Bundesamt
für Sicherheit in der
Informationstechnik

Änderungen in der Edition 2021 des IT-Grundschutz-Kompendiums

Inhaltsverzeichnis

Einleitung 4

Umbenannte und verschobene Bausteinen 5

Anpassung der Rollen 6

ISMS: Sicherheitsmanagement Änderungsdokumente 8
Änderungsdokument zum Baustein: ISMS.1 Sicherheitsmanagement 9

ORP: Organisation und Personal Änderungsdokumente 10
Änderungsdokument zum Baustein: ORP.1 Organisation 11
Änderungsdokument zum Baustein: ORP.2 Personal 13
Änderungsdokument zum Baustein: ORP.3 Sensibilisierung und Schulung zur Informationssicherheit 15
Änderungsdokument zum Baustein: ORP.4 Identitäts- und Berechtigungsmanagement 16
Änderungsdokument zum Baustein: ORP.5 Compliance Management (Anforderungsmanagement) 17

CON: Konzeption und Vorgehensweise Änderunsgdokumente 18
Änderungsdokument zum Baustein: CON.1 Kryptokonzept 19
Änderungsdokument zum Baustein: CON.3 Datensicherungskonzept 20
Änderungsdokument zum Baustein: CON.6 Löschen und Vernichten 21
Änderungsdokument zum Baustein: CON.7 Informationssicherheit auf Auslandsreisen 23
Änderungsdokument zum Baustein: CON.8 Software-Entwicklung 24
Änderungsdokument zum Baustein: CON.9 Informationsaustausch 26

OPS: Betrieb Änderunsgdokumente 27
Änderungsdokument zum Baustein: OPS.1.1.2 Ordnungsgemäße IT-Administration 28
Änderungsdokument zum Baustein: OPS.1.1.3 Patch- und Änderungsmanagement 29
Änderungsdokument zum Baustein: OPS.1.1.4 Schutz vor Schadprogrammen 31
Änderungsdokument zum Baustein: OPS.1.1.5 Protokollierung 32
Änderungsdokument zum Baustein: OPS.1.1.6 Software-Tests und -Freigaben 33
Änderungsdokument zum Baustein: OPS.1.2.4 Telearbeit 34
Änderungsdokument zum Baustein: OPS.1.2.5 Fernwartung 35
Änderungsdokument zum Baustein: OPS.2.2 Cloud-Nutzung 36

DER: Detektion und Reaktion Änderunsgdokumente 37
Änderungsdokument zum Baustein: DER.1 Detektion von sicherheitsrelevanten Ereignissen 38
Änderungsdokument zum Baustein: DER.2.1 Behandlung von Sicherheitsvorfällen 39
Änderungsdokument zum Baustein: DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle 40
Änderungsdokument zum Baustein: DER.3.1 Audits und Revisionen 41
Änderungsdokument zum Baustein: DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision 42

APP: Anwendungen Änderunsgdokumente 43
Änderungsdokument zum Baustein: APP.1.1 Office-Produkte 44
Änderungsdokument zum Baustein: APP.1.2 Webbrowser 46
Änderungsdokument zum Baustein: APP.1.4 Mobile Anwendungen (Apps) 47
Änderungsdokument zum Baustein: APP.2.1. Allgemeiner Verzeichnisdienst 49
Änderungsdokument zum Baustein: APP.2.2 Active Directory 50
Änderungsdokument zum Baustein: APP.2.3 OpenLDAP 51
Änderungsdokument zum Baustein: APP.3.1 Webanwendungen 52
Änderungsdokument zum Baustein: APP.3.2 Webserver 54
Änderungsdokument zum Baustein: APP.3.3 Fileserver 55
Änderungsdokument zum Baustein: APP.3.4 Samba 56
Änderungsdokument zum Baustein: APP.3.6 DNS-Server 57
Änderungsdokument zum Baustein: APP.4.2 SAP-ERP-System 58
Änderungsdokument zum Baustein: APP.4.3 Relationale Datenbanken 59

Änderungsdokument zum Baustein: APP.4.6 SAP ABAP-Programmierung....60
Änderungsdokument zum Baustein: APP.5.2 Microsoft Exchange und Outlook....61
Änderungsdokument zum Baustein: APP.7 Entwicklung von Individualsoftware....62

SYS: IT-Systeme Änderunsgdokumente 64
Änderungsdokument zum Baustein: SYS.1.1 Allgemeiner Server....65
Änderungsdokument zum Baustein: SYS.1.2.2 Windows Server 2012....67
Änderungsdokument zum Baustein: SYS.1.3 Server unter Linux und Unix....68
Änderungsdokument zum Baustein: SYS.1.5 Virtualisierung....69
Änderungsdokument zum Baustein: SYS.1.7 IBM Z-System....70
Änderungsdokument zum Baustein: SYS.1.8 Speicherlösungen....71
Änderungsdokument zum Baustein: SYS.2.1 Allgemeiner Client....73
Änderungsdokument zum Baustein: SYS.2.2.2 Clients unter Windows 8.1....75
Änderungsdokument zum Baustein: SYS.2.2.3 Clients unter Windows 10....76
Änderungsdokument zum Baustein: SYS.2.3 Clients unter Linux und Unix....77
Änderungsdokument zum Baustein: SYS.2.4 Clients unter macOS....78
Änderungsdokument zum Baustein: SYS.3.1 Laptops....79
Änderungsdokument zum Baustein: SYS.3.2.1 Allgemeine Smartphones und Tablets....80
Änderungsdokument zum Baustein: SYS.3.2.2 Mobile Device Management....82
Änderungsdokument zum Baustein: SYS.3.2.3 iOS (for Enterprise)....84
Änderungsdokument zum Baustein: SYS.3.2.4 Android....85
Änderungsdokument zum Baustein: SYS.3.3 Mobiltelefon....86
Änderungsdokument zum Baustein: SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte....87
Änderungsdokument zum Baustein: SYS.4.3 Eingebettete Systeme....88
Änderungsdokument zum Baustein: SYS.4.4 Allgemeines IoT-Gerät....89
Änderungsdokument zum Baustein: SYS.4.5 Wechseldatenträger....90

IND: Industrielle IT Änderunsgdokumente 91
Änderungsdokument zum Baustein: IND.1 Prozessleit- und Automatisierungstechnik....92
Änderungsdokument zum Baustein: IND.2.1 Allgemeine ICS-Komponente....94
Änderungsdokument zum Baustein: IND.2.2 Speicherprogrammierbare Steuerung (SPS)....96
Änderungsdokument zum Baustein: IND.2.7 Safety Instrumented Systems....97

NET: Netze und Kommunikation Änderunsgdokumente 98
Änderungsdokument zum Baustein: NET.1.1 Netzarchitektur und -design....99
Änderungsdokument zum Baustein: NET.1.2 Netzmanagement....100
Änderungsdokument zum Baustein: NET.2.1 WLAN-Betrieb....102
Änderungsdokument zum Baustein: NET.2.2 WLAN-Nutzung....103
Änderungsdokument zum Baustein: NET.3.1 Router und Switches....104
Änderungsdokument zum Baustein: NET.3.2 Firewall....105
Änderungsdokument zum Baustein: NET.3.3 VPN....106
Änderungsdokument zum Baustein: NET.4.1 TK-Anlagen....107
Änderungsdokument zum Baustein: NET.4.2 VoIP....108

INF: Infrastruktur Änderunsgdokumente 109
Änderungsdokument zum Baustein: INF.1 Allgemeines Gebäude....110
Änderungsdokument zum Baustein: INF.2 Rechenzentrum sowie Serverraum....112
Änderungsdokument zum Baustein: INF.5 Raum sowie Schrank für technische Infrastruktur....114
Änderungsdokument zum Baustein: INF.7 Büroarbeitsplatz....115
Änderungsdokument zum Baustein: INF.8 Häuslicher Arbeitsplatz....116
Änderungsdokument zum Baustein: INF.9 Mobiler Arbeitsplatz....117
Änderungsdokument zum Baustein: INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume....118
Änderungsdokument zu den Bausteinen: INF.3 Elektrotechnische Verkabelung und INF.4 IT-Verkabelung; nun: INF.12 Verkabelung....119

Einleitung

Fast alle Bausteine der Edition 2020 wurden für die Edition 2021 fachlich überarbeitet. Dabei wurden vor allem Redundanzen bei den Anforderungen bausteinübergreifend aufgelöst, um die Bausteine zu vereinheitlichen und zu verschlanken.

Inhaltliche Änderungen, die Auswirkungen auf Zertifizierungsverfahren oder bestehende Sicherheitskonzepte haben können, sind ausführlich für die entsprechenden Bausteine im vorliegenden Dokument beschrieben.

Geringfügige sprachliche und redaktionelle Änderungen sowie Überarbeitungen aus Gründen der besseren Verständlichkeit werden nicht separat aufgeführt.

Eine weitere inhaltliche Anpassung ist im Bereich der Rollen erfolgt. Ihre Anzahl wurden für eine bessere Anwendbarkeit reduziert, indem Rollen zusammengefasst und verallgemeinert wurden. Details hierzu finden sich ebenfalls in diesem Dokument.

Umbenannte und verschobene Bausteine

Die folgenden IT-Grundschutz-Bausteine der Edition 2020 sind im Rahmen ihrer Überarbeitung umbenannt, zusammengefasst und/oder in eine andere Schicht verschoben worden:

Edition 2020	Edition 2021
APP.5.1 *Allgemeine Groupware*	APP.5.3 *Allgemeiner E-Mail-Client und -Server*
CON.4 *Auswahl und Einsatz von Standard-Software*	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*	
ORP.3 *Sensibilisierung und Schulung*	ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*

Anpassung der Rollen

Für das IT-Grundschutz-Kompendium 2021 wurden die Rollen, die für Zuständigkeiten in den Bausteinen verwendet werden, überarbeitet und vereinheitlicht. Dabei wurden spezielle Rollen durch allgemeinere, übergreifende Rollen ersetzt. Dies soll es den Anwendern erleichtern, Zuständigkeiten entsprechend der individuellen Möglichkeiten festzulegen. Zudem wurden viele „Leiter"-Rollen in die Rollenbezeichnung ihrer jeweiligen Organisationseinheit integriert, da der Leiter hier ohnehin stets die Verantwortung trägt.

Die Rollen sind als Empfehlungen und nicht als verbindliche Vorgabe zu verstehen.

