilen dokumentiert
- Betrifft 10 Bausteine aus der Edition 2020

Nicht-überarbeitete oder geringfügig veränderte IT-Grundschutz Bausteine

- CON.2 Datenschutz
- OPS.1.2.2 Archivierung
- OPS.2.1 Outsourcing für Kunden
- OPS.3.1 Outsourcing für Dienstleister
- DER.2.2 Vorsorge für die IT-Forensik
- DER.4 Notfallmanagement
- IND.2.3 Sensoren und Aktoren
- IND.2.4 Maschine
- NET.4.3 Faxgeräte und Faxserver
- INF.6 Datenträgerarchiv



Neue Übersicht aller Prozess-Bausteine

ISMS
ISMS.1 Sicherheitsmanagement

ORP
ORP.1 Organisation
ORP.2 Personal
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
ORP.4 Identitäts- und Berechtigungsmanagement
ORP.5 Compliance Management

CON
CON.1 Kryptokonzept
CON.2 Datenschutz
CON.3 Datensicherungskonzept
CON.6 Löschen und Vernichten
CON.7 Informationssicherheit auf Auslandsreisen
CON.8 Software-Entwicklung
CON.9 Informationsaustausch
CON.10 Entwicklung von Webanwendungen

OPS
OPS.1.1.2 Ordnungsgemäße IT-Administration
OPS.1.1.3 Patch- und Änderungsmanagement
OPS.1.1.4 Schutz vor Schadprogrammen
OPS.1.1.5 Protokollierung
OPS.1.1.6 Software-Tests und -Freigaben
OPS.1.2.2 Archivierung
OPS.1.2.4 Telearbeit
OPS.1.2.5 Fernwartung
OPS.2.1 Outsourcing für Kunden
OPS.2.2 Cloud-Nutzung
OPS.3.1 Outsourcing für Dienstleister

DER
DER.1 Detektion von sicherheitsrelevanten Ereignissen
DER.2.1 Behandlung von Sicherheitsvorfällen
DER.2.2 Vorsorge für die IT-Forensik
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
DER.3.1 Audits und Revisionen
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision
DER.4 Notfallmanagement

Neue Übersicht aller System-Bausteine

APP

- APP.1.1 Office-Produkte
- APP.1.2 Web-Browser
- APP.1.4 Mobile Anwendungen
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory
- APP.2.3 OpenLDAP
- APP.3.1 Webanwendungen
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.4 Samba
- APP.3.6 DNS-Server
- APP.4.2 SAP-ERP-System
- APP.4.3 Relationale Datenbanksysteme
- APP.4.6 SAP ABAP-Programmierung
- APP.5.2 Microsoft Exchange und Outlook
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.6 Allgemeine Software
- APP.7 Entwicklung von Individualsoftware

IND

- IND.1 Prozessleit- und Automatisierungstechnik
- IND.2.1 Allgemeine ICS-Komponente
- IND.2.2 Speicherprogrammierbare Steuerung (SPS)
- IND.2.3 Sensoren und Aktoren
- IND.2.4 Maschine
- IND.2.7 Safety Instrumented Systems

INF

- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume
- INF.11 Allgemeines Fahrzeug
- INF.12 Verkabelung

Neue Übersicht aller System-Bausteine

NET
NET.1.1 Netzarchitektur und -design
NET.1.2 Netzmanagement
NET.2.1 WLAN-Betrieb
NET.2.2 WLAN-Nutzung
NET.3.1 Router und Switches
NET.3.2 Firewall
NET.3.3 VPN
NET.4.1 TK-Anlagen
NET.4.2 VoIP
NET.4.3 Faxgeräte und Faxserver

SYS	
SYS.1.1 Allgemeiner Server	SYS.3.2.4 Android
SYS.1.2.2 Windows Server 2012	SYS.3.3 Mobiltelefon
SYS.1.5 Virtualisierung	SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
SYS.1.7 IBM Z-System	SYS.4.3 Eingebettete Systeme
SYS.1.8 Speicherlösungen	SYS.4.4 Allgemeines IoT-Gerät
SYS.2.1 Allgemeiner Client	SYS.4.5 Wechseldatenträger
SYS.2.2.2 Clients unter Windows 8.1	
SYS.2.2.3 Clients unter Windows 10	
SYS.2.3 Clients unter Unix	
SYS.2.4 Clients unter macOS	
SYS.3.1 Laptops	
SYS.3.2.1 Allgemeine Smartphones und Tablets	
SYS.3.2.2 Mobile Device Management (MDM)	
SYS.3.2.3 iOS (for Enterprise)	

Umbenannte und überarbeitete Bausteine

Alte IT-Grundschutz Bausteine		Neue IT-Grundschutz Bausteine
ORP.3 Sensibilisierung und Schulung	=	ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
APP.5.1 Allgemeine Groupware	=	APP.5.3 Allgemeiner E-Mail-Client und –Server
CON.4 Auswahl und Einsatz von Standardsoftware	=	APP.6 Allgemeine Software
CON.5 Entwicklung und Einsatz von Individualsoftware	=	APP.7 Entwicklung von Individualsoftware
IND.1 Betriebs- und Steuerungstechnik	=	IND.1 Prozessleit- und Automatisierungstechnik
INF.3 Elektrotechnische Verkabelung	=	INF.12 Verkabelung
INF.4 IT-Verkabelung		

3. Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020

Überarbeitete Bausteine: Neue Rollen

Alte IT-Grundschutz Rolle		Neue IT-Grundschutz Rolle
Änderungsmanager	=	Fachverantwortlicher
Archivverwalter		
Ermittler		
Ermittlungsleiter		
Fax-Verantwortlicher		
TK-Anlagen-Verantwortlicher		
Beschaffer	=	Beschaffungsstelle
Leiter Beschaffung		

Überarbeitete Bausteine: Neue Rollen

Alte IT-Grundschutz Rolle		Neue IT-Grundschutz Rolle
Betriebsleiter	=	OT-Leiter
Leiter Produktion und Fertigung		
Innerer Dienst	=	Zentrale Verwaltung
Leiter Organisation		
Leitstellen-Operator	=	Mitarbeiter
Telearbeiter		

Überarbeitete Bausteine: Neue Rollen

Alte Rolle		Neue Rolle
Hersteller	*entfallen*	
ICS-Administrator	=	OT-Betrieb
Leiter Entwicklung	=	Entwickler
Leiter Haustechnik	=	Haustechnik
Leiter IT	=	IT-Betrieb
Leiter Netze	=	Planer
Leiter Personal	=	Personalabteilung
Pressestelle	=	Institutionsleitung
Verantwortlicher für die IS-Revision	=	Informationssicherheits-beauftragter (ISB)

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: INF.11 Allgemeines Fahrzeug

Anforderung	Maßnahme

INF.11.A1 Planung und Beschaffung [Fachverantwortliche, Beschaffungsstelle, Datenschutzbeauftragter] (B)	- Planung des Einsatzzweckes vor Beschaffung
	- Erhebung funktionaler Anforderungen an die Fahrzeuge und insbesondere die Anforderungen an die Informationssicherheit, sowie den Datenschutz der verbauten IT-Komponenten
	- Berücksichtigung folgender Aspekte:
	  - Einsatzszenarien der Fahrzeuge,
	  - nähere Einsatzumgebung der Fahrzeuge sowie
	  - der gesamte Lebenszyklus der Fahrzeuge.
	- Einsatz angemessener Schließsysteme, sofern nicht durchgehend durch andere Maßnahmen gesichert
	- Berücksichtigung, dass viele Fahrzeuge Daten an den Fahrzeughersteller und weitere Dritte übermitteln können.

INF.11.A2 Wartung, Inspektion und Updates [Fachverantwortliche, IT-Betrieb] (B)	- Wartung der Fahrzeuge und die dazugehörenden IT-Komponenten nach den Vorgaben des Herstellers - Berücksichtigung, dass Intervalle der herkömmlichen Wartung und von Updates der integrierten IT-Komponenten voneinander abweichen können - Klare Regelung darüber, wer in welcher Umgebung die Updates (auch „Over-the-Air“ (OTA) Updates) installieren darf - Durchführung von Wartungs- und Reparaturarbeiten von befugtem und qualifiziertem Personal - Regelungen zum Umgang mit Fremdfirmen - Prüfung, ob portable IT-Systeme entfernt werden sollten, wenn Fahrzeuge in fremden Institutionen gewartet werden - Bei Wiederintegration in den Einsatzbetrieb Prüfung mittels Checkliste, ob alle Beanstandungen und Mängel auch behoben wurden und die vorhandenen IT-Komponenten einsatzfähig sind.

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: INF.11 Allgemeines Fahrzeug

Anforderung	Maßnahme
INF.11.A3 Regelungen für die Fahrzeugbenutzung [IT-Betrieb, Fachverantwortliche, Benutzer, Datenschutzbeauftragter] (B)	- Regelung über Einsatz von Tätigkeiten, die sich auf die Sicherheit der in den Fahrzeugen verarbeiteten Informationen auswirken können, welche Informationen dabei transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind. - Dies muss für jede Art von Information gelten, auch für Gespräche in den Fahrzeugen. - Regelung in welchem Umfang Infotainmentsysteme, Anwendungen und sonstige Services der Fahrzeuge genutzt werden dürfen und wie Schnittstellen abzusichern sind. - Regelungen zum Umgang wie mitgeführte IT in den Fahrzeugen verwendet und aufbewahrt werden darf in den Geschäfts- bzw. Dienstanweisungen
INF.11.A4 Erstellung einer Sicherheitsrichtlinie [Fachverantwortliche, IT-Betrieb] (S)	- Dokumentation aller relevanter Sicherheitsanforderungen für die IT innerhalb der Fahrzeuge in einer für Mitarbeiter verpflichtenden Sicherheitsrichtlinie - Die Richtlinie sollte allen relevanten Mitarbeitern der Institution bekannt sein, die Grundlage für ihren Umgang mit Fahrzeugen darstellen, die Zuständigkeiten für einzelne Aufgaben klar regeln, regelmäßig überprüft und anlassbezogen aktualisiert werden.

INF.11.A5 Erstellung einer Inventarliste (S)	- Erstellung einer Inventarliste für jedes Fahrzeug über
	  - die im Fahrzeug fest verbauten oder zugehörigen IT-Komponenten (z. B. Handfunkgeräte),
	  - die Fachverfahren, die auf den integrierten IT-Komponenten ausgeführt werden,
	  - Handlungsanweisungen und Betriebsdokumentationen sowie
	  - die mit dem Infotainmentsystem gekoppelten Mobilgeräte geführt werden.
	- Die Inventarliste sollte regelmäßig und anlassbezogen aktualisiert werden.
	- Prüfung, ob noch alle inventarisierten IT-Komponenten vorhanden sind und keine mobilen Endgeräte unerlaubt mit dem Infotainmentsystem gekoppelt worden sind.

