Bundesamt
für Sicherheit in der
Informationstechnik

Änderungen in der Edition 2021 des IT-Grundschutz-Kompendiums

Inhaltsverzeichnis

Änderungsdokument zum Baustein: SYS.4.4 Allgemeines IoT-Gerät

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.4.4.A2 *Authentisierung:* Die Teilanforderungen zum sicheren Passwort, zur Passwortrichtlinie, sowie zum Ändern voreingestellter Passwörter wurden entfernt, da sie redundant zu den Anforderungen ORP.4.A22 *Regelung zur Passwortqualität,* ORP.4.A23 *Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme* und ORP.4.A8 *Regelung des Passwortgebrauchs* sind.

Entfernung von Anforderungen

- SYS.4.4.A3 *Regelmäßige Aktualisierung*: Die Anforderung wurde entfernt, da sie redundant zur Anforderungen OPS.1.1.3.A16 *Regelmäßige Suche nach Informationen zu Patches und Schwachstellen* ist.
- SYS.4.4.A9 *Regelungen des Einsatzes von IoT-Geräten*: Die Teilanforderung zum Aspekt Informieren über Meldewege bei Sicherheitsvorfällen wurde entfernt, da sie redundant zur Anforderung DER.1.A4 *Sensibilisierung der Mitarbeiter* ist.
- SYS.4.4.A12 *Sichere Integration in übergeordnete Systeme*: Die Anforderung wurde entfernt, da sie redundant zur Anforderung SYS.4.4.A5 *Einschränkung des Netzzugriffs* ist.
- SYS.4.4.A14 *Einsatzfreigabe*: Die Anforderung wurde entfernt, da sie redundant zur Anforderung OPS.1.1.3.A9 *Test- und Abnahmeverfahren für neue Hardware* ist.
- SYS.4.4.A19 *Schutz der Administrationsschnittstellen*: Die Teilanforderungen zu Administrationsschnittstellen und Protokollierung der Administration wurden entfernt, da sie redundant zu den Anforderungen OPS.1.1.2.A16 *Zugangsbeschränkungen für administrative Zugänge* und OPS.1.1.2.A18 *Durchgängige Protokollierung administrativer Tätigkeiten* sind.
- SYS.4.4.A20 *Geregelte Außerbetriebnahme von IoT-Geräten*: Die Teilanforderung zum Löschen von Daten bei der Außerbetriebnahme wurde entfernt, da sie redundant zur Anforderung CON.6.A4 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern* ist.

Änderungsdokument zum Baustein: SYS.4.5 Wechseldatenträger

Kapitel 1.3: Abgrenzung und Modellierung

- Verweise auf nicht relevante Bausteine entfernt.

Kapitel 2: Gefährdungen

- Gefährdung *Datendiebstahl mit Wechseldatenträgern* entfernt, da nicht spezifisch genug.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.4.5.A7 *Sicheres Löschen der Datenträger vor und nach der Verwendung*: Teilanforderung zum Bereitstellen geeigneter Programme entfernt, da redundant zu *CON.6.A4 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern.*
- SYS.4.5.A10 *Datenträgerverschlüsselung*: Anforderung nach Basis verschoben. Datenträger müssen nun immer verschlüsselt werden, wenn sie außerhalb eines sicheren Bereiches vertrauliche Daten transportieren.

IND: Industrielle IT Änderunsgdokumente

Änderungsdokument zum Baustein: IND.1 Prozessleit- und Automatisierungstechnik

Kapitel 1.3: Abgrenzung und Modellierung

- Der Baustein IND.1 *Betriebs- und Steuerungstechnik* wurde umbenannt in IND.1 *Prozessleit- und Automatisierungstechnik*.
- Ergänzung der Abgrenzung gegenüber dem Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit.*
- Ergänzung der Abgrenzung gegenüber dem Baustein OPS.1.1.5 *Protokollierung.*

Kapitel 3: Anforderungen

Neue Anforderungen

- IND.1.A18 *Protokollierung*
- IND.1.A19 *Erstellung von Datensicherungen*
- IND.1.A20 *Systemdokumentation*
- IND.1.A21 *Dokumentation der Kommunikationsbeziehungen*
- IND.1A22 *Zentrale Systemprotokollierung und -überwachung*
- IND.1.A23 *Aussonderung von ICS-Komponenten*
- IND.1.A24 *Kommunikation im Störfall*