Neu eingeführt wurden die folgenden Rollenbezeichnungen:

- Institution
- Zentrale Verwaltung
- OT-Leiter
- OT-Betrieb

Die folgenden Rollen wurden gemäß der Tabelle überführt:

Alte Rollenbezeichnung	Neue Rollenbezeichnung
Änderungsmanager	Fachverantwortlicher
Archivverwalter	
Ermittler	
Ermittlungsleiter	
Fax-Verantwortlicher	
TK-Anlagen-Verantwortlicher	
Beschaffer	Beschaffungsstelle
Leiter Beschaffung	
Betriebsleiter	OT-Leiter
Leiter Produktion und Fertigung	
Innerer Dienst	Zentrale Verwaltung
Leiter Organisation	
Leitstellen-Operator	Mitarbeiter
Telearbeiter	

Alte Rollenbezeichnung	Neue Rollenbezeichnung
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	Informationssicherheitsbeauftragter (ISB)

ISMS: Sicherheitsmanagement Änderungsdokumente

Änderungsdokument zum Baustein: ISMS.1 Sicherheitsmanagement

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- ISMS.1.A4 *Benennung eines Informationssicherheitsbeauftragten*: Qualifizierung des ISB wurde aus dieser Anforderung entfernt, da dieser Aspekt bereits durch die Anforderung ORP.2.A15 *Qualifikation des Personals* des Bausteins ORP.2 *Personal* abgedeckt ist.
- ISMS.1.A5 *Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten*: Qualifizierung des externen ISB wurde aus dieser Anforderung entfernt, da dieser Aspekt bereits durch die Anforderung ORP.2.A15 *Qualifikation des Personals* des Bausteins ORP.2 *Personal* abgedeckt ist.
- ISMS.1.A6 *Aufbau einer geeigneten Organisationsstruktur für Informationssicherhei*t: Die Anforderung wurde um den Aspekt der Definition und Zuweisung von Rollen erweitert.
- ISMS.1.A8 *Integration der Mitarbeiter in den Sicherheitsprozess*: Die Anforderung wurde um die Konsequenzen einer Verletzung von Sicherheitsvorgaben erweitert.
- ISMS.1.A10 *Erstellung eines Sicherheitskonzepts*: Information der Mitarbeiter wurde aus dieser Anforderung entfernt, da dieser Aspekt bereits durch die Anforderung ISMS.1.A8 *Integration der Mitarbeiter in den Sicherheitsprozess* abgedeckt ist. Eignung, Angemessenheit, Umsetzbarkeit und Effizienz der Maßnahmen wurden aus dieser Anforderung entfernt, da diese Aspekte bereits durch die Anforderung ISMS.1.A11 *Aufrechterhaltung der Informationssicherheit* abgedeckt sind.
- ISMS.1.A15 *Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit*: Bedarf an Ressourcen (einschl. separate Teilanforderung zum Thema Zeit für Sicherheitsaufgaben) wurde aus dieser Anforderung entfernt, da dieser Aspekt bereits durch ISMS.1.A4 *Benennung eines Informationssicherheitsbeauftragten* abgedeckt ist.
- ISMS.1.A16 *Erstellung von zielgruppengerechten Sicherheitsrichtlinien*: Information der Mitarbeiter wurde aus dieser Anforderung entfernt, da dieser Aspekt bereits durch die Anforderung ISMS.1.A8 *Integration der Mitarbeiter in den Sicherheitsprozess* abgedeckt ist.

Entfernung von Anforderungen

- ISMS.1.A14 *Sensibilisierung zur Informationssicherheit*: Die Vorgaben dieser Anforderung gehen nicht über die Vorgaben des Bausteins ORP.3 *Schulung und Sensibilisierung zur Informationssicherheit* hinaus.

ORP: Organisation und Personal Änderungsdokumente

Änderungsdokument zum Baustein: ORP.1 Organisation

Kapitel 2: Gefährdungslage

- Die Gefährdung *Unbefugter Zutritt zu schutzbedürftigen Räumen* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Unerlaubte Ausübung von Rechten* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Manipulation von Informationen und Geräten* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Zerstörung, Vandalismus und Sabotage* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Diebstahl und Verlust von Informationen und Geräten* wurde entfernt, da nicht weiter relevant für den Baustein.

Kapitel 3: Anforderungen

Neue Anforderungen

- ORP.1.A15 *Ansprechpartner zu Sicherheitsfragen* (Basis-Anforderung)
- ORP.1.A16 *Mitarbeiterrichtlinie zur sicheren IT-Nutzung* (Standard-Anforderung)

Änderungen an 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.A13 *Sicherheit bei Umzügen*: Es ist eine Teilanforderung zur Zutrittskontrolle entfallen, da im übergreifenden Baustein INF.1 *Allgemeines Gebäude* abgedeckt.
- ORP.1.A16 *Richtlinie zur sicheren IT-Nutzung*: Die zeitliche Vorgabe für die Aktualisierung der Richtlinie wurde auf "regelmäßig" angepasst.

Entfernung von Anforderungen

- ORP.1.A5 *Vergabe von Berechtigungen*: Diese Anforderung ist bereits durch die Anforderungen ORP.4.A5 *Vergabe von Zutrittsberechtigungen,* ORP.4.A6 *Vergabe von Zugangsberechtigungen* und ORP.4.A7 *Vergabe von Zugriffsrechten* im übergreifenden Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt.
- ORP.1.A6 *Schutz von sensiblen Informationen am Arbeitsplatz*: Diese Anforderung ist bereits durch die Anforderung INF.7.A6 *Aufgeräumter Arbeitsplatz* im übergreifenden Baustein INF.7 *Büroarbeitsplatz* abgedeckt.
- ORP.1.A7 *Geräteverwaltung* ist entfallen, da Anforderung in ORP.1.A8 *Betriebsmittelverwaltung* inkludiert wurde.
- ORP.1.A10 *Reaktion auf Verletzungen der Sicherheitsvorgaben* ist entfallen, da die Anforderung im Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* abgedeckt ist.
- ORP.1.A11 *Rechtzeitige Beteiligung der Personalvertretung* ist entfallen, da dies kein Thema der Informationssicherheit ist.

- ORP.1.A12 *Regelungen für Wartungs- und Reparaturarbeiten* ist entfallen, da die Anforderung bereits durch die gleichnamige Anforderung OPS.1.1.2.A12 im Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* abgedeckt ist.
- ORP.1.A14 *Kontrollgänge* ist entfallen, da im übergreifenden Baustein INF.1 *Allgemeines Gebäude (INF.1.A6 Geschlossene Fenster und Türen und INF.1.A7 Zutrittsregelung und -kontrolle)* abgedeckt.

Änderungsdokument zum Baustein: ORP.2 Personal

Kapitel 2: Gefährdungslage

- Die Gefährdung *Missbrauch von Berechtigungen* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Sorglosigkeit im Umgang mit Informationen* wurde um die Aspekte „Unberechtigte Verwendung eigener IT-Systeme“ , „Missbrauch sozialer Netzwerke“ und „Manipulation oder Zerstörung von Geräten, Informationen oder Software“ gekürzt.
- Die Gefährdung *Social Engineering* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Unberechtigte Verwendung eigener IT-Systeme* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Missbrauch sozialer Netzwerke* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Manipulation oder Zerstörung von Geräten, Informationen oder Software* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Unzureichende Qualifikationen der Mitarbeiter* wurde hinzugefügt.

Kapitel 3: Anforderungen

Neue Anforderungen

- ORP.2.A14 *Aufgaben und Zuständigkeiten von Mitarbeitern*: Neue Basisanforderung.
- ORP.2.A15 *Auswahl von Personal nach Qualifikation*: Neue Basisanforderung.

Änderungen an bestehenden Anforderungen

- ORP.2.A1 *Geregelte Einarbeitung neuer Mitarbeiter*: Die Anforderungen zu Regelungen im Sicherheitsprozess wurden entfernt, da beschrieben in der ORP.2.A14 *Aufgaben und Zuständigkeiten von Mitarbeitern.*
- 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.

Entfernung von Anforderungen

- ORP.2.A6 *Überprüfung von Kandidaten bei der Auswahl von Personal*: Die Teilanforderung zur Vermeidung von Interessenkonflikte beim Stellenwechsel wurde in die Basis-Anforderung ORP.2.A2 *Geregelte Verfahrensweise beim Weggang von Mitarbeitern* überführt. Die Teilanforderung zu erforderlichen Qualifikationen wurde in die neue Basis-Anforderung ORP.2.A15 *Qualifikation bei der Auswahl von Personal* überführt.
- ORP.2.A8 *Aufgaben und Zuständigkeiten von Mitarbeitern*: Die Aspekte dieser Anforderung wurden verschoben in die neue Basisanforderung ORP.2.A14 *Qualifikation bei der Auswahl von Personal.*
- ORP.2.A9 *Schulung von Mitarbeitern*: Die Anforderung ist entfallen, da redundant zum Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit.*
- ORP.2.*A10 Vermeidung von Störungen des Betriebsklimas:* Dies ist kein Thema der Informationssicherheit.
- ORP.2.A11 *Analyse der Sicherheitskultur*: Diese Anforderung wurde verschoben nach ORP.1.A16 *Richtlinie zur sicheren IT-Nutzung.*

- ORP.2.A12 *Benennung einer Vertrauensperson*: Diese Anforderung wurde entfernt, da der Bezug zur Informationssicherheit fehlt.

Änderungsdokument zum Baustein: ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

Der Baustein ORP.3 *Sensibilisierung und Schulung* wurde umbenannt in ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit.*

Kapitel 3: Anforderungen

Änderungen an 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 Informationssicherhei*t. 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.* Der Aspekt zur zielgruppenorientierten Schulung wurde entfernt, da redundant zu ORP.3.A4 *Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit*. Die Teilanforderung zum regelmäßigen Austausch des ISB mit der Personalabteilung wurde verschoben in ORP.3.A8 *Messung und Auswertung des Lernerfolgs.*
- ORP.3.A8 *Messung und Auswertung des Lernerfolgs*: Die Anforderung wurde um den regelmäßigen Austausch des ISB mit der Personalabteilung erweitert.

Entfernung von Anforderungen

- ORP.3.A2 *Ansprechpartner zu Sicherheitsfragen*: Entfallen, da redundant zu ORP.1.A15 *Ansprechpartner zu Informationssicherheitsfragen*.
- ORP.3.A5 *Analyse der Zielgruppen für Sensibilisierungs- und Schulungsprogramme*: Entfallen und mit ORP.3.A4 *Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit* zusammengefasst.

Kapitel 4: Weiterführende Informationen

- Ergänzung der BSI-Schulungen zum IT-Grundschutz-Praktiker und IT-Grundschutz-Berater.

Änderungsdokument zum Baustein: ORP.4 Identitäts- und Berechtigungsmanagement

Kapitel 3: Anforderungen

Neue Anforderungen

- ORP.4.A24 *Vier-Augen-Prinzip für administrative Tätigkeiten:* Diese Anforderung wurde neu in den Baustein aufgenommen.

Änderungen an 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 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen:* Umbenennung zu ORP.4.A2 *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.
- 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.

Änderungsdokument zum Baustein: ORP.5 Compliance Management (Anforderungsmanagement)

Kapitel 1.3: Abgrenzung und Modellierung

- Sprachliche Schärfung, der Begriff "strukturellen Vorgaben" wurde durch "sonstige Vorgaben" ersetzt, der auch interne Richtlinien mit einbezieht.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- ORP.5.A1 *Identifikation der Rahmenbedingungen*: Schärfung des Titels, Aspekte des Aufbaus eines Prozesses aus der Basis-Anforderung entfernt und in ORP.5.A4 *Konzeption und Organisation des Compliance Managements* aufgenommen. 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.