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: INF.11 Allgemeines Fahrzeug

Anforderung	Maßnahme

INF.11.A6 Festlegung von Handlungsanweisungen [Fachverantwortliche, Benutzer] (S)	- Handlungsanweisungen in Form von Checklisten für alle wesentlichen Situationen
	- Integration der Handlungsanweisungen in die Sicherheitsrichtlinie und als Checklisten, die zur Verfügung stehen sollen, während das Fahrzeug benutzt wird
	- Die Handlungsanweisungen sollten insbesondere nachfolgende Szenarien behandeln:
	  - Ausfall von IT-Komponenten der Fahrzeuge,
	  - Notfallsituationen wie Unfälle,
	  - unerlaubtes Betreten der Fahrzeuge sowie
	  - Diebstahl der Fahrzeuge oder darin abgelegter Gegenstände mit Relevanz für die Informationssicherheit.
	- Anhand der Checkliste sollte dokumentiert werden, wie sie in diesen Situation vorgegangen sind.
	- Dokumentation der Zuständigkeiten in der Checkliste

INF.11.A7 Sachgerechter Umgang mit Fahrzeugen und schützenswerten Informationen [Fachverantwortliche, Benutzer] (S)	- Die Institution sollte die Handlungsanweisungen zur Fahrzeugbenutzung um Aspekte ergänzen, wann, wie und wo Fahrzeuge sachgerecht abgestellt bzw. angedockt werden dürfen. - Regelung, welche Umgebungen die Fahrzeuge angemessenen vor unerlaubten Zutritt oder Sachbeschädigung schützen. - Regelung über Aufbewahrung von Informationen und IT-Systeme in den Fahrzeugen - Ausreichende Maßnahmen zum Zutrittsschutz; Sichere Verstauung der Fahrzeug Ladung - Sicherstellung, dass schützenswerte Informationen nicht von außerhalb der Fahrzeuge von Unbefugten eingesehen, mitgehört oder entwendet werden können. - Mitarbeiter sollen mit der grundlegenden Funktionsweise der Fahrzeuge und den betreffenden IT-Komponenten vertraut sein und über die bestehenden Sicherheitsrisiken informieren.

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: INF.11 Allgemeines Fahrzeug

Anforderung	Maßnahme
INF.11.A8 Schutz vor witterungsbedingten Einflüssen [Benutzer, Fachverantwortliche] (S)	- Schutz vor witterungsbedingten Einflüssen zusätzliche Schutzmaßnahmen je nach Fahrzeugart, Einsatzort und Einsatzumgebung - Für kurzfristig auftretende extreme Wettererscheinungen sollten entsprechende Schutzmaßnahmen getroffen werden. => Dokumentation in Handlungsanweisung
INF.11.A9 Sicherstellung der Versorgung [Fachverantwortliche] (S)	- Bevor Fahrzeuge eingesetzt werden, sollte geplant werden, wie diese mit Betriebsstoffen während des Einsatzes versorgt werden. Die Fahrzeuge sollten dabei während des Einsatzes immer ausreichend mit Betriebsstoffen versorgt werden
INF.11.A10 Aussonderung [IT-Betrieb, Fachverantwortliche] (S)	- Werden Fahrzeuge ausgesondert, sollten keine schützenswerten Informationen in den Fahrzeugen verbleiben. Bevor Fahrzeuge endgültig ausgesondert werden, sollte anhand der Inventarliste geprüft werden, ob keine inventarisierten Gegenstände und darüber hinaus relevante Gegenstände zurückgelassen worden sind.
INF.11.A11 Ersatzvorkehrungen bei Ausfällen [Fachverantwortliche] (H)	- Für den Fall, dass Fahrzeuge oder Fahrzeugführer ausfallen, sollten innerhalb der Institution vorbereitende Maßnahmen getroffen werden (z.B. Ersatzfahrzeuge und -fahrzeugführer oder Rahmenvertrag mit einer geeigneten Fremdinstitution) geschlossen werden.
INF.11.A12 Diebstahlsicherung bzw. Bewachung [Fachverantwortliche, Mitarbeiter] (H)	- Eine Alarmanlage und Wegfahrsperre muss vorhanden sein. Wird das Fahrzeug verlassen, sollten die Alarmanlage und Wegfahrsperre aktiviert werden. Alternativ sollten die Fahrzeuge bewacht werden
INF.11.A13 Schädigende Fremdeinwirkung [Fachverantwortliche] (H)	- Je nach Art der Fahrzeuge SOLLTEN geeignete Maßnahmen ergriffen werden, um die Fahrzeuge vor potentieller Fremdeinwirkung in der geplanten Einsatzumgebung zu schützen, wie z. B. störenden Funkstrahlen.

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: INF.11 Allgemeines Fahrzeug

Anforderung	Maßnahme
INF.11.A14 Schutz sensibler Informationen vor unbefugtem Zugriff und Kenntnisnahme [IT-Betrieb, Fachverantwortliche] (H)	- Schutz sensibler Informationen vor unbefugtem Zugriff und Kenntnisnahme - die vorhandenen Schutzvorkehrungen der Hersteller müssen überprüft und bei Bedarf angepasst werden.
INF.11.A15 Physische Absicherung der Schnittstellen [IT-Betrieb, Fachverantwortliche] (H)	- Alle physischen internen und externen Schnittstellen der Fahrzeuge sollten physisch gegen unbefugte Benutzung und äußere Einflüsse abgesichert werden.
INF.11.A16 Brandlöschanlage [Fachverantwortliche] (H)	- Brandlöschanlage muss verfügbar sein und einen Brand von außen und innen löschen können. Alternativ sollten geeignete Mittel zur Brandbekämpfung mitgeführt werden.

INF.11.A17 Netztrennung des In-Vehicle-Network mit einem Sonderfahrzeugnetz über Gateways (H)	- Generell sollte die Institution sicherstellen, dass keine Informationen unerlaubt und undefiniert
	- zwischen
	  - dem In-Vehicle-Network (IVN), das wiederum an die Netze der Fahrzeughersteller angebunden ist und
	  - den einsatzspezifischen IT-Komponenten ausgetauscht werden.
	- Hierzu sollten Gateways mit standardisierten Protokollen (z. B. nach Standard CiA 447) eingesetzt werden. Die Gateways sollten dabei vom Fahrzeughersteller freigegeben sein.

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: CON.10 Entwicklung von Webanwendungen

Anforderung	Maßnahme
CON.10.A1 Authentisierung bei Webanwendungen (B)	- Verwendung einer zentralen Authentisierungskomponente zur Authentisierung von Benutzern. - Bei Speicherung von Authentisierungsdaten auf einem Client muss der Benutzer explizit auf die Risiken der Funktion hingewiesen werden und zustimmen („Opt-In“) - Möglichkeit zur Festlegung von Grenzwerten für fehlgeschlagene Anmeldeversuche - Sofortige Information des Benutzers über zurückgesetztes Passwort
CON.10.A2 Zugriffkontrolle bei Webanwendungen (B)	- Zugriff nur über Berechtigungen - Jeder Zugriff auf geschützte Inhalte muss vor Ausführung kontrolliert werden - Bei fehlerhaften Zugriffskontrollen muss der Zugriff verweigert werden - Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen
CON.10.A3 Sicheres Session-Management (B)	- Angemessener Schutz und sichere Generierung von Session-IDs - Möglichkeit zur Beendung der bestehenden Sitzung - Implementierung einer maximalen Gültigkeitsdauer der Session-ID (Timeout) und Löschung der Sitzungsdaten
CON.10.A4 Kontrolliertes Einbinden von Inhalten bei Webanwendungen (B)	- Ausschließlich vorgesehene Daten und Inhalte einbinden und ausliefern - Einschränkung der Weiterleitungsfunktion => Benutzer dürfen ausschließlich auf vertrauenswürdige Webseiten weitergeleitet werden - Information des Benutzers über das Verlassen der Domäne

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: CON.10 Entwicklung von Webanwendungen

Anforderung	Maßnahme
CON.10.A5 Upload-Funktionen (B)	- Upload durch Benutzer nur im vorgegebenen Pfad - Benutzer dürfen Ablageort der Uploads nicht beeinflussen können - Integration von Funktionen, mit denen der Betreiber der Webanwendung die Uploads konfigurieren kann
CON.10.A6 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen (B)	- Sicherheitsmechanismen zum Schutz vor automatisierten Zugriffen - Berücksichtigung von Auswirkungen auf die Nutzungsmöglichkeiten berechtigter Benutzer
CON.10.A7 Schutz vertraulicher Daten (B)	- Übertragung vertraulicher Daten von Clients zu Servern nur mit der HTTP-Post-Methode - Direktiven gewährleisten, dass clientseitig keine schützenswerten Daten zwischengespeichert werden - Keine Anzeige von vertraulichen Formulardaten im Klartext angezeigt werden - Verhinderung von unerwarteter Speicherung vertraulicher Daten durch den Webbrowser - Serverseitiger Schutz sämtlicher Zugangsdaten der Webanwendung mit Hilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff (Salted Hash) - Schutz der Dateien mit Quelltexten der Webanwendung vor unerlaubten Abrufen

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: CON.10 Entwicklung von Webanwendungen

Anforderung	Maßnahme
CON.10.A8 Umfassende Eingabevalidierung und Ausgabekodierung (B)	- Behandlung sämtlicher übergebenen Daten an die Webanwendung als potenziell gefährlich und geeignete Filterung - Serverseitige Validierung sämtlicher Eingabedaten, Datenströme und Sekundärdaten, (z. B. Session-Ids) - Fehleingaben sollten möglichst nicht automatisch behandelt werden (Sanitizing). Lässt es sich jedoch nicht vermeiden, muss Sanitizing sicher umgesetzt werden. - Kodierung der Ausgabedaten, sodass schadhafter Code auf dem Zielsystem nicht interpretiert oder ausgeführt werden kann
CON.10.A9 Schutz vor SQL-Injection (B)	- Bei Weiterleitung von Daten an ein DBMS müssen Stored Procedures bzw. Prepared SQL Statements eingesetzt werden - Wenn weder Stored Procedures noch Prepared SQL Statements von der Einsatzumgebung unterstützt werden, müssen die SQL-Queries separat abgesichert werden
CON.10.A10 Restriktive Herausgabe sicherheitsrelevanter Informationen (B)	- Webseiten, Rückantworten und Fehlermeldungen von Webanwendungen dürfen keine Informationen enthalten, die Hinweise darauf geben, wie Sicherheitsmechanismen umgangen werden können

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: CON.10 Entwicklung von Webanwendungen

Anforderung	Maßnahme
CON.10.A11 Softwarearchitektur einer Webanwendung (S)	- Dokumentation der Softwarearchitektur mit allen Bestandteilen und Abhängigkeiten - Anpassung und Aktualisierung der Dokumentation bereits während des Entwicklungsverlaufs - Gestaltung der Dokumentation: muss in der Entwicklungsphase benutzt werden können und Entscheidungen nachvollziehbar sein, alle für den Betrieb notwendigen Komponenten gekennzeichnet werden, die nicht Bestandteil der Webanwendung sind, beschrieben sein, welche Komponenten welche Sicherheitsmechanismen umsetzen, wie die Webanwendung in eine bestehende Infrastruktur integriert wird und welche kryptographischen Funktionen und Verfahren eingesetzt werden.
CON.10.A12 Verifikation essenzieller Änderungen (S)	- Wichtige Einstellungen mit der die Anwendung geändert werden sollen, sollten durch die Eingabe eines Passworts erneut verifiziert werden. Falls nicht möglich, sollte die Webanwendung auf andere geeignete Weise sicherstellen, dass sich die Benutzer authentisieren - Information der Benutzer über Änderungen mit Hilfe von Kommunikationswegen außerhalb der Webanwendung
CON.10.A13 Fehlerbehandlung (S)	- Behandlung von Fehlern während der Laufzeit, sodass die Webanwendung weiter in einem konsistenten Zustand bleibt - Protokollierung von Fehlermeldungen - Veranlasste Aktionen, die einen Fehler verursachen, sollten abgebrochen werden - Verweigerung des Zugriffs auf angeforderte Ressourcen und Funktionen im Fehlerfall - Freigabe von zuvor reservierten Ressourcen SOLLTEN im Rahmen der Fehlerbehandlung - Der Fehler sollte möglichst von der Webanwendung selbst behandelt werden

Neuerungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: CON.10 Entwicklung von Webanwendungen

Anforderung	Maßnahme
CON.10.A14 Sichere HTTP-Konfiguration bei Webanwendungen (S)	- Zum Schutz vor Clickjacking, Cross-Site-Scripting und anderen Angriffen sollten geeignete HTTP-Response-Header gesetzt werden - Es sollten mindestens die folgenden HTTP-Header verwendet werden: Content-Security-Policy, Strict-Transport-Security, Content-Type, X-Content-Type-Options sowie Cache-Control. - Die verwendeten HTTP-Header sollten auf die Webanwendung abgestimmt werden. Die verwendeten HTTP-Header sollten so restriktiv wie möglich sein.
CON.10.A15 Verhinderung von Cross-Site-Request-Forgery (S)	- Implementierung von Sicherheitsmechanismen, die eine Unterscheidung zwischen beabsichtigten Seitenaufrufen des Benutzers von unbeabsichtigt weitergeleiteten Befehlen Dritter ermöglichen. - Dabei sollte mindestens geprüft werden, ob neben der Session-ID ein geheimes Token für den Zugriff auf geschützte Ressourcen und Funktionen benötigt wird.
CON.10.A16 Mehr- Faktor- Authentisierung (S)	- Implementierung einer Mehr-Faktor-Authentisierung
CON.10.A17 Verhinderung der Blockade von Ressourcen (H)	- Vermeidung ressourcenintensiver Operationen zum Schutz vor Denial-of-Service (DoS)-Angriffen - Besondere Absicherung ressourcenintensiverer Operationen - Überwachung und Verhinderung eines möglichen Überlaufs von Protokollierungsdaten
CON.10.A18 Kryptografische Absicherung vertraulicher Daten (H)	- Schutz vertraulicher Daten durch sichere, kryptographische Algorithmen

4. Änderungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020

Änderungen im IT-Grundschutz-Kompendium 2021 im Vergleich zu 2020: ORP.1 Organisation

Neue Anforderungen:

- ORP.1.A15 Ansprechpartner zu Sicherheitsfragen (Basis-Anforderung) (vorher ORP.3.A2)
- ORP.1.A16 Mitarbeiterrichtlinie zur sicheren IT-Nutzung (Standard-Anforderung) (vorher SYS.2.1.A25)

Änderungen an den bestehenden Anforderungen:

- ORP.1.A2 Zuweisung der Verantwortung: Die Anforderung wurde umbenannt in Zuweisung der Zuständigkeiten.
- ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen: Die Anforderung wurde um den Aspekt der Beaufsichtigung von Fremdpersonen in sensiblen Sicherheitsbereichen ergänzt.
- ORP.1.A8 Betriebsmittel- und Geräteverwaltung: Die Anforderung wurde um die Aspekte der früheren Anforderung ORP.1.A7 Geräteverwaltung erweitert.
- ORP.1.A16 Richtlinie zur sicheren IT-Nutzung: Die zeitliche Vorgabe für die Aktualisierung der Richtlinie wurde auf "regelmäßig" angepasst.

- Nur in diesen Baustein verschoben
- Tatsächlich neue Anforderung

Änderungen an den Bausteinen der Edition 2020: ORP.2 Personal

Neue Anforderungen:

- ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern (B)
- ORP.2.A15 Qualifikation des Personals (B)

Änderungen an den bestehenden Anforderungen:

- ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern: Die Anforderung wurde um den Aspekt des Führens einer Checkliste erweitert.
- ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal: Die Anforderung wurde um den Aspekt der schriftlichen Form ergänzt.
- ORP.2.A13 Sicherheitsüberprüfung: Die Anforderung wurde um den Aspekt erweitert, Mitarbeiter beim Arbeiten mit Verschlusssachen einer Überprüfung nach SÜG zu unterziehen.

- Nur in diesen Baustein verschoben
- Tatsächlich neue Anforderung

Änderungen an den Bausteinen der Edition 2020: ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

Änderungen an den bestehenden Anforderungen:

- ORP.3.A4 Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit: Die Anforderung wurde umbenannt in Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit. Sie wurde um den Aspekt, dass Informationen und Fähigkeiten den Mitarbeitern innerhalb des Schulungsprogramm vermittelt werden verschärft aus der Anforderung ORP.3.A6 Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit. Die Anforderung umfasst nun auch zusätzliche Anforderungen an die Planung eines Schulungsprogramms aus der entfallenen ORP.3.A5 Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme.
- ORP.3.A6 Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit: Die Anforderung wurde umbenannt in Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit.
- ORP.3.A8 Messung und Auswertung des Lernerfolgs: Die Anforderung wurde um den regelmäßigen Austausch des ISB mit der Personalabteilung erweitert.

Änderungen an den Bausteinen der Edition 2020: ORP.4 Identitäts- und Berechtigungsmanagement

Neue Anforderungen:

- ORP.4.A24 Vier-Augen-Prinzip für administrative Tätigkeiten (analog zu OPS.1.1.2.A17)

Änderungen an den bestehenden Anforderungen:

- ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen: Ergänzung der Teilaspekte eindeutige Zuordnung und Deaktivieren bei Inaktivität sowie Umgang mit nicht benötigten Benutzerkennungen.
- ORP.4.A2 Umbenennung zu „Einrichtung, Änderung und Entzug von Berechtigungen“ und Ergänzung des Teilaspekts Systemverzeichnisse und -dateien sowie Schärfung in Bezug auf die Vergabe von Berechtigungen (Erforderlichkeitsprinzip).
- ORP.4.A3 Dokumentation der Benutzerkennungen und Rechteprofile: Schärfung des Teilaspekts Dokumentation und Prüfung der Benutzerkennungen und Rechteprofile.
- ORP.4.A8 Regelung des Passwortgebrauchs: Ergänzung des Teilaspekts zu Passwort-Managern mit Online-Funktionen.
- ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme: Ergänzung des Teilaspekts zu Passwortwechseln bei technischen Benutzern.
- ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen: Schärfung in Bezug auf die Übertragung von Authentisierungsinformationen.

Änderungen an den Bausteinen der Edition 2020: ORP.4 Identitäts- und Berechtigungsmanagement

Änderungen an den bestehenden Anforderungen:

- ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen: Ergänzung der Teilanforderung zum Verhalten bei erfolglosen Authentisierungsversuchen.
- ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle: Die Teilanforderungen zur Dokumentation aller eingerichteten Benutzer und Rechte sowie zu Zugriffsrechten wurden entfernt, da diese bereits durch die Anforderungen ORP.4.A3 Dokumentation der Benutzerkennungen und Rechteprofile und ORP.4.A9 Identifikation und Authentisierung abgedeckt ist.

Änderungen an den Bausteinen der Edition 2020: ORP.5 Compliance Management (Anforderungsmanagement)

Änderungen an den bestehenden Anforderungen:

- ORP.5.A1 Identifikation der Rahmenbedingungen: Schärfung des Titels. Schärfung auf gesetzliche, vertragliche und sonstige Vorgaben.
- ORP.5.A2 Beachtung der Rahmenbedingungen: Schärfung des Titels, Schärfung auf gesetzliche, vertragliche und sonstige Vorgaben. Der Aspekt der Beachtung wurde in die Anforderung ORP.5.A2 Beachtung der Rahmenbedingungen verschoben.
- ORP.5.A4 Konzeption und Organisation des Compliance Managements: Aspekt des Aufbaus eines Prozesses aus der Basis-Anforderung übernommen.
- ORP.5.A5 Ausnahmegenehmigungen: Sprachliche Schärfung des Aspekts der Ausnahmen in Einzelfällen.

Änderungen an den Bausteinen der Edition 2020: CON.1 Kryptokonzept

Änderungen an den bestehenden Anforderungen:

- CON.1.A4 Geeignetes Schlüsselmanagement: Anforderungen zum sicheren Schlüsselaustausch ergänzt.

Änderungen an den Bausteinen der Edition 2020: CON.3 Datensicherungskonzept

Änderungen an den bestehenden Anforderungen:

- CON.3.A2 Festlegung der Verfahrensweise für die Datensicherung: Ergänzung, dass geprüft werden muss, ob in virtuellen Umgebungen eine Sicherung durch Snapshots möglich ist.
- CON.3.A12 Geeignete Aufbewahrung der Backup-Datenträger: Umbenannt in Geeignete Aufbewahrung der Datenträger von Datensicherungen zur einheitlichen Verwendung des Begriffs Datensicherung.

Änderungen an den Bausteinen der Edition 2020: CON.6 Löschen und Vernichten

Neue Anforderungen:

- CON.6.A12 Mindestanforderungen an Verfahren zur Löschung und Vernichtung: Neue Anforderungen an konkrete Verfahren zum Löschen und Vernichten.
- CON.6.A13 Vernichtung digitaler Datenträger bei fehlender Möglichkeit zur sicheren Löschung: Neue Anforderung zur Behandlung von defekten Datenträgern.
- CON.6.A14 Vernichten von Datenträgern auf erhöhter Sicherheitsstufe: Neue Anforderung zur Regelung der Vernichtung von Datenträgern.

Änderungen an den bestehenden Anforderungen:

- CON.6.A1 Regelung für die Löschung und Vernichtung von Informationen: Neuformulierung der Anforderung mit Ergänzung von rechtlichen Aspekten.
- CON.6.A2 Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen: Anpassung der Anforderung an die neuen Mindestanforderungen an die Verfahren zum sicheren Löschen und Vernichten. Verschiebung der Aspekte zu externen Dienstleistern in CON.6.A11 Löschung und Vernichtung von Datenträgern durch externe Dienstleister. Ergänzung des Bezugs zur Entsorgung.

Änderungen an den Bausteinen der Edition 2020: CON.6 Löschen und Vernichten

Änderungen an den bestehenden Anforderungen:

- CON.6.A11 Löschung und Vernichtung von Datenträgern durch externe Dienstleister: Bündelung aller relevanten Aspekte zur Einbindung externer Dienstleister in dieser Anforderung und Verschiebung in eine Basis-Anforderung, da die Einbindungen von externen Dienstleistern immer berücksichtigt werden muss, sofern von diesen ein Löschen oder Vernichten durchgeführt wird.
- CON.6.A4 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern: Anpassung an die neue Anforderung CON.6.A12 Mindestanforderungen an Verfahren zur Löschung und Vernichtung

Änderungen an den Bausteinen der Edition 2020: CON.7 Informationssicherheit auf Auslandsreisen

Umsortierung der bestehenden Anforderungen:

- CON.7.A11 Einsatz von Diebstahl-Sicherungen: Die Anforderung wurde in eine Standard-Anforderung überführt, da keine MUSS-Anforderungen gestellt werden.

Änderungen an den Bausteinen der Edition 2020: CON.8 Software-Entwicklung

Neue Anforderungen:

- CON.8.A21 Bedrohungsmodellierung: Ergänzung der Bedrohungsmodellierung.
- CON.8.A22 Sicherer Software-Entwurf: Ergänzung des sicheren Software-Entwurfs.