Änderungen an bestehenden Anforderungen

- IND.1.A1 *Einbindung in die Sicherheitsorganisation*: Entfernung von Teilanforderungen, die bereits aus ISMS.1.A1 *Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene* hervorgehen.
- IND.1.A3 *Schutz vor Schadprogrammen*: Entfernung allgemeiner Anforderungen zum Thema Schadprogramme, da sie die redundant zu OPS.1.1.4.A1 *Erstellung eines Konzepts für den Schutz vor Schadprogrammen* sind. Aspekte zum Thema Signaturen wurden ebenfalls entfernt, da sie redundant zu OPS.1.1.4.A6 *Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen* sind.
- IND.1.A4 *Dokumentation der OT-Infrastruktur*: Die Teilanforderung zur Dokumentation der Sicherheitszonen wurde entfernt, da sie redundant zur Anforderung NET.1.1.A2 *Dokumentation des Netzes* ist.
- IND.1.A5 *Entwicklung eines geeigneten Zonenkonzepts*: Entfernung von Teilanforderungen, die bereits aus NET.1.1.A23 *Trennung von Sicherheitssegmenten* hervorgehen. Der Aspekt zur Durchführung und Umfang einer Risikoanalyse wurde entfernt, da sich bereits aus der IT-Grundschutz-Methodik ergibt, wann eine Risikoanalyse durchzuführen ist.
- IND.1.A6 *Änderungsmanagement im OT-Betrieb*: Die Teilanforderungen zu Art und Umfang des Konzeptes eines Änderungsmanagements wurden entfernt, da sie redundant zur Anforderung OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement* sind.
- IND.1.A7 *Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT*: Entfernung von Teilanforderungen, die bereits umfassend aus ORP.4 *Identitäts- und Berechtigungsmanagement* hervorgehen. Der Anforderungstitel wurde teilweise konkretisiert.
- IND.1.A8 *Sichere Administration*: Entfernung redundanter Teilanforderungen. Der Aspekt zur Deaktivierung des Fernwartungszugangs nach Nutzung geht bereits aus OPS.1.2.5.A3 *Absicherung der Schnittstellen zur Fernwartung* hervor. Der Aspekt zur Dokumentation geht aus OPS.1.2.5.A7 *Dokumentation bei der Fernwartung* hervor. Der Aspekt zur Vermeidung von unerwünschten Tunneln geht aus OPS.1.2.5.A17 *Authentisierungsmechanismen bei der Fernwartung* hervor.

- 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.A10 *Monitoring, Protokollierung und Detektion*: Der Aspekt zum Thema Reaktionsplan ist redundant zur Anforderung DER.2.1.A2 *Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen und wurde entfernt*.
- 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.A16 *Stärkere Abschottung der Zonen*: Der Aspekt zur Ableitung spezifischer Einzelsicherungsmaßnahmen wurde entfernt, da dies bereits aus der IT-Grundschutz-Methodik hervorgeht.
- IND.1.A17 *Regelmäßige Sicherheitsüberprüfung*: Die Formulierung wurde angepasst und geschärft.
- IND.1.A18 *Protokollierung*: Die Teilanforderung zum Aspekt Protokollierung und Auswertung von sicherheitsrelevanten Ereignissen wurde entfernt, da sie bereits aus IND.1.A10 *Monitoring, Protokollierung und Detektion* hervorgeht.

Entfernung von Anforderungen

- IND.1.A2 *Sensibilisierung und Schulung des Personals*: Entfallen, da die Anforderung redundant zur Anforderung ORP.3.A6 *Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit* ist.

Änderungsdokument zum Baustein: IND.2.1 Allgemeine ICS-Komponente

Kapitel 2: Gefährdungslage

- Die Gefährdung *Beeinträchtigung durch schädliche Umgebungseinflüsse* wurde in dem Baustein IND.1 *Prozessleit- und Steuerungstechnik* verschoben.
- Die Gefährdung *Unvollständige Dokumentation* wurde entfernt, da die gegenwirkende Anforderung im Baustein IND.1 *Prozessleit- und Automatisierungstechnik* enthalten ist.
- Die Gefährdung *Unzureichende Protokollierung* wurde entfernt, da die gegenwirkende Anforderung in dem Baustein IND.1 *Prozessleit- und Automatisierungstechnik* enthalten ist.
- Die Gefährdung *Unzureichende Sicherheitsanforderungen bei der Beschaffung* wurde entfernt, da die gegenwirkende Anforderung in dem Baustein IND.1 *Prozessleit- und Automatisierungstechnik* enthalten ist.