Entfernung von Anforderungen

- ORP.5.A3 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*: Entfallen, da redundant zu ORP.2.A14 *Aufgaben und Zuständigkeiten von Mitarbeitern* in Baustein ORP.2 *Personal.*
- ORP.5.A6 *Einweisung des Personals in den sicheren Umgang mit IT*: Entfallen, da redundant zu ORP.3 *Sensibilisierung und Schulung.*

CON: Konzeption und Vorgehensweise Änderunsgdokumente

Änderungsdokument zum Baustein: CON.1 Kryptokonzept

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

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

Änderungsdokument zum Baustein: CON.3 Datensicherungskonzept

Kapitel 3: Anforderungen

Änderungen an 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.

Änderungsdokument zum Baustein: CON.6 Löschen und Vernichten

Kapitel 1.3: Abgrenzung und Modellierung

- Entfernung des Verweises auf spezifische Anforderungen zum Löschen und Vernichten in einzelnen Bausteinen, da diese im Zuge der Redundanzreduzierung in diesem Baustein gesammelt worden sind.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlende oder unzureichend dokumentierte Regelungen beim Löschen und Vernichten* wurde um konkrete Beispiele ergänzt.
- Die Gefährdungen *Vertraulichkeitsverlust durch Restinformationen auf Datenträgern* und *Verlust der Vertraulichkeit durch Auslagerungs- und temporäre Dateien* wurden aufgrund inhaltlicher Überschneidungen zusammengefasst.
- Die Gefährdung *Unstrukturierte Datenhaltung* wurde entfernt, da die Gefährdung nicht Gegenstand des Geltungsbereichs dieses Bausteins ist.
- Die Gefährdung *Ungeeignete Entsorgung der Datenträger und Dokumente* wurde aufgrund redundanter Inhalte zu den weiteren Gefährdungen entfernt.
- Die Gefährdung *Ungeeignete Einbindung externer Dienstleister in das Löschen und Vernichten* wurde neu hinzugefügt.
- Die Gefährdung *Ungeeigneter Umgang mit defekten Datenträgern oder IT-Geräten* wurde neu hinzugefügt.

Kapitel 3: Anforderungen

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 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.
- 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.*

Entfernung von Anforderungen

- CON.6.A3 *Löschen der Datenträger vor und nach dem Austausch:* Diese Anforderung ist entfallen, da sich nicht in den Geltungsbereich des Bausteins fällt und bereits hinreichend von OPS.1.1.2.A12 *Regelungen für Wartungs- und Reparaturarbeiten* behandelt wird.

- CON.6.A5 *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern*: Diese Anforderung ist entfallen, da sich nicht in den Geltungsbereich des Bausteins fällt und bereits hinreichend von OPS.1.1.2.A12 *Regelungen für Wartungs- und Reparaturarbeiten* behandelt wird.
- CON.6.A7 *Beseitigung von Restinformationen*: Die Anforderung wurde entfernt, da diese Aspekte durch den Baustein CON.9 *Informationsaustausch* geregelt werden.
- CON.6.A6 *Einweisung aller Mitarbeiter in die Methoden zur Löschung oder Vernichtung von Informationen*: Die Inhalte dieser Anforderung werden bereits durch CON.6.A8 *Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen* abgedeckt.
- CON.6.A9 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern bei erhöhtem Schutzbedarf*: Inhalte dieser Anforderung werden durch die neue Anforderung CON.6.A12 *Mindestanforderungen an Verfahren zur Löschung und Vernichtung* und die bestehende Anforderung CON.6.A4 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern* abgedeckt.
- CON.6.A10 *Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten:* Entfernung der Anforderung, da hier keine spezifischen Anforderungen an das Löschen oder Vernichten definiert werden.

Änderungsdokument zum Baustein: CON.7 Informationssicherheit auf Auslandsreisen

Umsortierung von Anforderungen

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

Änderungsdokument zum Baustein: CON.8 Software-Entwicklung

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung der Abgrenzung gegenüber dem Baustein APP.7 *Entwicklung von Individualsoftware*.
- Ergänzung von Modellierungshinweisen zu den angrenzenden Bausteinen ORP.5 *Compliance Management*, OPS.2.1 *Outsourcing für Kunden* und CON.1 *Kryptokonzept*.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Auswahl eines ungeeigneten Vorgehensmodells* wurde um weitere Aspekte der Informationssicherheit ergänzt.
- Die Gefährdung *Unzureichend gesicherter Einsatz von Entwicklungsumgebungen* wurde um Aspekte zum Datenverlust ergänzt.
- Die Gefährdung *Software-Konzeptionsfehler* wurde um Aspekte der Software-Architektur ergänzt.
- Die Gefährdung *Fehlendes oder unzureichendes Test- und Freigabeverfahren* wurde um den Aspekt fehlender Tests von Sicherheitsanforderung ergänzt.
- Die Gefährdung *Softwaretest mit Produktivdaten wurde neu strukturier*t, um besser zwischen den einzelnen Gefährdungen in diesem Kontext zu differenzieren.

Kapitel 3: Anforderungen

Neue Anforderungen

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

Änderungen an 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 *Verwendung von Bibliotheken aus vertrauenswürdigen Quellen*: 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 *Anwendung von Testverfahren*: Umbenennung in *Durchführung von entwicklungsbegleitenden Softwaretests* zur besseren Abgrenzung zu Softwaretests im Rahmen der Abnahme. Ergänzung der Anforderung hinsichtlich der Trennung der unterschiedlichen Umgebungen. Die automatische statische Code-Analyse wurde von einer MUSS zu einer SOLLTE-Anforderung geändert.
- 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.A17 *Auswahl vertrauenswürdiger Entwicklungswerkzeuge*: Entfernung der Aspekte zum Manipulationsschutz, da dieser redundant mit den Anforderungen CON.8.A18 *Regelmäßige Sicherheitsaudits für die Entwicklungsumgebung* und CON.8.A19 *Regelmäßige Integritätsprüfung der Entwicklungsumgebung* ist.

- CON.8.A20 *Überprüfung von externen Komponenten:* Präzisierung der Anforderung und Ergänzung von Aspekten zur Integritätsprüfung.

Entfernung von Anforderungen

- CON.8.A4 *Einhaltung des Vorgehensmodells:* Entfernt. Die Inhalte wurden nach CON.8.A2 *Auswahl eines Vorgehensmodells* und CON.8.A7 *Durchführung von entwicklungsbegleitenden Software-Tests* verschoben. Verschiebung der Inhalte zu externen Komponenten in die Anforderung CON.8.A6 *Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen.*
- CON.8.A9 *Berücksichtigung von Compliance-Anforderungen*: Compliance-Anforderungen werden über die Anwendung des Bausteins ORP.5 *Compliance Management* berücksichtigt.
- CON.8.A13 *Beschaffung von Werkzeugen*: Diese Anforderung ist entfallen, da sie bereits durch den immer anzuwendenden Baustein APP.6 *Allgemeine Software* abgedeckt wird.
- CON.8.A15 *Sicherer Einsatz der Test- und Entwicklungsumgebungen*: Die Inhalte der Anforderung sind in die zutreffenderen Anforderungen CON.8.A7 *Durchführung von entwicklungsbegleitenden Softwaretest* sowie CON.8.A5 *Sicheres Systemdesign* verschoben worden.

Kapitel 4: Weiterführende Informationen

- Ergänzung von Hinweisen zum Thema Bedrohungsmodellierung.

Änderungsdokument zum Baustein: CON.9 Informationsaustausch

Kapitel 2: Gefährdungslage

- Die Gefährdung *Schadprogramme in übertragenen Dateien* wurde entfernt.

Kapitel 3: Anforderungen

Neue Anforderungen

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

OPS: Betrieb Änderunsgdokumente

Änderungsdokument zum Baustein: OPS.1.1.2 Ordnungsgemäße IT-Administration

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung in den Formulierungen zur Modellierung.
- Ergänzung des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* in der Abgrenzung.

Kapitel 3: Anforderungen

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 bestehenden Anforderungen

- OPS.1.1.2.A2 *Vertretungsregelungen und Notfallvorsorge:* Teilanforderung zur Schaffung von Vertretungsregelungen gestrichen, da dies bereits durch die Anforderung ORP.2.A3 *Festlegung von Vertretungsregelungen* im Baustein ORP.2 *Personal* abgedeckt ist.
- OPS.1.1.2.A3 *Geregelte Einstellung von IT-Administratoren:* Teilanforderung über Regelungen beim Betrieb durch Dritte entfernt, da dies bereits durch den Baustein OPS.2.1 *Outsourcing für Kunden* ausführlich behandelt wird. Weitere Teilanforderung zur Verpflichtung der Einhaltung von Gesetzen entfernt, da dies bereits durch ORP.2.A14 *Aufgaben und Zuständigkeiten von Mitarbeitern* im Baustein ORP.2 *Personal* behandelt wird.
- OPS.1.1.2.A4 *Beendigung der Tätigkeit als IT-Administrator:* Teilanforderung über Regelungen beim Betrieb durch Dritte entfernt, da dies bereits durch den Baustein OPS.2.1 *Outsourcing für Kunden* ausführlich behandelt wird. Teilanforderung über die Zurückgabe von ausgehändigten Geräten und Zugangsmitteln entfernt, da dies bereits durch ORP.2.A2 *Geregelte Verfahrensweise beim Weggang von Mitarbeitern* im Baustein ORP.2 *Personal* abgedeckt ist.
- OPS.1.1.2.A6 *Schutz administrativer Tätigkeiten:* Die Anforderung wurde um die Aspekte Zugriff auf administrative Schnittstellen, Administrationsnetz und sichere Protokolle ergänzt. Die Teilanforderung der Nutzung verschiedener Passwörter wurde gestrichen, da dies bereits durch die Anforderung ORP.4.A8 *Regelung des Passwortgebrauchs* im Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* abgedeckt ist.
- OPS.1.1.2.A10 *Fortbildung und Information:* Ergänzung von Anwendungen in der Aufzählung zu den Themen, über die sich Administratoren regelmäßig informieren sollten.
- OPS.1.1.2.A12 *Regelungen für Wartungs- und Reparaturarbeiten:* Die Teilanforderung zum Aspekt der Beaufsichtigung von Wartungspersonal wurde entfernt, da dies bereits durch die Anforderung ORP.1.A3 *Beaufsichtigung oder Begleitung von Fremdpersonen* im Baustein ORP.1 *Organisation* abgedeckt ist.

Entfernung von Anforderungen

- OPR.1.1.2.A1 *Personalauswahl für administrative Tätigkeiten*: Diese Anforderung ist bereits durch die Anforderung ORP.2.A15 *Qualifikation des Personals* im Baustein ORP.2 *Personal* sowie ORP.1.A4 *Funktionstrennung zwischen unvereinbaren Aufgaben* im BausteinORP.1 *Organisation* abgedeckt.

Änderungsdokument zum Baustein: OPS.1.1.3 Patch- und Änderungsmanagement

Kapitel 1.3: Abgrenzung und Modellierung

- Bessere Abgrenzung gegenüber dem Änderungsmanagement in ITIL.
- Klare Abgrenzung gegenüber dem Baustein *OPS.1.1.6 Software-Tests und -Freigaben*.