Änderungen an den bestehenden Anforderungen:

- CON.8.A1 Definition von Rollen und Verantwortlichkeiten: Umbenennung in Definition von Rollen und Zuständigkeiten und Ergänzung von konkreten fachlichen Themen, die von den Rollen abgedeckt werden sollten. Verschiebung der Anforderung zu Standard-Anforderung, da diese nicht inhaltlich priorisiert im Rahmen der Basis-Absicherung durchgeführt werden muss.
- CON.8.A5 Sicheres Systemdesign: Ergänzung weiterer sicherheitsrelevanter Vorgaben.
- CON.8.A6 Anpassung des Titel in „Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen“, um zu schärfen, dass die Anforderung nur bei externen Bibliotheken anzuwenden ist.
- CON.8.A7 Umbenennung in „Durchführung von entwicklungsbegleitenden Softwaretests“ zur besseren Abgrenzung zu Softwaretests im Rahmen der Abnahme. Ergänzung hinsichtlich der Trennung unterschiedlicher Umgebungen. Die automatische statische Code-Analyse wurde von einer MUSS zu einer SOLLTE-Anforderung.

Änderungen an den Bausteinen der Edition 2020: CON.8 Software-Entwicklung

Änderungen an den bestehenden Anforderungen:

- CON.8.A8 Bereitstellung von Patches, Updates und Änderungen: Entfernung der Teilanforderung hinsichtlich des Einspielens durch den IT-Betrieb, da dies nicht zu dem Geltungsbereich des vorliegenden Bausteins gehört.
- CON.8.A12 Ausführliche Dokumentation: Ergänzung um die Bedrohungsmodellierung, Software-Architektur und Berücksichtigung im Vorgehensmodell.
- CON.8.A14 Schulung des Projektteams zur Informationssicherheit: Ergänzung um konkrete Schulungsinhalte.
- CON.8.A20 Überprüfung von externen Komponenten: Präzisierung der Anforderung und Ergänzung von Aspekten zur Integritätsprüfung.

Änderungen an den Bausteinen der Edition 2020: CON.9 Informationsaustausch

Neue Anforderungen:

- CON.9.A9 Vertraulichkeitsvereinbarungen: Neue Anforderung für den erhöhten Schutzbedarf zum Abschließen von Vertraulichkeitsvereinbarungen.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.2 Ordnungsgemäße IT-Administration

Neue Anforderungen:

- OPS.1.1.2.A20 Verwaltung und Inbetriebnahme von Geräten: Diese Anforderung wurde in diesen Baustein verschoben aus Baustein ORP.1 Organisation, Anforderung ORP.1.A7 Geräteverwaltung.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.2 Ordnungsgemäße IT-Administration

Änderungen an den bestehenden Anforderungen:

- OPS.1.1.2.A10 Fortbildung und Information: Ergänzung von Anwendungen in der Aufzählung zu den Themen, über die sich Administratoren regelmäßig informieren sollten.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.3 Patch- und Änderungsmanagement

Neue Anforderungen:

- OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software: Neue Basisanforderung im Zuge der Konsolidierung. Regelmäßige Bewertung und Implementierung von Sicherheitskorrekturen.
- OPS.1.1.3.A16 Regelmäßige Suche nach Informationen zu Patches und Schwachstellen: Neue Basisanforderung im Zuge der Konsolidierung. Regelmäßiges Suchen nach Informationen über Patches

Änderungen an den bestehenden Anforderungen:

- OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement: Formulierung geschärft und Klassifizierung/Bewertung der Patches und verschoben.
- OPS.1.1.3.A2 Festlegung der Zuständigkeiten: Die Rolle Änderungsmanager wurde durch den Fachverantwortlichen für das Patch- und Änderungsmanagement ersetzt. Im Zuge der klareren Trennung hat eine begriffliche Schärfung stattgefunden.
- OPS.1.1.3.A5 Umgang mit Änderungsanforderungen: Anforderung stärker auf die Aspekte der Informationssicherheit ausgerichtet, da diese explizit das Änderungsmanagement betrifft.
- OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen: Anforderung stärker auf die Aspekte der Informationssicherheit ausgerichtet, da diese explizit das Änderungsmanagement betrifft.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.3 Patch- und Änderungsmanagement

Änderungen an den bestehenden Anforderungen:

- OPS.1.1.3.A9 Test- und Abnahmeverfahren für und neue Hardware: Test- und Freigabeverfahren für Software und Patches sind in dem Baustein OPS.1.1.6 Software-Tests und -Freigaben behandelt. Daher behandelt diese Anforderung nur noch neue Hardware. Titel und Anforderung sind entsprechend angepasst.
- OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen: Bezug aus vertrauenswürdiger Quelle wurde ergänzt. Die Anforderung wurde um den Aspekt Installation erweitert.
- OPS.1.1.3.A12 Einsatz von Werkzeugen beim Änderungsmanagement: Die Formulierung wurde generalisiert und der Titel entsprechend angepasst.
- OPS.1.1.3.A13 Erfolgsmessung von Änderungsanforderungen: Die Rolle Änderungsmanager wurde durch den Fachverantwortlichen für das Patch- und Änderungsmanagement ersetzt.
- OPS.1.1.3.A14 Synchronisierung innerhalb des Änderungsmanagements: Die Formulierung wurde geschärft.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.4 Schutz vor Schadprogrammen

Änderungen an den bestehenden Anforderungen:

- OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen: Wenn Schutzmechanismen nicht genutzt werden, MUSS dies nun begründet dokumentiert werden.
- OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes für Endgeräte: Verallgemeinerung, um die Anforderung OPS.1.1.4.A4 Auswahl eines Virenschutzprogrammes für Gateways und IT-Systeme zum Datenaustausch mit abzudecken.
- OPS.1.1.4.A5 Betrieb und Konfiguration von Virenschutzprogrammen: Sprachliche Anpassungen, "transparent" durch "nachvollziehbar" dokumentiert ersetzt. Ergänzung um Teilanforderung: Deaktivierung durch die Benutzer.
- OPS.1.1.4.A7 Sensibilisierung und Verpflichtung der Benutzer: Die Anforderung wurde um Aspekte zur Meldung von Verdachtsfällen aus OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen erweitert.
- OPS:1.1.4.A9 Meldung von Infektionen mit Schadprogrammen: Der Absatz zur Meldung von Verdachtsfällen durch den Benutzer wurde verschoben.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.5 Protokollierung

Änderungen an den bestehenden Anforderungen:

- OPS.1.1.5.A6 Aufbau einer zentralen Protokollierungsinfrastruktur: Der zweite Absatz (Pull-Prinzip) wurde komplett gestrichen. Der Aspekt restriktive Auslegung von Kommunikationsverbindungen ist bereits durch die Anforderung NET.3.2.A2 Festlegen der Firewall-Regeln im Baustein NET.3.2 Firewall abgedeckt.
- OPS.1.1.5.A8 Archivierung von Protokollierungsdaten: Diese Anforderung wurde abgeschwächt. Die Protokollierungsdaten sollten archiviert werden, hierfür ist im vorliegenden Baustein jedoch kein Konzept erforderlich.
- OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten: Diese Anforderung wurde grundlegend überarbeitet.
- OPS.1.1.5.A13 Hochverfügbare Protokollierungssysteme: Sprachliche Anpassung des Anforderungstitels.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.6 Software-Tests und -Freigaben

Neue Anforderungen:

- OPS.1.1.6.A15 Überprüfung der Installation und zugehörigen Dokumentation (S)
- OPS.1.1.6.A16 Sicherheitsüberprüfung der Tester (H)

Änderungen an bereits bestehenden Anforderungen:

- OPS.1.1.6.A1 Planung der Software-Tests: Es wurde ergänzt, dass die Testumgebung die zukünftige Produktivumgebung möglich repräsentativ und vollständig widerspiegeln muss.
- OPS.1.1.6.A5 Durchführung von Software-Tests für nicht funktionale Anforderungen: Anpassung des Titels, um klarer herauszustellen, das Tests nichtfunktionaler Anforderungen gemeint sind.
- OPS.1.1.6.A7 Personalauswahl der Software-Tester: Anpassung, sodass klarer zwischen den Anforderungen bei Tests von Individualsoftware und standardisierter Software differenziert wird. Entfernung der Teilanforderung, dass Personal für jegliche öffentliche Einrichtungen sicherheitsüberprüft sein muss.
- OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten: Verschiebung der Anforderung zu den Basis-Anforderungen und vollständige Neuformulierung, um klarer herauszustellen, wann anonymisiert werden muss.

Änderungen an den Bausteinen der Edition 2020: OPS.1.1.6 Software-Tests und -Freigaben

Änderungen an bereits bestehenden Anforderungen:

- OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung: Anpassung des Titels zur Vereinfachung der Sprache. Die Aspekte hinsichtlich der repräsentativen Abdeckung der Produktivumgebung durch die Test-Umgebung wurden in OPS.1.1.6.A1 Planung der Software-Test verschoben.

Änderungen an den Bausteinen der Edition 2020: OPS.1.2.4 Telearbeit

Neue Anforderungen:

- OPS.1.2.5.A25 Entkopplung der Netzmanagement-Kommunikation bei der Fernwartung (S) (analog zu NET.1.2.A21)
- Änderungen an bereits bestehenden Anforderungen:
- OPS.1.2.5.A3 Absicherung der Schnittstellen zur Fernwartung: Anforderung geschärft, Fernwartungsverbindungen über nicht vertrauenswürdige Netze müssen verschlüsselt werden.
- OPS.1.2.5.A14 Dedizierte IT-Systeme bei der Fernwartung: Anforderung umbenannt in Dedizierte Clients bei der Fernwartung.

Änderungen an den Bausteinen der Edition 2020: OPS.2.2 Cloud-Nutzung

Änderungen an bereits bestehenden Anforderungen:

- OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie: Sprachliche Anpassung des Anforderungstitels.

Änderungen an den Bausteinen der Edition 2020: DER.1 Detektion von sicherheitsrelevanten Ereignissen

Änderungen an bereits bestehenden Anforderungen:

- DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten: Die Anforderung wurde um den Aspekt Schadcode in Protokoll-Einträgen erweitert.
- DER.1.A9 Einsatz zusätzlicher Detektionssysteme: Die Anforderung wurde um die Festlegung von zu schützenden Segmenten (DER.1.A8 Festlegung von zu schützenden Segmenten) ergänzt.

Änderungen an den Bausteinen der Edition 2020: DER.2.1 Behandlung von Sicherheitsvorfällen

Änderungen an bereits bestehenden Anforderungen:

- DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen: Der Aspekt externe Dienstleister wurde gestrichen, weil dieser im vorliegenden Baustein nicht relevant ist.
- DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen: Die Anforderung wurde um den Aspekt der Anpassung erweitert: "Bei Bedarf SOLLTE die Vorgehensweise angepasst werden."
- DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement: Die erste Teilanforderung “Als Teil des Sicherheitsmanagements SOLLTE die Behandlung von Sicherheitsvorfällen in der Sicherheitsleitlinie bzw. im Sicherheitskonzept der Institution geregelt werden.” wurde gestrichen.
- DER.2.1.A15 Schulung der Mitarbeiter der zentralen Anlaufstelle des IT-Betriebs zur Behandlung von Sicherheitsvorfällen: Die letzte Teilanforderung “Die Checklisten des Service Desk SOLLTEN auch Fragen enthalten, um Sicherheitsvorfälle identifizieren zu können.” wurde gestrichen, weil sie zu sehr in die Umsetzung hineingreift.
- DER.2.1.A22 Überprüfung der Effizienz des Managementsystems zur Behandlung von Sicherheitsvorfällen: Geringfügige Anpassung des Anforderungstitels.