Kapitel 3: Anforderungen

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.
- IND.2.1.A13 *Geeignete Inbetriebnahme der ICS-Komponenten*: Die Teilanforderung zur Einbindung der ICS-Komponenten in das Änderungs- und Berechtigungsmanagement, das Schwachstellenmanagement, den Schutz vor Schadsoftware, die betriebliche Überwachung sowie Notfallplanung und die regelmäßige Sicherheitsüberprüfung der Systeme wurde entfernt, da sie bereits aus folgenden Anforderungen hervorgeht: OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement*, ORP.4.A3 *Dokumentation der Benutzerkennungen und Rechteprofile*, IND.1.A12 *Etablieren eines Schwachstellen-Managements*, IND.1.A3 *Schutz vor Schadprogrammen*, DER.4.A14 *Regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen* und DER.1.A9 *Einsatz zusätzlicher Detektionssysteme*.

Entfernung von Anforderungen

- IND.2.1.A3 *Protokollierung*: Die Anforderung wurde entfernt, da sie aus OPS.1.1.5.A1 *Erstellung einer Sicherheitsrichtlinie für die Protokollierung* und aus OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene* hervorgeht.
- IND.2.1.A5 *Deaktivierung nicht genutzter Benutzerkonten*: Die Anforderung wurde entfernt, da sie bereits aus ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* hervorgeht.
- IND.2.1.A9 *Dokumentation der Kommunikationsbeziehungen*: Die Anforderung wurde verschoben nach IND.1.A21 *Dokumentation der Kommunikationsbeziehungen*.
- IND.2.1.A10 *Systemdokumentation*: Die Anforderung wurde verschoben nach IND.1.A20 *Systemdokumentation*.

- IND.2.1.A12 *Beschaffung von ICS-Komponenten*: Die Anforderung wurde verschoben nach IND.1.A11 *Sichere Beschaffung und Systementwicklung*.
- IND.2.1.A14 *Aussonderung von ICS-Komponenten*: Die Anforderung wurde verschoben nach IND.1.A23 *Aussonderung von ICS-Komponenten*.
- IND.2.1.A15 *Zentrale Systemprotokollierung und -überwachung*: Die Anforderung wurde entfernt, da sie bereits aus folgenden Anforderungen hervorgeht: OPS.1.1.5.A9 *Bereitstellung von Protokollierungsdaten für die Auswertung*, OPS.1.1.5.A6 *Aufbau einer zentralen Protokollierungsinfrastruktur* und DER.1.A5 *Einsatz von mitgelieferten Systemfunktionen zur Detektion*.

Änderungsdokument zum Baustein: IND.2.2 Speicherprogrammierbare Steuerung (SPS)

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- IND.2.2.A2 *Benutzerkontrolle und restriktive Rechtevergabe*: Diese Anforderung ist bereits durch den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt und daher entfallen.

Änderungsdokument zum Baustein: IND.2.7 Safety Instrumented Systems

Kapitel 3: Anforderungen

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.

NET: Netze und Kommunikation Änderunsgdokumente

Änderungsdokument zum Baustein: NET.1.1 Netzarchitektur und -design

Kapitel 1.3: Abgrenzung und Modellierung

- Begriffe "Sicherheitszone" und "Sicherheitssegment" umbenannt in "Zone" bzw. "Netzsegment". Dabei deutlich herausgestellt, dass Zonen gegenüber Netzsegmenten immer eine physische Trennung erfordern.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.1.1.A8 *Grundlegende Absicherung des Internetzugangs:* Die erste Teilanforderung "Der Internetzugang MUSS entsprechend NET.1.1.A4 Netztrennung in Sicherheitszonen gestaltet werden." ist bereits durch die Anforderung NET.1.1.A4 *Netztrennung in Sicherheitszonen* abgedeckt.
- 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 Managemen-Netzsegmenten:* Sprachliche Anpassung des Anforderungstitels und der Anforderung.