Kapitel 2: Gefährdungslage

- Mangelhafte Berücksichtigung von mobilen Endgeräten: Wegen Redundanzen mit Bausteinen der Schicht SYS gestrichen.

Kapitel 3: Anforderungen

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 und Updates sowie der Umgang damit.

Änderungen an bestehenden Anforderungen

- OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement:* Formulierung geschärft und Klassifizierung/Bewertung der Patches in OPS.1.1.3.A15 *Regelmäßige Aktualisierung von IT-Systemen und Software* verschoben.
- OPS.1.1.3.A2 *Festlegung der Zuständigkeiten:* Die Rolle Änderungsmanager wurde durch den Fachverantwortlichen für das Patch- und Änderungsmanagement ersetzt. Daher entfällt die Benennung hier. Zusätzlich sind Qualifikationen in ORP.2.A15 *Qualifikation des Personals* geregelt und müssen hier nicht wiederholt werden. Im Zuge der klareren Trennung zwischen Zuständigen und Verantwortlichen ist die Anforderung inklusive Titel hier begrifflich geschärft worden.
- 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.
- 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 (siehe Abgrenzung und OPS.1.1.3.A15 *Regelmäßige Aktualisierung von IT-Systemen und Software*). 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.

Entfernung von Anforderungen

- OPS.1.1.3.A4: *Planung des Änderungsmanagementprozesses:* Entfallen, da der Fokus dieses Baustein mehr auf Patchmanagement gelegt wurde und das Änderungsmanagement hier nur in Bezug auf Informationssicherheit betrachtet wird. Siehe auch Änderungen zur Abgrenzung.

Kapitel 4: Weiterführende Informationen

- Hinweis auf das Change Management aus ITIL ergänzt.

Änderungsdokument zum Baustein: OPS.1.1.4 Schutz vor Schadprogrammen

Kapitel 1.3: Abgrenzung und Modellierung

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

Kapitel 2: Gefährdungslage

- *Infektionen durch mobile Datenträger und andere USB-Geräte*: Entfernt, da bereits im Baustein SYS.4.5 *Wechseldatenträger* behandelt.

Kapitel 3: Anforderungen

Änderungen an 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*: Sprachliche Anpassungen der Anforderungen zur Nutzung von Cloud-Funktionen. 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 zur Deaktivierung durch die Benutzer aufgenommen.
- OPS.1.1.4.A6 *Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen*: Anforderungen entfernt, die redundant zu den Anforderungen des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* sind. Verweis auf zeitnahes Einspielen aufgenommen.
- 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 in OPS.1.1.4.A7 *Sensibilisierung und Verpflichtung der Benutzer* verschoben.

Entfernung von Anforderungen

- OPS.1.1.4.A4 *Auswahl eines Virenschutzprogrammes für Gateways und IT-Systeme zum Datenaustausch*: Die Anforderung ist in OPS.1.1.4.A3 *Auswahl eines Virenschutzprogrammes* mit aufgegangen.
- OPS.1.1.4.A8 *Nutzung von Cloud-Diensten zur Detektionsverbesserung*: Entfallen da redundant zu OPS.1.1.4.A3 *Auswahl eines Virenschutzprogrammes.*
- OPS.1.1.4.A15 *Externer Beratung zum Schutz vor Schadprogrammen*: Entfallen, da nicht bausteinspezifisch.

Änderungsdokument zum Baustein: OPS.1.1.5 Protokollierung

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung um die Aspekte Definition sowie Zuweisung von Kompetenzen und Zuständigkeit im Vorfeld der Protokollierung von sicherheitsrelevanten Ereignissen.
- Ergänzung der Abgrenzung um den Aspekt Auswertung von Protokollierungsdaten im Rahmen der Detektion von sicherheitsrelevanten Ereignissen.

Kapitel 3: Anforderungen

Änderungen an 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 Protokolierungsdaten 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.

Entfernung von Anforderungen

- OPS.1.1.5.A2 *Festlegung von Rollen und Verantwortlichkeiten:* Diese Anforderung ist bereits durch die Anforderung ORP.1.A1 *Festlegung von Verantwortlichkeiten und Regelungen* im Baustein ORP.1 *Organisation* abgedeckt.
- OPS.1.1.5.A7 *Sichere Administration von Protokollierungsservern:* Der Aspekt "Out-of-Band-Management" ist bereits durch die Anforderung NET.1.1.A21 *Separierung des Management-Bereichs* im Baustein NET.1.1 *Netzarchitektur und -design* abgedeckt. Der Aspekt Zugriffskontrolle auf den Protokollierungsserver ist bereits durch die Anforderung ORP.4.A7 *Vergabe von Zugriffsrechten* im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt.

Änderungsdokument zum Baustein: OPS.1.1.6 Software-Tests und -Freigaben

Übergreifende Anpassungen

- Aktualisierung der Rollen an das überarbeitete Rollenkonzept
- Anpassung von OPS.1.1.6 *Software-Tests und -Freigaben* an die Neugestaltung von APP.6 *Allgemeine Software*.

Kapitel 3: Anforderungen

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 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.
- 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.

Entfernung von Anforderungen

- OPS.1.1.6.A8 *Fort- und Weiterbildung der Software-Tester*: Entfallen, da diese Anforderung nur auf ORP.3 *Sensibilisierung und Schulung* verwiesen hat und die Aspekte zum Prozess zur regelmäßigen Schulung der Tester bereits durch ORP.2.A9 *Schulung von Mitarbeitern* behandelt werden.
- OPS.1.1.6.A9 *Beschaffung von Test-Software:* Entfallen, da redundant zu den Anforderungen des immer anzuwendenden Bausteins APP.6 *Allgemeine Software*.

Änderungsdokument zum Baustein: OPS.1.2.4 Telearbeit

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlende oder unzureichende Schulung der Mitarbeiter* wurde entfernt, da nicht weiter relevant für den Baustein.
- Die Gefährdung *Unzureichende Vertretungsregelungen für Telearbeit* wurde entfernt, da nicht weiter relevant für den Baustein.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- OPS.1.2.4.A1 *Regelungen für Telearbeit*: Aspekte zu Vertretungsregelungen entfernt, da redundant zu ORP.2.A3 *Festlegung von* Vertretungsregelungen im Baustein ORP.2 *Personal*.
- OPS.1.2.4.A2 *Sicherheitstechnische Anforderungen an den Telearbeitsrechner*: Nichtspezifische Teilanforderungen entfernt, da redundant zu ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen.*

Entfernung von Anforderungen

- OPS.1.2.4.A3 *Sicherheitstechnische Anforderung an die Kommunikationsverbindung*: Entfallen, da bereits abgedeckt durch die konkreten Bausteine der Schicht NET.3 *Netzkomponenten.*
- OPS.1.2.4.A4 *Datensicherung bei der Telearbeit*: Entfallen, da redundant zu Baustein CON.3 *Datensicherungskonzept*.

Änderungsdokument zum Baustein: OPS.1.2.5 Fernwartung

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung gegenüber dem Baustein NET.3.2 *Firewall*.

Kapitel 2: Gefährdungslage

- Gefährdung *Unerlaubtes Ausüben von Rechten bei der Fernwartung* entfernt, da inhaltlich nicht spezifisch für die Fernwartung.

Kapitel 3: Anforderungen

Neue Anforderungen

- OPS.1.2.5.A25 *Entkopplung der Fernwartung*: Neue Standard-Anforderung zur Entkopplung der Netzmanagement-Kommunikation bei der Fernwartung.

Änderungen an bestehenden Anforderungen

- OPS.1.2.5.A1 *Planung des Einsatzes der Fernwartung*: Teilanforderung zu In- und Outband-Administration entfernt, da nicht spezifisch für die Fernwartung. Teilanforderung zur Auswahl von Schnittstellen und Protokoll entfernt, da dies in Anforderung OPS.1.2.5.A8 *Sichere Protokolle bei der Fernwartung* behandelt wird.
- OPS.1.2.5.A3 *Absicherung der Schnittstellen zur Fernwartung*: Anforderung geschärft, Fernwartungsverbindungen über nicht vertrauenswürdige Netze müssen verschlüsselt werden.
- OPS.1.2.5.A20 *Betrieb der Fernwartung*: Auswertung von Protokolldaten entfernt, da redundant zu DER.1.A6 *Kontinuierliche Überwachung und Auswertung von Protokolldaten*.
- OPS.1.2.5.A14 *Dedizierte IT-Systeme bei der Fernwartung*: Anforderung umbenannt in *Dedizierte Clients bei der Fernwartung*.

Entfernung von Anforderungen

- OPS.1.2.5.A4 *Einbindung der Fernwartung in der Firewall-Regelwerk*: Entfallen, da redundant zu NET.3.2.A2 *Festlegen der Firewall-Regeln*.

Änderungsdokument zum Baustein: OPS.2.2 Cloud-Nutzung

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

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

DER: Detektion und Reaktion Änderunsgdokumente

Änderungsdokument zum Baustein: DER.1 Detektion von sicherheitsrelevanten Ereignissen

Kapitel 1.3: Abgrenzung und Modellierung

- Entfernung des Verweises auf den Baustein OPS.1.2.2 *Archivierung.*
- Ergänzung der Abgrenzung um die Aspekte Definition sowie Zuweisung von Kompetenzen und Zuständigkeit im Vorfeld der Detektion von sicherheitsrelevanten Ereignissen.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlende oder unzureichende Protokollierung* wurde entfernt, da sie bereits im Baustein OPS.1.15 *Protokollierung* beschrieben wird.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- DER.1.A4 *Sensibilisierung der Mitarbeiter:* Die ersten beiden Teilanforderungen sind bereits durch den Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* abgedeckt.
- DER.1.A5 *Einsatz von mitgelieferten Systemfunktionen zur Detektion:* Die zweite Teilanforderung zum Aspekt Aktivierung der Protokollierung ist bereits durch die Anforderung OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene* abgedeckt.
- 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.
- DER.1.A11 *Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse:* Die Aspekte zur zentralen Speicherung von Ereignismeldungen mithilfe eines Tools sowie zur zeitlichen Synchronisation sind bereits durch die Anforderungen OPS.1.1.5.A6 *Aufbau einer zentralen Protokollierungsinfrastruktur* bzw. OPS.1.1.5.A4 *Zeitsynchronisation der IT-Systeme* abgedeckt.

Entfernung von Anforderungen

- DER.1.A8 *Festlegung von zu schützenden Segmenten:* Der zugrundeliegende Aspekt wurde nach DER.1.A9 *Einsatz zusätzlicher Detektionssysteme* verschoben.

Kapitel 4: Weiterführende Informationen

- Ergänzung von Hinweisen um den Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen.