Änderungen an den Bausteinen der Edition 2020: APP.1.1 Office-Produkte

Neue Anforderungen:

- APP.1.1.A17 Sensibilisierung zu spezifischen Office-Eigenschaften: Neue Anforderung zu spezifischen Sensibilisierungsinhalten.

Änderungen an den bestehenden Anforderungen:

- APP.1.1.A6 Testen neuer Versionen von Office-Produkten: Offenere Formulierung für den Umgang mit Arbeitsmitteln bei Inkompatibilität.
- APP.1.1.A10 Regelung der Software-Entwicklung durch Endbenutzer: Verantwortlichkeiten durch Zuständigkeiten ersetzt und sprachlich geschärft.
- APP.1.1.A11 Geregelter Einsatz von Erweiterungen für Office-Produkte: Sprachlich geschärft.
- APP.1.1.A12 Verzicht auf Cloud-Speicherung: Beispiele entfernt und sprachlich geschärft.
- APP.1.1.A13 Verwendung von Viewer-Funktionen: Beispiele entfernt und sprachlich geschärft.

Änderungen an den Bausteinen der Edition 2020: APP.1.1 Office-Produkte

Änderungen an bestehenden Anforderungen:

- APP.1.1.A14 Schutz gegen nachträgliche Veränderungen von Dokumenten: Schulungsaspekte entfernt. Zusätzlich sprachlich geschärft.
- APP.1.1.A16 Integritätsprüfung von Dokumenten: Verfahren verallgemeinert und Anforderung sprachlich geschärft.

Änderungen an den Bausteinen der Edition 2020: APP.1.2 Webbrowser

Neue Anforderungen:

- APP.1.2.A13 Nutzung von DNS-over-HTTPS: Neue Basisanforderung zur Nutzung von DoH.

Änderungen an den bestehenden Anforderungen:

- APP.1.2.A1 Verwendung von Sandboxing: Anforderung umbenannt in Verwendung von grundlegenden Sicherheitsmechanismen. Weitere Sicherheitsmechanismen ergänzt.
- APP.1.2.A2 Unterstützung sicherer Verschlüsselung der Kommunikation: HSTS-Preload-Liste aus Anforderung entfernt.
- APP.1.2.A3 Verwendung von vertrauenswürdigen Zertifikaten: Anforderung zum Umgang mit mitgelieferten Wurzelzertifikaten geschärft.
- APP.1.2.A7 Datensparsamkeit in Webbrowsern: Anforderung im Bezug

Änderungen an den Bausteinen der Edition 2020: APP.1.2 Webbrowser

Umsortierung von Anforderungen:

- APP.1.2.A6 Kennwortmanagement im Webbrowser: Anforderung nach Basis verschoben.

Änderungen an den Bausteinen der Edition 2020: APP.1.4 Mobile Anwendungen

Neue Anforderungen:

- APP.1.4.A16: Mobile Application Management

Umsortierung von Anforderungen:

- APP.1.4.A3 Verteilung schutzbedürftiger Apps: Die Anforderung wurde in eine Standard-Anforderung überführt (vorher Basis-Anforderung), da nach der Entfernung von Redundanzen nur noch eine SOLLTE-Anforderung erhalten blieb.

Änderungen an den Bausteinen der Edition 2020: APP.2.1. Allgemeiner Verzeichnisdienst

Änderungen an den bestehenden Anforderungen:

- APP.2.1.A6 Sicherer Betrieb von Verzeichnisdiensten: Anforderung um Teilanforderung zur Absicherung der Arbeitsplätze von Administratoren erweitert, die ursprünglich aus dem nachgeordneten Baustein APP.2.2 Active Directory stammt (APP.2.2.A7 Umsetzung sicherer Verwaltungsmethoden für Active Directory).
- APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten: Erweiterung der Anforderung um generelle Anforderungen an die Verschlüsselung des Netzwerkverkehrs und die Erreichbarkeit des Servers aus dem Internet.

Änderungen an den Bausteinen der Edition 2020: APP.2.3 OpenLDAP

Änderungen an den bestehenden Anforderungen:

- APP.2.3.A4 Konfiguration der durch OpenLDAP verwendeten Datenbank: BerkeleyDB in Datenbank allgemein geändert.

Änderungen an den Bausteinen der Edition 2020: APP.3.1 Webanwendungen

Änderungen an den bestehenden Anforderungen:

- APP.3.1.A1 Authentisierung bei Webanwendungen: Entfernung aller entwicklungsspezifischen Aspekte. Das Thema wird nun im neuen Baustein CON.10 Entwicklung von Webanwendungen behandelt.
- APP.3.1.A4 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen: Entfernung aller entwicklungsspezifischen Aspekte.
- APP.3.1.A7 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen: Entfernung aller entwicklungsspezifischen Aspekte.
- APP.3.1.A8 Systemarchitektur einer Webanwendung: Entfernung aller entwicklungsspezifischen Aspekte. Entfernung von Aspekten, die den Webserver betreffen.
- APP.3.1.A9 umbenannt in „Beschaffung von Webanwendungen“: Entfernung aller entwicklungsspezifischen Aspekte.
- APP.3.1.A11 Sichere Anbindung von Hintergrundsystemen: Aspekte entfernt, die nicht direkt auf Webanwendungen bezogen sind.
- APP.3.1.A12 Sichere Konfiguration von Webanwendungen: Ergänzung sicherheitsrelevanter Konfigurationsaspekte.
- APP.3.1.A14 Schutz vertraulicher Daten: Entfernung aller entwicklungsspezifischen Aspekte.
- APP.3.1.A22 Überprüfung von Webanwendungen: Anforderung umbenannt in Penetrationstest und Revision.

Änderungen an den Bausteinen der Edition 2020: APP.3.2 Webserver

Änderungen an bestehenden Anforderungen:

- APP.3.2.A1 Sichere Konfiguration eines Webservers: Anforderungen an Diensttrennung pro Server ergänzt.
- APP.3.2.A2 Schutz der Webserver-Dateien: Redundante Anforderung zum Abschalten nicht benötigter Funktionen und zu Zugriffsrechten entfernt. Der IT-Betrieb muss nun regelmäßig überprüfen, ob vertrauliche Daten in öffentlichen Verzeichnissen gespeichert wurden.
- APP.3.2.A8 Planung des Einsatzes eines Webservers: Anforderung spezifiziert und zu APP.6.A1 Planung des Software-Einsatzes abgegrenzt.

Änderungen an den Bausteinen der Edition 2020: APP.3.3 Fileserver

Änderungen an bestehenden Anforderungen:

- APP.3.3.A13 Replizieren zwischen Standorten: Diese Anforderung wurde in Replikation zwischen Standorten umbenannt.

Änderungen an den Bausteinen der Edition 2020: APP.3.4 Samba

Änderungen an bestehenden Anforderungen:

- APP.3.4.A1 Planung des Einsatzes eines Samba-Servers: Die Umsetzung SOLLTE nun dokumentiert werden, außerdem wurde die Rolle des IT-Betriebs hervorgehoben.
- APP.3.4.A3 in „Sichere Konfiguration eines Samba-Servers“ umbenannt. Der Aspekt zu Kerberos wurde verschoben. Die Vorgaben dieser Anforderung zu Netports wurden hier entfernt.
- APP.3.4.A9 Sichere Konfiguration von Kerberos unter Samba: Der Aspekt zu Kerberos wurde aus APP.3.4.A3 Sichere Konfiguration des Samba-Servers übernommen.

Änderungen an den Bausteinen der Edition 2020: APP.3.6 DNS-Server

Änderungen an bestehenden Anforderungen:

- APP.3.6.A7 Überwachung von DNS-Servern: Die Teilanforderung zur Protokollierung wurde anhand von entsprechenden sicherheitsrelevanten Ereignissen konkretisiert.
- APP.3.6.A10 Auswahl eines geeigneten DNS-Server-Produktes: Die erste Teilanforderung wurde gestrichen, da zu generisch.
- APP.3.6.A15 Auswertung der Logdaten: Die Teilanforderung zur Auswertung von Protokollierungsdaten wurde anhand von entsprechenden sicherheitsrelevanten Ereignissen konkretisiert.

Änderungen an den Bausteinen der Edition 2020: APP.4.3 Relationale Datenbanken

Änderungen an bestehenden Anforderungen:

- APP.4.3.A1 Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme: Die im Bereich der Datenbank "verantwortlichen" Mitarbeiter wurden in die "zuständigen" Mitarbeiter geändert.
- APP.4.3.A3 Basishärtung des Datenbankmanagementsystems: Anforderungen zu Passwörtern entfernt, die bereits aus ORP.4.A8 Regelung des Passwortgebrauchs hervorgehen.
- APP.4.3.A18 Überwachung des Datenbankmanagementsystems: Aufnahme der Betriebszustände aus dem ersten Anforderungssatz in die restliche Anforderung. Außerdem SOLLTEN die zuständigen Mitarbeiter nun alarmiert werden (statt MÜSSEN).
- APP.4.3.A20 Regelmäßige Audits: Aufteilung einzelner Anforderungssätze in zwei Einzelsätze ohne Inhaltsänderung.
- APP.4.3.A22 Notfallvorsorge: Aufteilung einzelner Anforderungssätze in zwei Einzelsätze ohne Inhaltsänderung.

Änderungen an den Bausteinen der Edition 2020: APP.5.2 Microsoft Exchange und Outlook

Änderungen an bestehenden Anforderungen:

- APP.5.2.A10 Sichere Konfiguration von Outlook: Anforderung zum automatischen Öffnen von Anhängen entfernt, da diese nicht spezifisch für Outlook und allgemeingültig durch APP.5.3.A1 Sichere Konfiguration der E-Mail-Clients abgedeckt ist.

Änderungen an den Bausteinen der Edition 2020: APP.7 Entwicklung von Individualsoftware

Neue Anforderungen:

- APP.7.A1 Erweiterung der Planung des Software-Einsatzes um Aspekte von Individual-Software.
- APP.7.A2 Festlegung von Sicherheitsanforderungen an den Prozess der Software-Entwicklung.
- APP.7.A3 Festlegung der Sicherheitsfunktionen zur System-Integration.
- APP.7.A4 Anforderungsgerechte Beauftragung.
- APP.7.A7 Sichere Beschaffung von Individualsoftware.
- APP.7.A8 Frühzeitige Beteiligung des Fachverantwortlichen bei entwicklungsbegleitenden Software-Tests.
- APP.7.A10 Beauftragung zertifizierter Software-Entwicklungsunternehmen.

Änderungen an den Bausteinen der Edition 2020: APP.7 Entwicklung von Individualsoftware

Änderungen an bestehenden Anforderungen:

- APP.7.A5 Geeignete Steuerung der Anwendungsentwicklung: Abstimmung mit Auftragnehmer über Vorgehensmodell ergänzt (ursprünglich: CON.5.A8 Geeignete Steuerung der Anwendungsentwicklung).
- APP.7.A6 Dokumentation der Anforderungen an die Individualsoftware: Ergänzung des Sicherheitsprofils (ursprünglich: CON.5.A6 Dokumentation der Anforderungen an die Individualsoftware).
- APP.7.A7 Sichere Beschaffung von Individualsoftware: Ergänzung von Sicherheitsaspekten bei der Beschaffung (ursprünglich CON.5.A11 Geeignete und rechtskonforme Beschaffung).
- APP.7.A9 Treuhänderische Hinterlegung: Verschiebung von CON.5.A12 Treuhänderische Hinterlegung.