Änderungsdokument zum Baustein: NET.1.2 Netzmanagement

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung in Bezug auf zu verwaltende IT-Systeme.
- Ergänzung der Abgrenzung gegenüber dem Baustein CON.3 *Datensicherungskonzept.*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.1.2.A6 *Regelmäßige Datensicherung:* Die ersten beiden Teilanforderungen sind bereits durch die Anforderung CON.3.A5 *Regelmäßige Datensicherung* im übergreifenden Baustein CON.3 *Datensicherungskonzept* abgedeckt.
- NET.1.2.A7 *Grundlegende Protokollierung von Ereignissen:* Die erste Teilanforderung ist bereits durch den übergreifenden Baustein OPS.1.1.5 *Protokollierung* abgedeckt.
- NET.1.2.A8 *Zeit-Synchronisation:* Die Teilanforderung zum Aspekt Synchronisation der Uhrzeit innerhalb des lokalen Netzes ist nun eine SOLLTE-Teilanforderung. Gleiches gilt für die Teilanforderung zur Positionierung einer NTP-Instanz innerhalb eines Managementnetzes.
- 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.A20 *Absicherung des Zugangs zu Netzmanagement-Lösungen:* Die ersten beiden Teilanforderungen sind bereits durch die Anforderungen ORP.4.A1 *Regelung für die Einrichtung und Löschung von Benutzern*, ORP.4.A10 *Schutz von Benutzerkennungen mit weitreichenden Berechtigungen*, ORP.4.A18 *Einsatz eines zentralen Authentisierungsdienstes* sowie OPS.1.1.2.A5 *Nachweisbarkeit von administrativen Tätigkeiten* abgedeckt.
- NET.1.2.A26 *Alarming und Logging:* Sprachliche Anpassung des Anforderungstitels.
- NET.1.2.A35 *Festlegungen zur Beweissicherung:* Die Aspekte zu Festlegung sowie Dokumentation von Vorgehensweisen zur Beweissicherung sowie zu forensischen Untersuchungen im Rahmen des Netzmanagements sind bereits durch den Baustein *DER.2.2 Vorsorge für die IT-Forensik* abgedeckt.

Entfernung von Anforderungen

- NET.1.2.A3 *Rollen- und Berechtigungskonzept für das Netzmanagement:* Diese Anforderung ist bereits durch die Anforderungen ORP.4.A1 *Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen*, ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* und ORP.4.A15 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* im übergreifenden Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* abgedeckt.
- NET.1.2.A4 *Grundlegende Authentisierung für den Netzmanagement-Zugriff:* Diese Anforderung ist bereits durch die Anforderungen *ORP.4.A9 Identifikation und Authentisierung* und *ORP.4.A22 Regelung zur Passwortqualität* im übergreifenden Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* abgedeckt.
- NET.1.2.A5 *Einspielen von Updates und Patches:* Diese Anforderung ist bereits durch die Anforderungen OPS.1.1.3.A16 *Regelmäßige Suche nach Informationen zu Patches und Schwachstellen* sowie OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement* im übergreifenden Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* abgedeckt.
- NET.1.2.A19 *Starke Authentisierung des Management-Zugriffs:* Diese Anforderung ist bereits durch die Anforderungen ORP.4.A1 *Regelung für die Einrichtung und Löschung von Benutzern*, ORP.4.A10 *Schutz von*

Benutzerkennungen mit weitreichenden Berechtigungen, ORP.4.A18 *Einsatz eines zentralen Authentisierungsdienstes* sowie OPS.1.1.2.A5 *Nachweisbarkeit von administrativen Tätigkeiten* abgedeckt.

- NET.1.2.A20 *Absicherung des Zugangs zu Netzmanagement-Lösungen:* Die ersten beiden Teilanforderungen sind bereits durch die Anforderungen ORP.4.A1 *Regelung für die Einrichtung und Löschung von Benutzern*, ORP.4.A10 *Schutz von Benutzerkennungen mit weitreichenden Berechtigungen*, ORP.4.A18 *Einsatz eines zentralen Authentisierungsdienstes* sowie OPS.1.1.2.A5 *Nachweisbarkeit von administrativen Tätigkeiten* abgedeckt. Der Aspekt Zugriff auf Netz-Management-Werkzeuge wurde nach NET.1.2.A9 *Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge* verschoben.
- NET.1.2.A23 *Protokollierung der administrativen Zugriffe:* Diese Anforderung ist bereits durch die Anforderung OPS.1.1.2.A5 *Nachweisbarkeit von administrativen Tätigkeiten* im übergreifenden Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* sowie entsprechende Anforderungen in den Bausteinen OPS.1.1.5 *Protokollierung* und OPS.1.2.2 *Archivierung* abgedeckt.
- NET.1.2.A34 *Protokollierung von Inhalten administrativer Sitzungen:* Diese Anforderung ist bereits durch die Anforderungen OPS.1.1.2.A17 *IT-Administration im Vier-Augen-Prinzip* und OPS.1.1.2.A18 *Durchgängige Protokollierung administrativer Tätigkeiten* im übergreifenden Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* abgedeckt.