Änderungsdokument zum Baustein: DER.2.1 Behandlung von Sicherheitsvorfällen

Kapitel 3: Anforderungen

Änderungen an 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, da sie hier keinen nennenswerten Mehrwert bietet.
- DER.2.1.A15 *Schulung der Mitarbeiter der zentralen Anlaufstelle des IT-Betriebs zur Behandlung von Sicherheitsvorfällen:* Die erste Teilanforderungen “Die Mitarbeiter des Service Desk SOLLTEN die Richtlinien für die Behandlung von Sicherheitsvorfällen kennen.” wurde gestrichen, weil dieser Aspekt bereits durch die Anforderung DER.2.1.A2 *Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen* abgedeckt ist. 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.

Änderungsdokument zum Baustein: DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung in Bezug auf eine Inanspruchnahme forensischer Dienstleitungen.

Änderungsdokument zum Baustein: DER.3.1 Audits und Revisionen

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- DER.3.1.A28 *Sicherheitsüberprüfung der Auditoren*: Entfallen, da redundant zu ORP.2.A13 *Sicherheitsüberprüfung.*

Änderungsdokument zum Baustein: DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- DER.3.2.A23 *Sicherheitsüberprüfung bei der IS-Revision*: Entfallen, da redundant zu ORP.2.A13 *Sicherheitsüberprüfung*.

APP: Anwendungen Änderunsgdokumente

Änderungsdokument zum Baustein: APP.1.1 Office-Produkte

Kapitel 1.3: Abgrenzung und Modellierung

- PIM-Anwendungen gestrichen und Formulierung geschärft.

Kapitel 2: Gefährdungslage

- Mehrere Gefährdungen wegen Redundanzen mit anderen Bausteinen gestrichen:
    - *Fehlendes oder unzureichendes Test- und Freigabeverfahren bei Office-Produkten*
    - *Einsatz von unlizenzierten Office-Produkten*
    - *Datenverlust durch Passwortschutz von Office-Dokumenten*
    - *Unerlaubtes Ausüben von Rechten bei Office-Produkten*
    - *Schützenswerte Daten in Meta- und Restinformationen in Office-Dokumenten*
    - *Bezug von Office-Produkten und Updates aus unzuverlässiger Quelle*
    - *Software-Schwachstellen in Office-Produkten*
- Gefährdung *Schädliche Inhalte in Office-Dokumenten* geschärft.

Kapitel 3: Anforderungen

Neue Anforderungen

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

Änderungen an bestehenden Anforderungen

- APP.1.1.A2 *Einschränken von Aktiven Inhalten*: Schulungsaspekte entfernt und in APP.1.1.A17 *Sensibilisierung zu spezifischen Office-Eigenschaften* zusammengefasst. Zusätzlich sprachlich geschärft.
- APP.1.1.A3 *Sicheres Öffnen von Dokumenten aus externen Quellen*: Schulungsaspekte entfernt und in APP.1.1.A17 *Sensibilisierung zu spezifischen Office-Eigenschaften* zusammengefasst. Zusätzlich geschärft.
- 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.
- APP.1.1.A14 *Schutz gegen nachträgliche Veränderungen von Dokumenten*: Schulungsaspekte entfernt. Zusätzlich sprachlich geschärft.
- APP.1.1.A15 *Einsatz von Verschlüsselung und Digitalen Signaturen*: Teile sind redundant zu CON.1 *Kryptokonzept* (CON.1.A7 *Erstellung einer Sicherheitsrichtlinie für den Einsatz kryptografischer Verfahren und Produkte* und CON.1.A4 *Geeignetes Schlüsselmanagement*), unspezifische Inhalte entfernt.
- APP.1.1.A16 *Integritätsprüfung von Dokumenten:* Verfahren verallgemeinert und Anforderung sprachlich geschärft.

Entfernung von Anforderungen

- APP.1.1.A1 *Sicherstellen der Integrität von Office-Produkten*: Entfallen, da redundant zu OPS.1.1.3.A10 *Sicherstellung der Integrität und Authentizität von Softwarepaketen* und APP.6.A4 *Regelung*

für die Installation und Konfiguration von Software. Bei qualifizierten Administratoren wird das Wissen vorausgesetzt, was die Bedeutung von digitalen Signaturen ist.

- APP.1.1.A4 *Absichern des laufenden Betriebs von Office-Produkten*: Entfallen, da nicht spezifisch. Teile werden durch APP.1.1.A17 *Sensibilisierung zu spezifischen Office-Eigenschaften* abgedeckt, andere durch OPS.1.1.3 *Patch- und Änderungsmanagement* (OPS.1.1.3.A15 *Regelmäßige Aktualisierung von IT-Systemen und Software* und OPS.1.1.3.A16 *Regelmäßige Suche nach Informationen zu Patches und Schwachstellen*).
- APP.1.1.A5 *Auswahl geeigneter Office-Produkte*: Entfallen, da redundant zu APP.6 *Allgemeine Software* (APP.6.A1 *Planung des Software-Einsatzes*, APP.6.A2 *Erstellung eines Anforderungskatalogs für Software* und APP.6.A8 *Inventarisierung von Software*).
- APP.1.1.A7 *Installation und sichere Standardkonfiguration von Office-Produkten*: Entfallen, da redundant zu APP.6 *Allgemeine Software* (APP.6.A5 *Sichere Installation von Software* und APP.6.A6 *Auswahl und Bewertung potentieller Software*).
- APP.1.1.A8 *Regelmäßige Versionskontrolle von Office-Produkten*: Entfallen, da redundant zu APP.6.A8 *Inventarisierung von Software.*
- APP.1.1.A9 *Beseitigung von Restinformationen vor Weitergabe von Dokumenten*: Entfallen, da redundant zu CON.9.A5 *Beseitigung von Restinformationen vor Weitergabe* und sonst in APP.1.1.A14 *Schutz gegen nachträgliche Veränderungen von Dokumenten* abgedeckt oder nicht spezifisch.

Änderungsdokument zum Baustein: APP.1.2 Webbrowser

Kapitel 1.3: Abgrenzung und Modellierung

- Abgrenzung geschärft: Der Baustein ist nur auf Webbrowser anzuwenden, die Internetzugriff haben.
- Konkretisierung in Bezug auf Abgrenzung zum Baustein APP.6 *Allgemeine Software*.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehler bei Administration und Betrieb* wurde entfernt, da sie nicht spezifisch für Webbrowser ist.

Kapitel 3: Anforderungen

Neue Anforderungen

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

Umsortierung von Anforderungen

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

Änderungen an 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.A6 *Kennwortmanagement im Webbrowser*: Vorgaben zur Passwortqualität entfernt, da redundant zu den Vorgaben aus ORP.4 *Identitäts- und Berechtigungsmanagement*. Nutzung von Onlinediensten zur Passwortsynchronisation untersagt.
- APP.1.2.A7 *Datensparsamkeit in Webbrowsern*: Anforderung im Bezug auf Telemetriedaten und andere Übertragungen spezifiziert. Nutzung von Standortfreigaben ergänzt.

Entfernung von Anforderungen

- APP.1.2.A4 *Versionsprüfung und Aktualisierung des Webbrowsers*: Anforderung entfernt, da redundant zu OPS.1.1.2.A10 *Fortbildung und Information*, OPS.1.1.3.A16 *Zugangsbeschränkungen für administrative Zugänge* und APP.6.A4 *Regelung für die Installation und Konfiguration von Software*.
- APP.1.2.A5 *Verwendung einer zentralen Basiskonfiguration*: Anforderung entfernt, da redundant zu APP.6.A4 *Regelung für die Installation und Konfiguration von Software.*
- APP.1.2.A8 *Verwendung von Plug-ins und Erweiterungen*: Anforderung entfernt, da redundant zu APP.6.A10 *Verwendung von Plug-ins und Erweiterungen*.

Änderungsdokument zum Baustein: APP.1.4 Mobile Anwendungen (Apps)

Kapitel 1.3: Abgrenzung und Modellierung

- Verweis auf Notfallkonzept entfernt, da redundant und nicht spezifisch für mobile Anwendungen.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Mangelnde Kontrolle und Auswertungsmöglichkeiten* wurde entfernt, da redundant zum Baustein OPS.1.1.5 *Protokollierung*.
- Die Gefährdung *Mangelnde Ressourcen und Kompetenzen* wurde entfernt, weil diese nicht spezifisch für mobile Anwendungen ist.
- Die Gefährdung *Nicht verwaltete Apps und nicht verwaltete Endgeräte* wurde entfernt, da diese nicht spezifisch für mobile Anwendungen ist.

Kapitel 3: Anforderungen

Neue Anforderungen

- *APP.1.4.A16: Mobile Application Management*

Änderungen an bestehenden Anforderungen

- APP.1.4.A3 *Verteilung schutzbedürftiger Apps*: Teilweise entfallen, da redundant zu SYS.3.2.1.A8 *Installation von Apps*, Anforderungstitel wurde angepasst.
- APP.1.4.A12 *Sichere Deinstallation von Apps:* Teilweise entfallen, da redundant zu APP.6.A13 *Deinstallation von Software*.
- APP.1.4.A1 *Anforderungsanalyse für die Nutzung von Apps*: Redundanzen zu APP.6.A1 *Planung des Software-Einsatzes* sowie APP.6.A2 *Erstellung eines Anforderungskatalogs für Software* entfernt.

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.

Entfernung von Anforderungen

- APP.1.4.A2 *Regelungen für die Verwendung von mobilen Endgeräten und Apps*: Entfallen, da redundant zu SYS.3.2.1.A10 *Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten*.
- APP.1.4.A4 *Test und Freigabe von Apps*: Entfallen, da redundant zum themenumfassenden Baustein OPS.1.1.6 *Software-Tests und -Freigaben.*
- APP.1.4.A6 *Patchmanagement für Apps*: Entfallen, da nicht spezifisch.
- APP.1.4.A9 *Sichere Anbindung an Backend-Systeme*: Entfallen, da Anforderungen an die App-Entwicklung nicht im Fokus des Bausteins stehen.
- APP.1.4.A10 *Sichere Authentisierung von Apps*: Entfallen, da Anforderungen an die App-Entwicklung nicht im Fokus des Bausteins stehen.
- APP.1.4.A11 *Zentrales Management von Apps*: Entfallen, da redundant zu SYS.3.2.2. *Mobile Device Management (MDM).*
- APP.1.4.A13 *Entwicklungen von Fallback-Lösungen für Apps*: Entfallen, da nicht spezifisch für mobile Anwendungen.

Kapitel 4: Weiterführende Informationen

- Entfernung des Verweises auf die BSI-Broschüre zum Thema: „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Maßnahmen“, da diese veraltet ist.

Änderungsdokument zum Baustein: APP.2.1. Allgemeiner Verzeichnisdienst

Kapitel 1.3: Abgrenzung und Modellierung

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

Kapitel 2: Spezifische Gefährdungslage

- Es wurde ein Beispiel aus dem Baustein APP.2.3 *OpenLDAP* in verallgemeinerter Form aufgenommen.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.2.1.A5 *Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten:* Teilanforderung zu Zugriffsrechten entfernt, da redundant zu ORP.4.A9 *Identifikation und Authentisierung.*
- 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.A12 *Überwachung von Verzeichnisdiensten*: Teilanforderungen zu Überwachung und Protokollierung entfernt, da redundant zu OPS.1.1.5.A1 *Erstellung einer Sicherheitsrichtlinie für die Protokollierung*, OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene* und OPS.1.1.5.A9 *Bereitstellung von Protokollierungsdaten für die Auswertung*. Dafür wurde die Anforderung um eine Teilanforderung aus dem nachgeordneten Baustein APP.2.3 OpenLDAP zur Überwachung von Servern und Diensten (aus APP.2.3.A12 *Protokollierung und Überwachung von OpenLDAP*) ergänzt.
- 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.