Änderungen an den Bausteinen der Edition 2020: SYS.1.1 Allgemeiner Server

Neue Anforderungen:

- SYS.1.1.A35 Erstellung und Pflege eines Betriebshandbuchs: Neue Standard-Anforderung zur Nutzung eines Betriebshandbuchs. (vorher SYS.1.8.A10)
- SYS.1.1.A36 Absicherung des Bootvorgangs: Neue Anforderung bei erhöhtem Schutzbedarf zur Verwendung von Secure Boot. (vorher SYS.2.3.A16)

Änderungen an bestehenden Anforderungen:

- SYS.1.1.A1 Geeignete Aufstellung: Ergänzt, dass Arbeitsplatzrechner keine Server und Server keine Arbeitsplatzrechner sein dürfen.
- SYS.1.1.A5 umbenannt in „Schutz von Schnittstellen“. Grundsätzliche Betrachtungen zur Administration entfernt, da dieses Thema in OPS.1.1.2 Ordnungsgemäße IT-Administration umfassend behandelt wird. Deaktivieren nicht genutzter Schnittstellen ergänzt. Verbot von Servern als Arbeitsplatzrechner nach SYS.1.1.A1 Geeignete Aufstellung verschoben.

Änderungen an den Bausteinen der Edition 2020: SYS.1.1 Allgemeiner Server

Änderungen an bestehenden Anforderungen:

- SYS.1.1.A9 umbenannt in „Einsatz von Virenschutz-Programmen auf Servern“, da diese Anforderung den Baustein OPS.1.1.4 Schutz vor Schadprogrammen entsprechend konkretisiert.
- SYS.1.1.A10 Protokollierung: Aspekte entfernt, welche allgemeine Grundlagen der Protokollierung betreffen, da dieses Thema ausführlich und vollständig in OPS.1.1.5 Protokollierung behandelt wird.
- SYS.1.1.A16 Sichere Installation und Grundkonfiguration von Servern: Umbenannt in Sichere Grundkonfiguration von Servern und Aspekte zur Installation entfernt. Diese finden sich im neuen Baustein APP.6 Allgemeine Software, insbesondere in APP6.A4 Regelung für die Installation und Konfiguration von Software.
- SYS.1.1.A19 Einrichtung lokaler Paketfilter: Teilanforderung zur kryptographischen Absicherung von Verbindungen hinzugefügt.

Änderungen an den Bausteinen der Edition 2020: SYS.1.1 Allgemeiner Server

Änderungen an bestehenden Anforderungen:

- SYS.1.2.2.A14 Herunterfahren verschlüsselter Server und virtueller Maschinen: Ruhezustand als alternative zum Herunterfahren entfernt, da dies nicht in jedem Fall ausreichend schützt.

Änderungen an den Bausteinen der Edition 2020: SYS.1.3 Server unter Linux und Unix

Änderungen an bestehenden Anforderungen:

- SYS.1.3.A2 Sorgfältige Vergabe von IDs: Schärfung dahingehend, dass die Vergabe von Namen und IDs bei systemübergreifendem Zugriff konsistent sein muss.
- SYS.1.3.A6 Verwaltung von Benutzern und Gruppen: /etc/shadow wurde in die Liste der Dateien, die nicht direkt bearbeitet werden sollen, aufgenommen.

Änderungen an den Bausteinen der Edition 2020: SYS.1.8 Speicherlösungen

Änderungen an bestehenden Anforderungen:

- SYS.1.8.A6 Erstellung einer Sicherheitsrichtlinie für Speicherlösungen: Die Anforderung wurde um den Aspekt einer möglichen Aktualisierung der Richtlinie erweitert.

Änderungen an den Bausteinen der Edition 2020: SYS.2.1 Allgemeiner Client

Neue Anforderungen:

- SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen: Diese Anforderung wurde aus SYS.2.3 Clients unter Linux und Unix übernommen.
- SYS.2.1.A43 Lokale Sicherheitsrichtlinien für Clients: Diese Anforderung ist eine generalisierte Version der entfallenen Anforderung SYS.2.2.3.A7 Lokale Sicherheitsrichtlinien für Windows 10.
- SYS.2.1.A44 Verwaltung der Sicherheitsrichtlinien von Clients: Diese Anforderung ist eine generalisierte Version der entfallenen, Windows-10-spezifischen SYS.2.2.3.A8 Zentrale Verwaltung der Sicherheitsrichtlinien von Clients.
- SYS.2.1.A45 Erweiterte Protokollierung: Empfehlungen zur Protokollierung über Sicherheitsaspekte hinaus.

Änderungen an bestehenden Anforderungen:

- SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware: Die Anforderung wurde mit Fokus auf Client-Systeme neu konzipiert.
- SYS.2.1.A15 Sichere Installation und Konfiguration von Clients: Zeitliche Reihenfolge der Schritte bei Installation und Konfiguration präzisiert.

Änderungen an den Bausteinen der Edition 2020: SYS.2.1 Allgemeiner Client

Änderungen an bestehenden Anforderungen:

- SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen: Auflistung der zu deaktivierenden Komponenten erweitert und Anforderung insgesamt klarer gegliedert.
- SYS.2.1.A18 Nutzung von TLS: Anforderung verallgemeinert und daher umbenannt in Nutzung von verschlüsselten Kommunikationsverbindungen. Aspekt zur TLS-Verschlüsselung bei Webseiten und in Browsern entfernt.
- SYS.2.1.A20 Schutz der Administrationsschnittstellen: Umbenannt in Schutz der Administrationsverfahren bei Clients und präzisiert.
- SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern: Aspekte zum Umgang mit externen Geräten aus fremden Quellen ergänzt und geschärft.
- SYS.2.1.A28 Verschlüsselung der Clients: Aspekt des Schutzes von Schlüsselmaterial generalisiert.
- SYS.2.1.A30 Einrichten einer Referenzinstallation für Clients: Umbenennung in Einrichtung einer Referenzumgebung für Clients. Fokus der Anforderung auf Tests aus Benutzersicht geschärft.
- SYS.2.1.A31 Einrichtung lokaler Paketfilter: Präzisierung der Whitelist-Strategie.

Änderungen an den Bausteinen der Edition 2020: SYS.2.2.2 Clients unter Windows 8.1

Änderungen an bestehenden Anforderungen:

- SYS.2.2.2.A2 Festlegung eines Anmeldeverfahrens für Windows 8.1: Anforderung zur Festlegung eines identischen Anmeldeverfahrens auf allen Clients entfernt, da nicht praxisnah.
- SYS.2.2.2.A18 Aktivierung des Last-Access-Zeitstempels: Mögliche Auswirkungen dieser Einstellung konkretisiert.

Änderungen an den Bausteinen der Edition 2020: SYS.2.2.3 Clients unter Windows 10

Änderungen an bestehenden Anforderungen:

- SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen unter Windows 10: Die Anforderung wurde um die Nennung eines Telemetrielevels als Alternative zur netzseitigen Blockierung der Telemetrie ergänzt.
- SYS.2.2.3.A24 Aktivierung des Last-Access-Zeitstempels: Der Anforderungstext wurde überarbeitet, um ihn an die gleichnamige Anforderung im Baustein SYS.2.2.2 Clients unter Windows 8.1 anzupassen.

Änderungen an den Bausteinen der Edition 2020: SYS.3.1 Laptops

Änderungen an bestehenden Anforderungen:

- SYS.3.1.A13 Verschlüsselung von Laptops: Die Anforderung wurde präzisiert und die Vorgaben für die Verschlüsselung der Datenträger wurden entfernt, da dies über das verwendete Betriebssystem umzusetzen ist.
- SYS.3.1.A14 Geeignete Aufbewahrung von Laptops: Verschließen von Laptops in den Räumlichkeiten der Institution ist nun abhängig vom Schutzbedarf der gespeicherten Daten zu betrachten und keine generelle Anforderung mehr.
- SYS.3.1.A15 Geeignete Auswahl von Laptops: Berücksichtigung von Docking-Stationen und Monitoren entfernt, da nicht relevant für die Informationssicherheit.
- SYS.3.1.A16 Zentrale Administration von Laptops: Die Anforderung wurde umbenannt in Zentrale Administration und Verwaltung von Laptops, da beides im Anforderungstext eine Rolle spielt.

Umsortierung von Anforderungen:

- SYS.3.1.A9 Sicherer Fernzugriff mit Laptops: Dies ist nun eine Basis-Anforderung (vorher: Standard-Anforderung). Die Anforderung wurde im Hinblick auf den sicheren Zugriff auf das Netz der Institution generalisiert.

Änderungen an den Bausteinen der Edition 2020: SYS.3.2.1 Allgemeine Smartphones und Tablets

Neue Anforderungen:

- SYS.3.2.1.A2 Festlegung einer Strategie für die Cloud-Nutzung: Die Teilanforderung zum Aspekt Nutzung von Cloud-Diensten, wenn eine private Nutzung der Geräte erlaubt ist, wurde hinzugefügt.
- SYS.3.2.1.A31 Regelung zu Mobile-Payment
- SYS.3.2.1.A32 MDM-Nutzung
- SYS.3.2.1.A33 Auswahl und Installation von Sicherheits-Apps (vorher SYS.3.2.2.A9)
- SYS.3.2.1.A34 Konfiguration des verwendeten DNS-Servers (S)
- SYS.3.2.1.A35 Verwendung einer Firewall: Die Anforderung wurde aus dem Baustein SYS.3.2.4 Android hierher verschoben.

Änderungen an bestehenden Anforderungen:

- SYS.3.2.1.A6 Datenschutzeinstellung und Berechtigungen: Die Anforderung wurde umbenannt. Aspekte zum Umgang mit Berechtigungseinstellungen wurden ergänzt.
- SYS.3.2.1.A8 Keine Installation aus unsicheren Quellen: Die Anforderung wurde umbenannt in Installation von Apps. Zudem wurde sie um Aspekte zum Thema Berechtigungen und Freigabe zur Installation von Apps sowie erlaubte Quellen erweitert.
- SYS.3.2.1.A10 Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten: Aufgenommen wurde das Verbot, wesentliche Konfigurationen zu ändern.

Änderungen an den Bausteinen der Edition 2020: SYS.3.2.2 Mobile Device Management

Änderungen an bestehenden Anforderungen:

- SYS.3.2.2.A1 Festlegung einer Strategie für das Mobile Device Management: Das Thema „managed und unmanaged Bereich“ und welche Restriktionen die Institution vorgibt, wurde hinzugefügt. Der Aspekt „Einbindung des MDM in weitere Infrastrukturen“ wurde eingefügt.
- SYS.3.2.2.A17 Kontrolle der Nutzung von mobilen Endgeräten: Anforderung zu Jailbreaks und zum Routen wurde hinzugefügt.

Umsortierung von Anforderungen:

- SYS.3.2.2.A6 Protokollierung des Gerätestatus: Die Anforderung wurde in eine Standard-Anforderung überführt (vorher Basis-Anforderung), da aufgrund von entfernten Redundanzen nur eine SOLLTE-Anforderung enthalten blieb.