Änderungsdokument zum Baustein: NET.2.1 WLAN-Betrieb

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel wurde um Bausteine ergänzt, in denen das Thema WLAN-Betrieb ebenfalls zu betrachten ist.
- Absicherung von Authentisierungsdiensten wurde aufgenommen.

Kapitel 3: Anforderungen

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. Weitere Teilanforderungen wurden nach NET.2.2.A3 *Absicherung der WLAN-Nutzung* (Abschalten der Schnittstelle) verschoben.
- NET.2.1.A7 *Aufbau eines Distribution Systems:* Sprachliche Schärfung der Anforderung im Bezug auf das Distribution System.
- NET.2.1.A8 *Verhaltensregeln bei WLAN-Sicherheitsvorfällen*: Die Teilanforderung "Die möglichen Konsequenzen sicherheitskritischer Ereignisse MÜSSEN untersucht werden." wurde gestrichen, da redundant zu DER.2.1.A5 *Behebung von Sicherheitsvorfällen.*
- NET.2.1.A10 *Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs*: Zusätzliche Teilanforderung zur geeigneten Reaktion nach Prüfung der Umsetzung der Inhalte aufgenommen.
- NET.2.1.A14 *Regelmäßige Audits der WLAN-Komponenten*: Teilanforderung zur Prüfung der Sicherheitsmaßnahmen und Konfiguration wurde zum besseren Verständnis in zwei Teilanforderungen aufgeteilt.

Änderungsdokument zum Baustein: NET.2.2 WLAN-Nutzung

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel wurde um Bausteine ergänzt, in denen das Thema WLAN-Nutzung ebenfalls zu betrachten ist.

Kapitel 2: Gefährdungslage

- Zusätzliches Beispiel zu *Unzureichende Kenntnis über Regelungen*.

Kapitel 3: Anforderungen

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.

Änderungsdokument zum Baustein: NET.3.1 Router und Switches

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel wurde um Bausteine ergänzt, in denen das Thema Router und Switches ebenfalls zu betrachten ist. Dafür wurden die entsprechenden, nicht bausteinspezifischen Anforderungen aus dem Baustein entfernt.

Kapitel 2: Gefährdungslage

- Gefährdung *Softwareschwachstellen oder -fehler* entfernt, da sie für Router und Switches nicht spezifisch und bereits in den übergreifenden Bausteinen beschrieben ist.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.3.1.A1 *Sichere Grundkonfiguration eines Routers oder Switches:* Teilanforderungen zur Einrichtung und Verwendung von Benutzerkonten entfernt, da redundant zu OPS.1.1.2.A7 *Regelung der IT-Administrationstätigkeit*, ORP.4.A7 *Vergabe von Zugriffsrechten* und ORP.4.A9 *Identifikation und Authentisierung.* Zudem wurde der Aspekt zur Speicherung von Passwörtern sprachlich angepasst.
- NET.3.1.A7 *Protokollierung bei Routern und Switches:* Teilanforderungen zu rechtlichen Rahmenbedingungen und zur Konfiguration der Protokollierung entfallen, da redundant zu OPS.1.1.5.A5 *Einhaltung rechtlicher Rahmenbedingungen* bzw. OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene.*

Entfernung von Anforderungen

- NET.3.1.A2: *Einspielen von Updates und Patches*: Die Vorgaben dieser Anforderung gehen nicht über die Vorgaben des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* hinaus.
- NET.3.1.A3 *Restriktive Rechtevergabe*: Diese Anforderung ist bereits durch die Anforderung ORP.4.A7 *Vergabe von Zugriffsrechten* im übergreifenden Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* abgedeckt.

Änderungsdokument zum Baustein: NET.3.2 Firewall

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel wurde um Bausteine ergänzt, in denen das Thema Firewall ebenfalls zu betrachten ist. Dafür wurden die entsprechenden, nicht bausteinspezifischen Anforderungen aus dem Baustein entfernt.