Entfernung von Anforderungen

- APP.2.1.A10 *Schulung zur Administration und Betrieb von Verzeichnisdiensten*: Entfallen, da redundant zu OPS.1.1.2.A10 *Fortbildung und Information.*

Änderungsdokument zum Baustein: APP.2.2 Active Directory

Kapitel 1.3: Abgrenzung und Modellierung

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

Kapitel 2: Gefährdungslage

- Streichung einzelner Beispiele, da diese sich auf Themen übergeordneter Bausteine bezogen.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.2.2.A2 *Planung der Active-Directory-Administration*: Teilanforderungen zu Berechtigungen entfallen, da redundant zu ORP.4.A3 *Dokumentation der Benutzerkennungen und Rechteprofile* und ORP.4.A15 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement.*
- APP.2.2.A6 *Aufrechterhaltung der Betriebssicherheit von Active Directory*: Teilanforderungen zu Berechtigungen entfallen, da redundant zu ORP.4.A7 *Vergabe von Zugriffsrechten* und ORP.4.A16 *Richtlinien für die Zugriffs- und Zugangskontrolle.*
- APP.2.2.A7 *Umsetzung sicherer Verwaltungsmethoden für Active Directory*: Teilanforderungen zu Benutzerkonten entfallen, da redundant zu ORP.4.A13 *Geeignete Auswahl von Authentisierungsmechanismen und* ORP.4.A14 *Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. Anwendung*. Die Absicherung der Arbeitsplätze wurde in den übergeordneten Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* verschoben (APP.2.1.A6 *Sicherer Betrieb von Verzeichnisdiensten*).
- APP.2.2.A10 *Sicherer Einsatz von DNS für Active Directory*: Beispiel im ersten Anforderungssatz wurde entfernt.
- APP.2.2.A11 *Überwachung der Active-Directory-Infrastruktur*: Teilanforderungen zur Protokollierung entfallen, da redundant zu OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene.*
- APP.2.2.A12 *Datensicherung für Domänen-Controller*: Teilanforderungen zur Datensicherung entfallen, da redundant zu *CON.3.A5 Regelmäßige Datensicherung* und CON.3.A.12 *Geeignete Aufbewahrung der Backup-Datenträge*r.

Entfernung von Anforderungen

- APP.2.2.A4 *Schulung zur Active Directory Verwaltung*: Entfallen, da redundant zu OPS.1.1.2.A10 *Fortbildung und Information.*
- APP.2.2.A13 *Einsatz von Zwei-Faktor-Authentisierung*: Entfallen, da redundant zu ORP.4.A21 *Mehr-Faktor-Authentisierung.*

Änderungsdokument zum Baustein: APP.2.3 OpenLDAP

Kapitel 1.3: Abgrenzung und Modellierung

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

Kapitel 2: Gefährdungslage

- Streichung einzelner Beispiele, da diese sich auf Themen übergeordneter Bausteine bezogen. Beispiele zur BerkeleyDB entfernt, da diese bald veraltet ist.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.2.3.A4 *Konfiguration der durch OpenLDAP verwendeten Datenbank*: BerkeleyDB in Datenbank allgemein geändert.
- APP.2.3.A5 *Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP*: Teilanforderung zum Sicherheitskonzept entfallen, da redundant zu APP.2.1.A2 *Planung des Einsatzes von Verzeichnisdiensten*.
- APP.2.3.A10 *Sichere Aktualisierung von OpenLDAP*: Sprachliche Schärfung der Anforderung und Entfernung von Teilanforderungen zum Patchen, da redundant zu OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement*.

Entfernung von Anforderungen

- APP.2.3.A2 *Sichere Installation von OpenLDAP*: Entfallen, da redundant zu OPS.1.1.3.A11 *Kontinuierliche Dokumentation der Informationsverarbeitung* und APP.2.1.A2 *Planung des Einsatzes von Verzeichnisdiensten*.
- APP.2.3.A7 *Schulung von Administratoren von OpenLDAP*: Entfallen, da redundant zu OPS.1.1.2.A10 *Fortbildung und Information.*
- APP.2.3.A12 *Protokollierung und Überwachung von OpenLDAP*: Entfallen, da redundant zu OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene*. Die Teilanforderung zur Überwachung mit dem Server wurde in APP.2.1 *Allgemeiner Verzeichnisdienst* verschoben (APP.2.1..A12 *Überwachung von Verzeichnisdiensten).*
- APP.2.3.A13 *Datensicherung von OpenLDAP*: Entfallen, da redundant zu den Anforderungen des Bausteins CON.3 *Datensicherungskonzept.*

Kapitel 4: Weiterführende Informationen

- Der Verweis auf eine alte Masterarbeit wurde entfernt.

Änderungsdokument zum Baustein: APP.3.1 Webanwendungen

Kapitel 1.3: Abgrenzung und Modellierung

- Entwicklungsaspekte bei Webanwendungen aufgenommen.

Kapitel 2: Gefährdungslage

- Entfernung aller Gefährdungen, die sich auf Entwicklungsaspekte beziehen.

Kapitel 3: Anforderungen

Änderungen an 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. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt. Anforderung umbenannt in *"Kontrolliertes Einbinden von Dateien und Inhalten bei Webanwendungen*".
- APP.3.1.A7 S*chutz vor unerlaubter automatisierter Nutzung von Webanwendungen*: Entfernung aller entwicklungsspezifischen Aspekte. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A8 Systemarchitektur einer Webanwendung: Entfernung aller entwicklungsspezifischen Aspekte. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt. Entfernung von Aspekten, die den Webserver betreffen.
- APP.3.1.A9 *Beschaffung, Entwicklung und Erweiterung von Webanwendungen*: Entfernung aller entwicklungsspezifischen Aspekte. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt. Anforderung umbenannt in „*Beschaffung von Webanwendungen*“.
- 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. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A22 *Überprüfung von Webanwendungen*: Anforderung umbenannt in *Penetrationstest und Revision*.

Entfernung von Anforderungen

- APP.3.1.A2 Zugriffskontrolle *bei Webanwendungen*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A3 *Sicheres Session-Management*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A5 *Protokollierung*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen und redundant zu OPS.1.1.5 *Protokollierung*. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A13 *Restriktive Herausgabe sicherheitsrelevanter Informationen*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.

- APP.3.1.A15 *Verifikation essenzieller Änderungen*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A16 *Umfassende Eingabevalidierung und Ausgabekodierung*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A17 *Fehlerbehandlung*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A19 *Schutz vor SQL-Injection*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A23 *Verhinderung von Cross-Site-Request-Forgery*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A24 *Verhinderung der Blockade von Ressourcen*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.
- APP.3.1.A25 *Kryptografische Sicherung vertraulicher Daten*: Entfallen, da nicht spezifisch für den Betrieb von Webanwendungen. Das Thema wird nun im neuen Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.

Kapitel 4: Weiterführende Informationen

- Dokument „Hilfsmittel zur Nutzung des Bausteins Webanwendungen“ entfernt.

Änderungsdokument zum Baustein: APP.3.2 Webserver

Kapitel 2: Gefährdungslage

- Gefährdung *Software-Schwachstellen oder -Fehler*: Entfernt, da nicht spezifisch für Webserver.
- Gefährdung *Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen*: Entfernt, da nicht spezifisch für Webserver.

Kapitel 3: Anforderungen

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.

Entfernung von Anforderungen

- APP.3.2.A17 *Einsatz erweiterter Authentisierungsmethoden*: Entfernt, da redundant zu ORP.4.A21 *Mehr-Faktor-Authentisierung*.

Änderungsdokument zum Baustein: APP.3.3 Fileserver

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.3.3.A6 *Beschaffung eines Fileservers und Auswahl eines Dienstes:* Aspekte zur Anforderungsliste wurden entfernt, da redundant zu den Anforderungen APP.6.A3 *Sichere Beschaffung von Software* und APP.6.A6 *Auswahl und Bewertung potentieller Software* des übergreifenden Bausteins APP.6 *Auswahl und Einsatz von Software*.
- APP.3.3.A9 *Sicheres Speichermanagement*: Aspekte zum Protokollierungskonzept wurden entfernt, da redundant zu OPS.1.1.5 *Protokollierung*.
- APP.3.3.A12 *Verschlüsselung des Datenbestandes*: Aspekte zu kryptografischen Schlüsseln wurden entfernt, da redundant zu der Anforderung CON.1.A4 *Geeignetes Schlüsselmanagement* des übergreifenden Bausteins CON.1 *Kryptokonzept*.
- APP.3.3.A13 *Replizieren zwischen Standorten*: Diese Anforderung wurde in *Replikation zwischen Standorten* umbenannt.

Entfernung von Anforderungen

- APP.3.3.A5 *Restriktive Rechtevergabe*: Entfallen, da die Vorgaben dieser Anforderung nicht über die Vorgaben der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement* und OPS.1.1.2 *Ordnungsgemäße IT-Administration* hinausgehen.

Kapitel 4: Weiterführende Informationen

- Allgemeine Hinweise zur Härtung von hochverfügbaren Servern wurden entfernt.

Änderungsdokument zum Baustein: APP.3.4 Samba

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung gegenüber dem Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlerhafte Protokollierung bei Samba* wurde entfernt, da sie nicht spezifisch für Samba ist.
- Die Gefährdung *Schadprogramme im Umfeld von Samba-Diensten* wurde entfernt, da sie für jeden Fileserver gilt.
- Die Gefährdung *Fehlende Anpassung von Samba* wurde in *Unsichere Standardeinstellungen auf Samba-Servern* umbenannt.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.3.4.A1 *Planung des Einsatzes eines Samba-Servers*: Anforderungen an Virenschutz entfernt, da redundant zu OPS.1.1.4 *Schutz vor Schadprogrammen*. Die Umsetzung SOLLTE nun dokumentiert werden, außerdem wurde die Rolle des IT-Betriebs hervorgehoben.
- APP.3.4.A2 *Sichere Grundkonfiguration eines Samba-Servers*: Teilanforderung zum Aspekt Berechtigungsmanagement entfernt, da diese redundant zu ORP.4 *Identitäts- und Berechtigungsmanagement* ist.
- APP.3.4.A3 *Sichere Konfiguration des Samba-Servers*: Die Anforderung wurde in *Sichere Konfiguration eines Samba-Servers* umbenannt. Der Aspekt zu Kerberos wurde in APP.3.4.A9 *Sichere Konfiguration von Kerberos unter Samba* verschoben. Die Vorgaben dieser Anforderung zu Netports gehen nicht über die Vorgaben des Bausteins NET.3.2 *Firewall* hinaus und 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.