Änderungen an den Bausteinen der Edition 2020: SYS.3.2.4 Android

Änderungen an bestehenden Anforderungen:

- SYS.3.2.4.A3 Einsatz des Multi-User- und Gäste-Modus: Der Aspekt zur Nutzung eines Gerätes von mehreren Personen wurde aufgenommen.

Änderungen an den Bausteinen der Edition 2020: SYS.3.2.4 Android

Neue Anforderungen:

- SYS.3.3.A5 Nutzung der Sicherheitsmechanismen von Mobiltelefonen: Die Teilanforderung zur Nutzung von PIN/PUK wurde auf aufgenommen (um SYS.3.2.1.A17 ergänzt).

Änderungen an bestehenden Anforderungen:

- SYS.3.3.A1 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung: Der Aspekt zur Nutzung und Kontrolle der Geräte wurde aufgenommen.

Umsortierung von Anforderungen:

- SYS.3.3.A9 Sicherstellung der Energieversorgung von Mobiltelefonen: Anforderung wurde zu den Anforderungen bei erhöhtem Schutzbedarf verschoben.

Änderungen an den Bausteinen der Edition 2020: SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

Änderungen an bestehenden Anforderungen:

- SYS.4.1.A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten: Ergänzung von Kriterien, die bei der Planung berücksichtigt werden sollten.
- SYS.4.1.A4: Erstellung einer Sicherheitsrichtlinie für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten: Anpassung des Anforderungstitels und Konkretisierung von Sicherheitskonzept zur Sicherheitsrichtlinie.
- SYS.4.1.A14 Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten: Der Aspekt SecurePrinting wurde geschärft.
- SYS.4.1.A16 Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten: Anforderung wurde in Verringerung von Ausfallzeiten bei Druckern, Kopierern und Multifunktionsgeräten umbenannt.
- SYS.4.1.A18 Konfiguration von Druckern, Kopierern und Multifunktionsgeräten: Die Anforderung wurde um den Aspekt, dass diese Geräte nur vom IT-Personal administriert werden sollten, konkretisiert. Außerdem wurde die Deaktivierung von nicht benötigten Datenschnittstellen aufgenommen.
- SYS.4.1.A21 Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten: Zuständigkeit zum IT-Betrieb wurde hervorgehoben.

Änderungen an den Bausteinen der Edition 2020: SYS.4.3 Eingebettete Systeme

Änderungen an bestehenden Anforderungen:

- SYS.4.3.A4 Erstellung von Beschaffungskriterien für eingebettete Systeme: Der Aspekt zum Thema Trusted Plattform Module (TPM) wurde eingefügt.

Änderungen an den Bausteinen der Edition 2020: SYS.4.5 Wechseldatenträger

Änderungen an bestehenden Anforderungen:

- SYS.4.5.A10 Datenträgerverschlüsselung: Anforderung nach Basis verschoben. Datenträger müssen nun immer verschlüsselt werden, wenn sie außerhalb eines sicheren Bereiches vertrauliche Daten transportieren.

Änderungen an den Bausteinen der Edition 2020: IND.1 Prozessleit- und Automatisierungstechnik

Neue Anforderungen:

- IND.1.A18 Protokollierung
- IND.1.A19 Erstellung von Datensicherungen
- IND.1.A20 Systemdokumentation (vorher IND.2.1.A10)
- IND.1.A21 Dokumentation der Kommunikationsbeziehungen (vorher IND.2.1.A9)
- IND.1A22 Zentrale Systemprotokollierung und -überwachung (vorher IND.2.1.A15)
- IND.1.A23 Aussonderung von ICS-Komponenten (vorher IND.2.1.A14)
- IND.1.A24 Kommunikation im Störfall (vorher IND.2.1.A18)

Änderungen an den Bausteinen der Edition 2020: IND.1 Prozessleit- und Automatisierungstechnik

Änderungen an bestehenden Anforderungen:

- IND.1.A9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten: Der Anforderungstitel wurde konkretisiert zu Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen.
- IND.1.A12 Etablieren eines Schwachstellen-Managements: Die Formulierung wurde angepasst und geschärft.
- IND.1.A14 Starke Authentisierung an OT-Komponenten: Die Formulierung wurde angepasst und geschärft.
- IND.1.A15 Prüfung und Überwachung von Berechtigungen: Der Anforderungstitel wurde geändert in Überwachung von weitreichenden Berechtigungen.
- IND.1.A17 Regelmäßige Sicherheitsüberprüfung: Die Formulierung wurde angepasst und geschärft.

Änderungen an den Bausteinen der Edition 2020: IND.2.1 Allgemeine ICS-Komponente

Änderungen an bestehenden Anforderungen:

- IND.2.1.A1 Einschränkung des Zugriffs für Kommunikations- und Wartungsschnittstellen: Teilanforderungen wurden entfernt, die bereits aus ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme hervorgehen. Die Anforderung wurde konkretisiert.
- IND.2.1.A2 Nutzung sicherer Protokolle für die Konfiguration und Wartung: Der Anforderungstitel wurde geändert in Nutzung sicherer Übertragungsprotokolle für die Konfiguration und Wartung. Die Anforderung wurde konkretisiert.
- IND.2.1.A4 Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen: Der Anforderungstitel wurde geändert in Deaktivierung oder Deinstallation nicht genutzter Dienste, Funktionen und Schnittstellen.
- IND.2.1.A7 Backups: Die Anforderung wurde in Erstellung von Datensicherungen umbenannt. Die Anforderung wurde konkretisiert.
- IND.2.1.A8 Schutz vor Schadsoftware: Die Anforderung wurde konkretisiert.

Änderungen an den Bausteinen der Edition 2020: IND.2.7 Safety Instrumented Systems

Änderungen an bestehenden Anforderungen:

- IND.2.7.A2: Zweckgebundene Nutzung der Hard- und Softwarekomponenten: Die Formulierung der Anforderung wurde überarbeitet.
- IND.2.7.A6: Sichere Planung uns Spezifikation des SIS: Die Formulierung der Anforderung wurde überarbeitet.
- IND.2.7.A8: Zweckgebundene Nutzung der Hard- und Softwarekomponenten: Die Formulierung der Anforderung wurde überarbeitet.

Änderungen an den Bausteinen der Edition 2020: NET.1.1 Netzarchitektur und -design

Änderungen an bestehenden Anforderungen:

- NET.1.1.A18 P-A-P-Struktur für die Internet-Anbindung: Anforderung wurde sprachlich präzisiert und um den Aspekt einer Segmentierung des Transfernetzes bei gegenseitigem Angriffspotential der Sicherheits-Proxies untereinander erweitert.
- NET.1.1.A23 Trennung von Sicherheitssegmenten: Sprachliche Anpassung des Anforderungstitels und der Anforderung.
- NET.1.1.A24 Sichere logische Trennung mittels VLAN: Diese Anforderung wurde sprachlich präzisiert.
- NET.1.1.A31 Physische Trennung von Sicherheitssegmenten: Sprachliche Anpassung des Anforderungstitels und der Anforderung.
- NET.1.1.A32 Physische Trennung von Management-Netzsegmenten: Sprachliche Anpassung des Anforderungstitels und der Anforderung.

Änderungen an den Bausteinen der Edition 2020: NET.1.2 Netzmanagement

Änderungen an bestehenden Anforderungen:

- NET.1.2.A9 Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge: Die Anforderung wurde um die Absicherung des Zugriffs auf Netz-Management-Werkzeuge ergänzt. Außerdem wurde eine sprachliche Anpassung des Anforderungstitels vorgenommen.
- NET.1.2.A26 Alarming und Logging: Sprachliche Anpassung des Anforderungstitels.

Änderungen an den Bausteinen der Edition 2020: NET.2.1 WLAN-Betrieb

Änderungen an bestehenden Anforderungen:

- NET.2.1.A5 Sichere Basis-Konfiguration der Access Points: Konkretisierung der Teilanforderung zur Administration von Access Points.
- NET.2.1.A6 Sichere Konfiguration der WLAN-Clients: Umbenannt in Sichere Konfiguration der WLAN-Infrastruktur aufgrund der Änderungen innerhalb der Anforderung. Die Absicherung der Clients muss über die entsprechenden Bausteine der Schicht SYS erfolgen.
- NET.2.1.A7 Aufbau eines Distribution Systems: Sprachliche Schärfung der Anforderung im Bezug auf das Distribution System.
- NET.2.1.A10 Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs: Zusätzliche Teilanforderung zur geeigneten Reaktion nach Prüfung der Umsetzung der Inhalte aufgenommen.

Änderungen an den Bausteinen der Edition 2020: NET.2.2 WLAN-Nutzung

Änderungen an bestehenden Anforderungen:

- NET.2.2.A1 Erstellung einer Benutzerrichtlinie für WLAN: Zusätzliche Teilanforderung zur geeigneten Reaktion nach Prüfung der Umsetzung der Inhalte aufgenommen.
- NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzer: Zusätzliche Teilanforderung zu den Inhalten der Schulung mit aufgenommen.
- NET.2.2.A3 Absicherung der WLAN-Nutzung in unsicheren Umgebungen: Umbenannt in Absicherung der WLAN-Nutzung an Hotspots, um die Nutzung von Hotspots im Allgemeinen und nicht mehr nur in unsicheren Umgebungen zu behandeln. Anforderung wurde um weitere Punkte zur Verschlüsselung, zum automatischen Anmelden und zur Deaktivierung der Schnittstelle ergänzt.

Änderungen an den Bausteinen der Edition 2020: NET.3.2 Firewall

Neue Anforderungen:

- NET.3.2.A32 Notfallvorsorge für die Firewall: Die Anforderung wurde analog zu NET.3.1.A22 aufgenommen.

Änderungen an bestehenden Anforderungen:

- NET.3.2.A9 Protokollierung: Diese Anforderung wurde um eine neue Teilanforderung zur automatischen Dokumentation von Änderungen der Konfiguration aus NET.3.2.A14 Betriebsdokumentationen ergänzt.
- NET.3.2.A16 Aufbau einer „P-A-P“-Struktur: Die erste Teilanforderung "Der Aufbau einer 'Paketfilter – Application-Level-Gateway – Paketfilter'-(P-A-P)-Struktur SOLLTE aus mehreren Komponenten mit jeweils dafür geeigneter Hard- und Software bestehen." ist nun eine MUSS-Teilanforderung. Darüber hinaus wurde sie zum besseren Verständnis sprachlich präzisiert.

Änderungen an den Bausteinen der Edition 2020: INF.1 Allgemeines Gebäude

Neue Anforderungen:

- INF.1.A35 Perimeterschutz: Neue Anforderung für den erhöhten Schutzbedarf zum Perimeterschutz von Gebäuden.
- INF.1.A36 Regelmäßige Aktualisierungen der Dokumentation: Neue Standardanforderung zur regelmäßigen Aktualisierung der Dokumentation von Gebäuden.

Änderungen an bestehenden Anforderungen:

- INF.1.A3 Einhaltung von Brandschutzvorschriften: Die Anforderung wurde um den Aspekt der regelmäßigen Kontrolle der Fluchtwege erweitert.
- INF.1.A5 Handfeuerlöscher: Die Anforderung wurde um den Aspekt der regelmäßigen Einweisung konkretisiert.
- INF.1.A6 Geschlossene Fenster und Türen: Die Anforderung wurde um den Aspekt des Verschließens von Räumen ergänzt. Die Anforderung wurde um den Aspekt erweitert, dass entsprechende Vorgaben in einer geeigneten Anweisung festzuhalten sind, sowie alle Mitarbeiten dazu verpflichtet sein sollten, den Anweisungen nachzukommen.