Kapitel 2: Gefährdungslage

- Gefährdung *Softwareschwachstellen oder -fehler* entfernt, da sie für Firewalls nicht spezifisch und bereits in den übergreifenden Bausteinen beschrieben ist.

Kapitel 3: Anforderungen

Neue Anforderungen

- NET.3.2.A32 *Notfallvorsorge für die Firewall*: Die Anforderung wurde analog zum Baustein NET.3.1 *Router und Switches* aufgenommen.

Änderungen an bestehenden Anforderungen

- NET.3.2.A2: *Festlegen der Firewall-Regeln:* Teilanforderung zum internen Netzzugriff entfernt, da redundant zu NET.1.1.A11 *Absicherung eingehender Kommunikation vom Internet in das interne Netz.*
- NET.3.2.A4: *Sichere Konfiguration der Firewall:* Teilanforderungen zur Einrichtung und Verwendung von Benutzerkonten entfernt, da redundant zu OPS.1.1.2.A7 *Regelung der IT-Administrationstätigkeit*. Zudem wurde der Aspekt zur Speicherung von Passwörtern sprachlich angepasst.
- NET.3.2.A9 *Protokollierung*: Teilanforderung zu rechtlichen Rahmenbedingungen entfernt, da redundant zu OPS.1.1.5.A5 *Einhaltung rechtlicher Rahmenbedingungen.* Zudem wurde diese Anforderung um eine neue Teilanforderung zur automatischen Dokumentation von Änderungen der Konfiguration aus NET.3.2.A14 *Betriebsdokumentationen* ergänzt.
- NET.3.2.A14 *Betriebsdokumentationen:* Teilanforderung zur automatischen Dokumentation von Änderungen der Konfiguration nach NET.3.2.A9 *Protokollierung* verschoben.
- 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.
- NET.3.2.A23 *Systemüberwachung und Auswertung*: Teilanforderung zur Auswertung von Protokolldaten entfallen, da redundant zu DER.1.A6 *Kontinuierliche Überwachung und Auswertung von Protokolldaten*.

Entfernung von Anforderungen

- NET.3.2.A5 *Restriktive Rechtevergabe*: Entfallen, da redundant zu ORP.4.A7 *Vergabe von Zugriffsrechten.*
- NET.3.2.A11 *Einspielen von Updates und Patches:* Entfallen, da redundant zu den Anforderungen des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement*.
- NET.3.2.A12 *Vorgehen bei Sicherheitsvorfällen:* Entfallen, da redundant zu DER.2.1.A2 *Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen* und DER.2.1.A3 *Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen*.
- NET.3.2.A13 *Regelmäßige Datensicherung:* Entfallen, da redundant zu den Anforderungen des Bausteins CON.3 *Datensicherungskonzept*.

Änderungsdokument zum Baustein: NET.3.3 VPN

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel wurde um Bausteine ergänzt, in denen das Thema VPN ebenfalls zu betrachten ist. Dafür wurden die entsprechenden, nicht bausteinspezifischen Anforderungen im Baustein entfernt.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Probleme bei der lokalen Speicherung der Authentisierungsdaten für VPNs* wurde entfernt, da sie nicht in die Abgrenzung des Bausteins passt.
- Die Gefährdung *Diebstahl von mobilen Endgeräten mit VPN-Client* wurde entfernt, da sie nicht in die Abgrenzung des Bausteins passt.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.3.3.A2 *Auswahl eines VPN-Dienstleisters*: Sprachliche Schärfung der Anforderung.
- NET.3.3.A3 *Sichere Installation von VPN-Endgeräten*: Entfernung redundanter Teilanforderung zur Härtung von Betriebssystemen. Die entsprechenden Anforderungen sind den betriebssystemspezifischen Bausteinen der Schicht SYS zu entnehmen.
- NET.3.3.A11 *Sichere Anbindung eines externen Netzes*: Teilanforderungen zu Verschlüsselung und Schlüsselmanagement entfernt, die redundant zu ORP.4.A9 *Identifikation und Authentisierung*, CON.1.A3 *Verschlüsselung der Kommunikationsverbindungen*, CON.1.A1 *Auswahl geeigneter kryptografischer Verfahren* und CON.1.A4 *Geeignetes Schlüsselmanagement* sind.
- NET.3.3.A12 *Benutzer- und Zugriffsverwaltung bei Fernzugriff-VPNs*: Entfernung redundanter Teilanforderungen zu Authentisierung und Benutzermanagement, da diese übergeordnet im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* behandelt werden.
- NET.3.3.A13 *Integration von VPN-Komponenten in eine Firewall*: Sprachliche Schärfung der Anforderung.