Entfernung von Anforderungen

- APP.3.4.A11 *Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers*: Die Vorgaben dieser Anforderung gehen nicht über die Vorgaben des Bausteins NET.1.1 *Netzarchitektur und -design* hinaus.

Änderungsdokument zum Baustein: APP.3.6 DNS-Server

Kapitel 3: Anforderungen

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.
- APP.3.6.A19 *Aussonderung von DNS-Servern:* Die Teilanforderung zur sicheren Löschung von Speichermedien ist bereits durch die Anforderung CON.6.A2 *Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen* im übergreifenden Baustein CON.6 *Löschen und Vernichten* abgedeckt.

Entfernung von Anforderungen

- APP.3.6.A12 *Schulung der Verantwortlichen:* Diese Anforderung ist bereits durch die Anforderung *ORP.2.A9 Schulung von Mitarbeitern* im übergreifenden Baustein ORP.2 *Personal* abgedeckt.

Änderungsdokument zum Baustein: APP.4.2 SAP-ERP-System

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.4.2.A5 *Konfiguration und Absicherung der SAP-Benutzerverwaltung*: Allgemeine Schulungsanforderungen entfernt, da redundant zu ORP.2.A15 *Qualifikation des Personals*.
- APP.4.2.A6 *Erstellung und Umsetzung eines Benutzer- und Berechtigungskonzeptes:* Allgemeine Anforderungen zum Berechtigungsmanagement entfernt (Prinzip der minimalen Berechtigungen), da redundant zu ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen*.

Entfernung von Anforderungen

- APP.4.2.A10 *Regelmäßige Implementierung von Sicherheitskorrekturen*: Entfallen, da redundant zu OPS.1.1.3.A15 *Regelmäßige Implementierung von Sicherheitskorrekturen.*
- APP.4.2.A21 *Konfiguration des Security Audit Logs*: Entfallen, da redundant zu OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebenen*.

Änderungsdokument zum Baustein: APP.4.3 Relationale Datenbanken

Kapitel 1.3: Abgrenzung und Modellierung

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

Kapitel 2: Gefährdungslage

- *Unzureichende Vergabe von Berechtigungen*: Entfernt, da nicht spezifisch.
- *Unzureichendes Patchmanagement*: Entfernt, da nicht spezifisch.

Kapitel 3: Anforderungen

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.

Entfernung von Anforderungen

- APP.4.3.A2 *Installation des Datenbankmanagementsystems*: Entfallen, da redundant zu OPS.1.1.3.A10 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*, APP.6.A4 *Überprüfung der Integrität der Installationspakete* und APP.6.A5 *Regelung für die Installation von Software.*
- APP.4.3.A5 *Benutzer- und Berechtigungskonzept:* Entfallen, da redundant zu ORP.4.A15 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* und ORP.4.A16 *Richtlinien für die Zugriffs- und Zugangskontrolle.*
- APP.4.3.A6 *Passwortänderung*: Entfallen, da redundant zu ORP.4.A8 *Regelung des Passwortgebrauchs.*
- APP.4.3.A7 *Zeitnahes Einspielen von Sicherheitsupdates*: Entfallen, da redundant zu OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement* und OPS.1.1.3.A3 *Konfiguration von Autoupdate-Mechanismen.*
- APP.4.3.A8 *Datenbank-Protokollierung*: Entfallen, da diese Anforderung mit den Anforderungen des Bausteins OPS.1.1.5 *Protokollierung* abgedeckt ist.
- APP.4.3.A10 *Auswahl geeigneter Datenbankmanagementsysteme*: Entfallen, da redundant zu APP.6.A2 *Erstellung eines Anforderungskatalogs für Software* und APP.6.A3 *Sichere Beschaffung von Software.*
- APP.4.3.A14 *Überprüfung der Datensicherung eines Datenbanksystems*: Entfallen, da redundant zu CON.3.A5 *Regelmäßige Datensicherung.*
- APP.4.3.A15 *Schulung der Datenbankadministratoren*: Entfallen, da redundant zu OPS.1.1.2.A10 *Fortbildung und Information.*

Änderungsdokument zum Baustein: APP.4.6 SAP ABAP-Programmierung

Kapitel 1.3: Abgrenzung und Modellierung

- Anpassung auf geänderte Bausteinbezeichnungen (CON.8 *Software-Entwicklung* wird zu APP.6 *Allgemeine Software* und CON.4 *Auswahl und Einsatz von Standardsoftware* wird zu APP.7 *Entwicklung von Individualsoftware).*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.4.6.A11 *Vermeidung von eingeschleustem Schadcode:* Streichung eines Satzes, der keine Anforderung enthält.

Änderungsdokument zum Baustein: APP.5.2 Microsoft Exchange und Outlook

Kapitel 1.3: Abgrenzung und Modellierung

- Die Abgrenzung wurde geschärft und auf den neuen Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* angepasst.

Kapitel 3: Anforderungen

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.

Entfernung von Anforderungen

- APP.5.2.A14 *Schulung zu Sicherheitsmechanismen von Outlook:* Entfallen, da redundant zu APP.5.3.A7 *Schulung zu Sicherheitsmechanismen von E-Mail-Clients für Benutzer*.
- APP.5.2.A15 *Betriebsdokumentation für Microsoft Exchange:* Entfallen, da nicht spezifisch die Exchange.
- APP.5.2.A19 *Erstellung einer Sicherheitsrichtlinie für Microsoft Exchange:* Entfallen, da redundant zu APP.5.3.A6 *Festlegung einer Sicherheitsrichtlinie für E-Mail*.

Änderungsdokument zum Baustein: APP.7 Entwicklung von Individualsoftware

Kapitel 1.3: Abgrenzung und Modellierung

- Der Baustein löst CON.5 *Entwicklung und Einsatz von Individualsoftware* ab und wurde im Zuge der Neukonzeptionierung von APP.6 *Allgemeine Software* in die APP-Schicht verschoben und dabei neu aufgebaut.
- Konkretisierung der Abgrenzung gegenüber CON.8 *Software-Entwicklung.*

Kapitel 2: Gefährdungslage

- Die Gefährdung *Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten* wurde entfernt, da sie bereits durch den Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt wird.
- Die Gefährdung *Mangelhafte Steuerung der Software-Entwicklung* wurde hinzugefügt.
- Die Gefährdung *Beauftragung ungeeigneter Software-Entwickler* wurde ergänzt.

Kapitel 3: Anforderungen

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 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*.

Entfernung von Anforderungen

- CON.5.A1 *Festlegung benötigter Sicherheitsfunktionen der Individualsoftware*: Diese Anforderung ist bereits durch die Anforderung APP.6.A2 *Erstellung eines Anforderungskatalogs für Software* abgedeckt.
- CON.5.A3 *Sichere Installation von Individualsoftware*: Diese Anforderung ist bereits durch die Anforderung APP.6.A4 *Regelung für die Installation und Konfiguration von Software* abgedeckt.
- CON.5.A4 *Heranführen von Benutzerinnen und Benutzern an Individualsoftware*: Diese Anforderung ist bereits durch die Anforderung APP.6.A9 *Erstellung einer Sicherheitsrichtlinie für den Einsatz der Software* abgedeckt.
- CON.5.A9 *Außerbetriebnahme von Individualsoftware:* Diese Anforderung ist bereits durch die Anforderung APP.6.A11 *Geregelte Außerbetriebnahme von Software* abgedeckt.

- CON.5.A13 *Entwicklung eines Redundanzkonzeptes für Anwendungen:* Die Anforderung wurde entfernt, da diese nicht spezifisch für Individual-Software ist und bereits durch die Abgrenzung von APP.6 *Allgemeine Software* auf DER.4 *Notfallmanagement* behandelt wird.

SYS: IT-Systeme Änderunsgdokumente

Änderungsdokument zum Baustein: SYS.1.1 Allgemeiner Server

Kapitel 2: Gefährdungslage

- Die Gefährdung *Software-Schwachstellen oder -Fehler* wurde entfernt, da sie nicht spezifisch für Server ist. Das Erkennen und Beheben von solchen Schwachstellen ist Bestandteil eines Patch- und Änderungsmanagements.

Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.1.1.A35 *Erstellung und Pflege eines Betriebshandbuchs:* Neue Standard-Anforderung zur Nutzung eines Betriebshandbuchs.
- SYS.1.1.A36 *Absicherung des Bootvorgangs*: Neue Anforderung bei erhöhtem Schutzbedarf zur Verwendung von Secure Boot.

Änderungen an bestehenden Anforderungen

- SYS.1.1.A1 *Geeignete Aufstellung*: Regelungen zum Zutritt entfernt, da bereits abgedeckt durch ORP.4.A5 *Vergabe von Zutrittsberechtigungen*. Regelung zu Brandabschnitten entfernt, da Infrastrukturaspekte in INF.2 *Rechenzentrum sowie Serverraum*, dort speziell INF.2.A2 *Bildung von Brandabschnitten*, behandelt werden. Ergänzt, dass Arbeitsplatzrechner keine Server und Server keine Arbeitsplatzrechner (übernommen aus SYS.1.1.A5 *Schutz von Administrationsschnittstellen*) sein dürfen.
- SYS.1.1.A2 *Benutzerauthentisierung an Servern*: Regelungen zu Passwörtern entfernt, da dies in ORP.4 *Identitäts- und Berechtigungsmanagement*, speziell in ORP.4.A8 *Regelung des Passwortgebrauchs*, behandelt wird.
- SYS.1.1.A5 *Schutz von Administrationsschnittstellen*: Anforderung 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.
- SYS.1.1.A6 *Deaktivierung nicht benötigter Dienste und Kennungen*: Anforderung umbenannt in *Deaktivierung nicht benötigter Dienste* und Umgang mit Benutzerkennungen entfernt. Voreingestellte Passwörter werden in ORP.4.A23 *Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme* behandelt.
- SYS.1.1.A9 *Einsatz von Virenschutz-Programmen*: Anforderung umbenannt in *Einsatz von Virenschutz-Programmen auf Servern*, da diese Anforderung den Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* entsprechend konkretisiert. Die hier entfernten Aspekte zu Funktionen des Virenschutz-Programms bzw. regelmäßiger Aktualisierung finden sich dort in OPS.1.1.4.A3 *Auswahl eines Virenschutzprogrammes* bzw. OPS.1.1.4.A6 *Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen*.
- 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.A15 *Unterbrechungsfreie und stabile Stromversorgung*: Inhaltliche Anforderungen an die unterbrechungsfreie Stromversorgung und den Überspannungsschutz entfernt. Diese sind abgedeckt durch INF.2.A3 *Einsatz einer unterbrechungsfreien Stromversorgung* sowie INF.3.A6 *Überspannungsschutz*.
- 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.