Änderungen an den Bausteinen der Edition 2020: INF.1 Allgemeines Gebäude

Änderungen an bestehenden Anforderungen:

- INF.1.A7 Zutrittsregelung und -kontrolle: Die Anforderung wurde um den Aspekt der Kontrollen bei Umzügen ergänzt.
- INF.1.A9 Sicherheitskonzept für die Gebäudenutzung: Die Anforderung wurde um den Aspekt der Dokumentation des Sicherheitskonzeptes erweitert.
- INF.1.A19 Frühzeitige Information des Brandschutzbeauftragten: Der Anforderungstitel wurde um die Einschränkung „frühzeitig“ gekürzt.
- INF.1.A26 Pförtner- oder Sicherheitsdienst: Die Anforderung wurde um den Aspekt erweitert, dass der Pförtnerdienst alle Personenbewegungen nach dem Sicherheitskonzept kontrollieren muss.
- INF.1.A34 Gefahrenmeldeanlage: Die Anforderung wurde um den Aspekt erweitert, dass sichergestellt ist, dass die Empfänger von Gefahrenmeldungen in der Lage sind, technisch und personell angemessen auf den Alarm zu reagieren.

Änderungen an den Bausteinen der Edition 2020: INF.1 Allgemeines Gebäude

Umsortierung von Anforderungen:

- INF.1.A10 Einhaltung einschlägiger Normen und Vorschriften: Die Anforderung wurde in die Basis-Anforderungen verschoben (vorher Standard Anforderung).
- INF.1.A27 Einbruchschutz: Die Anforderung wurde in die Standard-Anforderungen verschoben (vorher erhöhter Schutzbedarf).

Änderungen an den Bausteinen der Edition 2020: INF.2 Rechenzentrum sowie Serverraum

Änderungen an bestehenden Anforderungen:

- Sprachliche Anpassungen im Zusammenhang mit der Unterscheidung des Betriebsbereichs ggü. dem gesamten Rechenzentrum.
- INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage: Verkürzung der Reaktionszeit von 5 auf 3 Minuten.
- INF.2.A10 Inspektion und Wartung der Infrastruktur: Sprachliche Anpassung mit Blick auf die Brandschottung.
- INF.2.A11 Automatische Überwachung der Infrastruktur: Sprachliche Anpassungen zum besseren Verständnis.
- INF.2.A12 Perimeterschutz für das Rechenzentrum: Die erste Anforderung zum Vorhandensein eines Perimeterschutzes wurde sprachlich präzisiert.
- INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen: Zusammenhang mit Sicherheitskonzept für das Gebäude stärker herausgearbeitet.
- INF.2.A14 Einsatz einer Netzersatzanlage: Die Anforderungen an die NEA MÜSSEN nun erfüllt werden, wenn eine NEA verwendet wird.
- INF.2.A15 Überspannungsschutzeinrichtung: Anpassung des Bezugs zu den gültigen Normen.

Änderungen an den Bausteinen der Edition 2020: INF.2 Rechenzentrum sowie Serverraum

Änderungen an bestehenden Anforderungen:

- INF.2.A17 Brandfrüherkennung: Neue Teilanforderung zur Klarstellung, dass eine Brandfrüherkennung in einem Rechenzentrum vorhanden sein MUSS, im Serverraum aber nur SOLLTE.
- INF.2.A22 Durchführung von Staubschutzmaßnahme: Konkretisierung, dass alle Baumaßnahmen gemeint sind.
- INF.2.A23 Sicher strukturierte Verkabelung im Rechenzentrum: Umbenannt in Zweckmäßiger Aufbau der Verkabelung im Rechenzentrum, um eine Verwechslung mit strukturierter Verkabelung zur vermeiden. Neustrukturierung der Anforderung mit Blick auf den Titel.
- INF.2.A29 Vermeidung und Überwachung nicht erforderlicher Leitungen: Sprachliche Anpassung der Teilanforderung zur Minimierung des von Leitungen ausgehenden Risikos.

Änderungen an den Bausteinen der Edition 2020: INF.5 Raum sowie Schrank für technische Infrastruktur

Änderungen an bestehenden Anforderungen:

- INF.5.A20 Schutz vor Einbruch und Sabotage: Die Anforderung wurde umbenannt in Erweiterter Schutz vor Einbruch und Sabotage, da der Titel zu ähnlich zu Anforderung INF.5.A4 Schutz vor Einbruch war. Die Anforderung wurde um Aspekte zum Schutz der Trassen und Datenleitungen gekürzt.
- INF.5.A23 Netzersatzanlange: Die Anforderung wurde bezüglich der Verantwortlichkeit konkretisiert.
- INF.5.A26 Überwachung der Energieversorgung: Die Anforderung wurde umformuliert und konkretisiert.

Umsortierung von Anforderungen:

- INF.5.A9 Stromversorgung: Die Anforderung wurde in eine Basis-Anforderung überführt (vorher Standard-Anforderung), da sie entsprechend konkretisiert wurde.

Änderungen an den Bausteinen der Edition 2020: INF.7 Büroarbeitsplatz

Änderungen an bestehenden Anforderungen:

- INF.7.A2 Geschlossene Fenster und abgeschlossene Türen: Die Anforderung wurde beim Aspekt des Schließens von Fenstern oder Türen konkretisiert.

Änderungen an den Bausteinen der Edition 2020: INF.9 Mobiler Arbeitsplatz

Neue Anforderungen:

- INF.9.A12 Nutzung eines Bildschirmschutzes

Änderungen an bestehenden Anforderungen:

- INF.9.A3 Zutritts- und Zugriffsschutz: Die Anforderung wurde um den Aspekt des Mitführens der IT-Systeme ergänzt. Der Aspekt, dass IT-Systeme beim Verlassen des Arbeitsplatzes heruntergefahren werden müssen, wurde gestrichen, da nicht praktikabel.

Änderungen an den Bausteinen der Edition 2020: INF.3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung; nun: INF.12 Verkabelung

Die Bausteine INF.3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung wurden zu einem neuen Baustein INF.12 Verkabelung zusammengelegt und dabei sprachlich und inhaltlich überarbeitet.

Folgende Dinge haben sich im Vergleich zu den Ursprungsbausteinen grundlegend geändert:

- Die Anforderungen zum Brandschott-Kataster wurden nicht mit übernommen. Das Thema wird im Baustein INF.1 Allgemeines Gebäude behandelt.
- Die Anforderung EMV-taugliche Stromversorgung ist nun im Vergleich zum Ursprungsbaustein eine Basis-Anforderung.

5. Methoden zur schnellen, effizienten Migration in das neue IT-Grundschutz-Kompendium

Erstellung einer Übersichtstabelle

Baustein	Anforderung	Teilanforderung	Vergleich	Status	Bewertung
IND.1 Betriebs- und Steuerungstechnik	IND.1.A3 Schutz vor Schadprogrammen	Beim Einsatz von Virenschutz-Software auf OT-Komponenten MUSS berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutz-Software vom Hersteller unterstützt wird. Ist dies nicht der Fall, MUSS der Bedarf an alternativen Schutzverfahren geprüft werden.	Beim Einsatz von Virenschutz-Software auf OT-Komponenten MUSS berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutz-Software vom Hersteller unterstützt wird. Ist dies nicht der Fall, MUSS der Bedarf an alternativen Schutzverfahren geprüft werden. Es MUSS ein Konzept zum Schutz vor Schadprogrammen erstellt und umgesetzt werden. Darin MÜSSEN die bedrohten IT-Systeme sowie die möglichen Infektionswege wie Außenschnittstellen, Wechselmedien, Service- und Parametrier-/Programmiergeräte betrachtet werden. Es MÜSSEN geeignete technische und organisatorische Schutzmaßnahmen festgelegt sein.	Änderung	Kritisch
IND.1 Betriebs- und Steuerungstechnik	IND.1.A3 Schutz vor Schadprogrammen	Die Virensignaturen DÜRFEN NICHT von OT-Systemen direkt aus dem Internet bezogen werden.	Die Virensignaturen DÜRFEN NICHT von OT-Systemen direkt aus dem Internet bezogen werden. Beim Einsatz von Virenschutz-Software auf OT-Komponenten MUSS berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutz-Software vom Hersteller unterstützt wird. Ist dies nicht der Fall, MUSS im Rahmen einer Risikobetrachtung der Bedarf an alternativen Schutzverfahren geprüft werden.	Änderung	Kritisch
IND.1 Betriebs- und Steuerungstechnik	IND.1.A18 Protokollierung	Jede Änderung an ICS-Komponenten MUSS protokolliert werden. Außerdem MÜSSEN alle Zugriffe auf ICS-Komponeten protokolliert werden.	Jede Änderung an ICS-Komponenten MUSS protokolliert werden. Außerdem MÜSSEN alle Zugriffe auf ICS-Komponeten protokolliert werden.	Neu	
IND.1 Betriebs- und Steuerungstechnik	IND.1.A19 Erstellung von Datensicherungen	Programme und Daten MÜSSEN regelmäßig gesichert werden. Auch nach jeder Systemänderung an OT-Komponenten MUSS eine Sicherung erstellt werden.	Programme und Daten MÜSSEN regelmäßig gesichert werden. Auch nach jeder Systemänderung an OT-Komponenten MUSS eine Sicherung erstellt werden.	Neu	
ORP.5 Compliance Management (Anforderungsmanagement)	ORP.5.A1 Identifikation der Rahmenbedingungen	Alle gesetzlichen, vertraglichen und sonstigen Vorgaben mit Auswirkungen auf das Informationssicherheitsmanagement MÜSSEN identifiziert und dokumentiert werden. Die für die einzelnen Bereiche der Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben SOLLTEN in einer strukturierten Übersicht herausgearbeitet werden. Die Dokumentation MUSS auf dem aktuellen Stand gehalten werden.	Alle gesetzlichen, vertraglichen und sonstigen Vorgaben mit Auswirkungen auf das Informationssicherheitsmanagement MÜSSEN identifiziert und dokumentiert werden. Die für die einzelnen Bereiche der Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben SOLLTEN in einer strukturierten Übersicht herausgearbeitet werden. Die Dokumentation MUSS auf dem aktuellen Stand gehalten werden. In der Institution MUSS ein Prozess aufgebaut sein, um alle relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren. Alle rechtlichen Rahmenbedingungen mit Auswirkungen auf das Informationssicherheitsmanagement MÜSSEN identifiziert und dokumentiert werden.	Änderung	Mittel

Unterstützung der Migration durch verinice

- Alle Editionen des IT-Grundschutz-Kompendiums für verinice kostenlos über den verinice.SHOP unter https://shop.verinice.com/de/content/it-gs-kompendium

- Übernahme der Änderungen der Edition 2021 ca. Anfang März 2021

- Wie wird die Migration mit Verinice vorgenommen? (zeigt Vorgehen zur Migration von 2019 zu 2020): https://www.youtube.com/watch?v=jAbq9vauY9w
  - u.a. Vereinfachung der Migration durch Drag and Drop nach neuer Modellierung und vorheriger Bewertung welche Anforderungen geändert wurden und welche neu sind

Offene Fragen

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com