Änderungsdokument zum Baustein: NET.4.1 TK-Anlagen

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel wurde um Bausteine ergänzt, in denen das Thema TK-Anlagen ebenfalls zu betrachten ist.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.4.1.A7 *Aufstellung der TK-Anlage*: Umbenannt in *Geeignete Aufstellung der TK-Anlage* analog zu den anderen Bausteinen des IT-Grundschutz-Kompendiums.
- NET.4.1.A16 *Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen:* Vereinheitlicht in *Sicherung von Endgeräten in frei zugänglichen Räumen.*
- NET.4.1.A17 *Wartung von TK-Anlagen*: Nicht spezifische Teilanforderung zu Zugängen entfernt, da redundant zu OPS.1.2.5.A3 *Absicherung der Schnittstellen zur Fernwartung*.

Entfernung von Anforderungen

- NET.4.1.A3 *Änderung voreingestellter Passwörter*: Diese Anforderung ist bereits durch die Anforderung ORP.4.A23 *Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme* im übergreifenden Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt.
- NET.4.1.A4 *Absicherung von Remote-Zugängen*: Diese Anforderung ist bereits durch die entsprechenden Anforderungen an Remote-Zugänge im übergeordneten Baustein OPS.1.2.5 *Fernwartung* abgedeckt.

Änderungsdokument zum Baustein: NET.4.2 VoIP

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel wurde um Bausteine ergänzt, in denen das Thema VoIP ebenfalls zu betrachten ist.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.4.2.A3 *Sichere Administration und Konfiguration von VoIP-Endgeräten*: Teilanforderung zum regelmäßigen Einspielen von Updates und Patches entfallen. Dies wird im Rahmen des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* übergreifend behandelt.
- NET.4.2.A5 *Sichere Konfiguration der VoIP-Middleware*: Die Teilanforderung "Es SOLLTE eine Regelung zur restriktiven Anmeldung von Geräten und Benutzern erstellt werden." ist bereits durch die Anforderung ORP.4.A7 V*ergabe von Zugriffsrechten* im übergreifenden Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt.

Entfernung von Anforderungen

- NET.4.2.A2 *Sichere Administration der VoIP-Middleware*: Diese Anforderung ist bereits durch die Anforderungen ORP.4.A12 *Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen* und OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement* abgedeckt.

- NET.4.2.A6 *Protokollierung bei VoIP*: Entfallen, da die Protokollierung im Baustein OPS.1.1.5 *Protokollierung* übergeordnet behandelt wird. Die Auswertung der Protokolldaten findet sich außerdem in DER.1.A6 *Kontinuierliche Überwachung und Auswertung von Protokolldaten.*

- NET.4.2.A10 *Schulung der Administratoren für die Nutzung von VoIP*: Diese Anforderung ist bereits durch die Anforderungen OPS.1.1.2.A10 *Fortbildung und Information* im übergreifenden Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* abgedeckt.

INF: Infrastruktur Änderunsgdokumente

Änderungsdokument zum Baustein: INF.1 Allgemeines Gebäude

Kapitel 2: Gefährdungslage

- Die Gefährdung *Umfeld-Gefährdungen* wurde geschärft.

Kapitel 3: Anforderungen

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.A4. *Branderkennung in Gebäuden:* Der Aspekt der regelmäßigen Kontrolle der Fluchtwege wurde in INF.1.A3 *Einhaltung von Brandschutzvorschriften verschoben.*
- 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.
- 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 Anforderungtitel wurde um die Einschränkung „frühzeitig“ gekürzt.
- INF.1.A23 *Bildung von Sicherheitszonen*: Die Teilanforderung zur Entwicklung und Dokumentation eines Sicherheitskonzeptes wurde gestrichen, da redundant zu INF.1.A9 *Sicherheitskonzept für die Gebäudenutzung.*
- 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.

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).

Entfernung von Anforderungen

- INF.1.A11 *Abgeschlossene Türen*: Entfallen, da redundant zu INF.7.A2 *Geschlossene Fenster und abgeschlossene Türen.*

Änderungsdokument zu den Bausteinen: 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.