Entfernung von Anforderungen

- SYS.1.1.A3 *Restriktive Rechtevergabe*: Entfallen, diese Aspekte werden in ORP.4 *Identitäts- und Berechtigungsmanagement*, insbesondere in ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen*, behandelt.
- SYS.1.1.A4 *Rollentrennung*: Entfallen, diese Aspekte werden in OPS.1.1.2.A6 *Schutz administrativer Tätigkeiten* behandelt.
- SYS.1.1.A7 *Updates und Patches für Firmware, Betriebssysteme und Anwendungen*: Entfallen, da dies in OPS.1.1.3 *Patch- und Änderungsmanagement* behandelt wird, speziell in OPS.1.1.3.A15 *Regelmäßige Bewertung und Implementierung von Sicherheitskorrekturen* sowie OPS.1.1.3.A16 *Regelmäßige Suche nach Informationen zu Patches und Schwachstellen.*
- SYS.1.1.A8 *Regelmäßige Datensicherung*: Entfallen, da das Thema Backups ausführlich im Baustein CON.3 *Datensicherungskonzept* behandelt wird.
- SYS.1.1.A14 *Erstellung eines Benutzer- und Administrationskonzepts*: Entfallen. Regelungen zu administrativen Aufgaben werden in OPS.1.1.2 *Ordnungsgemäße IT-Administration* umfassend behandelt, insbesondere in OPS.1.1.2.A7 *Regelung der IT-Administrationstätigkeit*. Regelungen zu Benutzerrollen sind nicht auf Ebene des IT-Systems sinnvoll, hier sind die einschlägigen Anforderungen aus ORP.1 *Organisation* wie ORP.1.A1 *Festlegung von Verantwortlichkeiten und Regelungen* und ORP.1.A5 *Vergabe von Berechtigungen* zu beachten, und in diesem Kontext entsprechende Anforderungen aus ORP.4 *Identitäts- und Berechtigungsmanagement.*
- SYS.1.1.A17 *Einsatzfreigabe für Server*: Entfallen, da redundant zu OPS.1.1.3.A9 *Test- und Abnahmeverfahren für neue Hard- und Software*.
- SYS.1.1.A18 *Verschlüsselung der Kommunikationsverbindungen*: Die Anforderung muss geeignet auf Anwendungs- bzw. Dienstebene erfüllt werden und nicht auf Ebene des IT-Systems. Sie wurde daher aus dem Baustein entfernt.
- SYS.1.1.A20 *Beschränkung des Zugangs über Netze*: Entfallen, da die Aspekte dieser Anforderung bereits durch NET.1.1 *Netzarchitektur und -design* abgedeckt sind, insbesondere NET.1.1.A4 *Netztrennung in Sicherheitszonen* und NET.1.1.A5 *Client-Server-Segmentierung*.
- SYS.1.1.A26 *Verwendung von Mehr-Faktor-Authentisierung*: Entfallen, da bereits durch ORP.4.A10 *Schutz von Benutzerkennungen mit weitreichenden Berechtigungen* abgedeckt.
- SYS.1.1.A29 *Einrichtung einer Testumgebung*: Entfallen, da redundant zu OPS.1.1.3.A9 *Test- und Abnahmeverfahren für neue Hard- und Software*.
- SYS.1.1.A32 *Zusätzlicher Schutz von privilegierten Anmeldeinformationen*: Entfallen, da die Aspekte bereits in ORP.4 *Identitäts- und Berechtigungsmanagement* behandelt werden, insbesondere durch ORP.4.A24 *Vier-Augen-Prinzip für administrative Tätigkeiten*.

Änderungsdokument zum Baustein: SYS.1.2.2 Windows Server 2012

Kapitel 2: Gefährdungslage

- Die Gefährdung *Verlust verschlüsselter Daten* wurde entfernt, da sie nicht spezifisch für Windows Server 2012 ist.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.1.2.2.A2 *Sichere Installation von Windows Server 2012*: Anforderung zu sicheren Installationsquellen entfernt, da bereits abgedeckt durch SYS.1.1.A16 *Sichere Installation und Grundkonfiguration von Servern*.
- SYS.1.2.2.A3 *Sichere Administration von Windows Server 2012*: Anforderung zu Passworten und administrativen Rechten entfernt, da diese Themen im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* umfassend behandelt werden.
- SYS.1.2.2.A4 *Sichere Konfiguration von Windows Server 2012*: Testen von Einstellungen entfernt, da bereits abgedeckt durch OPS.1.1.3 *Patch- und Änderungsmanagement*, insbesondere OPS.1.1.3.A1 *Konzept für das Patch- und Änderungsmanagement*.
- SYS.1.2.2.A5 *Schutz vor Schadsoftware auf Windows Server 2012*: Regelmäßige Aktualisierung der AV-Signaturen entfernt, da dies Bestandteil von OPS.1.1.4 *Schutz vor Schadprogrammen* ist, insbesondere OPS.1.1.4.A6 *Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen*.
- SYS.1.2.2.A6 *Sichere Authentisierung und Autorisierung in Windows Server 2012*: Anforderung zu lokalen Berechtigungen von Administratoren entfernt, da dies im Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* behandelt wird, insbesondere in OPS.1.1.2.A6 *Schutz administrativer Tätigkeiten*.
- SYS.1.2.2.A8 *Schutz der Systemintegrität*: Aspekte zu Secure Boot sind nun zu finden in SYS.1.1.A35 *Absicherung des Bootvorgangs*. Das Testen von Änderungen ist analog zu SYS.1.2.2.A4 bereits durch OPS.1.1.4 *Patch- und Änderungsmanagement* abgedeckt.
- 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.

Entfernung von Anforderungen

- SYS.1.2.2.A7 *Prüfung der Sicherheitskonfiguration von Windows Server 2012*: Entfallen, da regelmäßige Sicherheitsüberprüfungen bereits in SYS.1.1.A24 *Sicherheitsprüfungen* gefordert werden.
- SYS.1.2.2.A9 *Lokale Kommunikationsfilterung*: Entfallen, da bereits durch SYS.1.1.A19 *Einrichtung lokaler Paketfilter* abgedeckt.
- SYS.1.2.2.A10 *Festplattenverschlüsselung bei Windows Server 2012*: Entfallen, da bereits durch SYS.1.1.A34 *Festplattenverschlüsselung* abgedeckt.
- SYS.1.2.2.A13 *Starke Authentifizierung bei Windows Server 2012*: Entfallen, da diese Themen im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* umfassend behandelt werden.

Änderungsdokument zum Baustein: SYS.1.3 Server unter Linux und Unix

Kapitel 3: Anforderungen

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.A5 *Sichere Installation von Software-Paketen*: Allgemeine Anforderungen zu Software aus sicheren Quellen entfernt, da bereits durch APP6.A3 *Sichere Beschaffung von Software* gefordert.
- SYS.1.3.A6 *Verwaltung von Benutzern und Gruppen*: */etc/shadow* wurde in die Liste der Dateien, die nicht direkt bearbeitet werden sollen, aufgenommen.
- SYS.1.3.A17 *Zusätzlicher Schutz des Kernels*: Allgemeine Forderung nach rollenbasierten Zugriffskontrollen entfernt, da dies in ORP.4 *Identitäts- und Berechtigungsmanagement* und OPS.1.1.2 *Ordnungsgemäße IT-Administration* ausführlich behandelt wird.

Entfernung von Anforderungen

- SYS.1.3.A1 *Authentisierung von Administratoren und Benutzern*: Entfallen, da redundant zu SYS.1.1.A2 *Benutzerauthentisierung an Servern*.
- SYS.1.3.A9 *Absicherung des Bootvorgangs*: Entfallen, da dieses Thema nun unabhängig vom Betriebssystem in SYS.1.1.A35 *Absicherung des Bootvorgangs* abgedeckt wird.
- SYS.1.3.A11 *Einsatz der Sicherheitsmechanismen von NFS*: Entfallen, da dieses Themengebiet auf Dienste-Ebene umfassend im Baustein APP.3.3 *Fileserver* behandelt wird.
- SYS.1.3.A12 *Einsatz der Sicherheitsmechanismen von NIS*: Entfallen, da NIS zunehmend durch sicherere Verzeichnisdienste wie LDAP ersetzt wurde. Diese werden in APP.2.1 *Allgemeiner Verzeichnisdienst* und APP.2.3 *OpenLDAP* behandelt.
- SYS.1.3.A15 *Zusätzliche Absicherung des Bootvorgangs*: Entfallen, da dieses Thema nun unabhängig vom Betriebssystem in SYS.1.1.A35 *Absicherung des Bootvorgangs* abgedeckt wird.

Änderungsdokument zum Baustein: SYS.1.5 Virtualisierung

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.1.5.A6 *Protokollierung in der virtuellen Infrastruktur:* Der Aspekt Auswertung von Protokollierungsdaten ist bereits durch die Anforderung DER.1.A6 *Kontinuierliche Überwachung und Auswertung von Protokolldaten* im übergreifenden Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* abgedeckt.
- SYS.1.5.A8 *Planung einer virtuellen Infrastruktur:* Der Aspekt ausreichende Qualifikation von Administratoren ist bereits durch die Anforderung OPS.1.1.2.A10 *Fortbildung und Information* im übergreifenden Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* abgedeckt.
- SYS.1.5.A10 *Einführung von Verwaltungsprozessen für virtuelle IT-Systeme:* Die folgende Teilanforderung "Bevor ein virtuelles IT-System betrieben wird, SOLLTE in einer Test- und Entwicklungsumgebung geprüft werden, ob es für den Produktiveinsatz geeignet ist." ist bereits durch die Anforderung OPS.1.1.3.A9 *Test- und Abnahmeverfahren für neue Hardware* abgedeckt.

Entfernung von Anforderungen

- SYS.1.5.A1 *Einspielen von Aktualisierungen und Sicherheitsupdates:* Diese Anforderung ist bereits durch die Anforderung OPS.1.1.3.A15 *Regelmäßige Aktualisierung von IT-Systemen und Software* im übergreifenden Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* abgedeckt.
- SYS.1.5.A18 *Schulung der Administratoren virtueller Umgebungen:* Diese Anforderung ist bereits durch die Anforderung OPS.1.1.2.A10 *Fortbildung und Information* im übergreifenden Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* abgedeckt.

Änderungsdokument zum Baustein: SYS.1.7 IBM Z-System

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- SYS.1.7.A10 *Absichern des Login-Vorgangs unter z/OS*: Entfallen, da keine spezifische Anforderung für z/OS. Die Aspekte zu berechtigten Benutzern werden in ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* behandelt. Die Deaktivierung nicht benötigter Dienste ist bereits allgemein in SYS.1.1.A6 *Deaktivierung nicht benötigter Dienste* gefordert.
- SYS.1.7.A12 *Planung von Z-Systemen*: Entfallen, da keine spezifischen Inhalte für z/OS. Die Aspekte werden umfassender in SYS.1.1.A12 *Planung des Server-Einsatzes* behandelt.
- SYS.1.7.A13 *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*: Entfallen, da keine spezifischen Inhalte für z/OS. Die Aspekte werden in SYS.1.1.A11 *Festlegung einer Sicherheitsrichtlinie für Server* behandelt.
- SYS.1.7.A15 *Überprüfungen zum sicheren Betrieb von z/OS*: Entfallen, da keine spezifischen Inhalte für z/OS. Die Aspekte werden in SYS.1.1.A24 *Sicherheitsprüfungen für Server* behandelt.

Änderungsdokument zum Baustein: SYS.1.8 Speicherlösungen

Kapitel 1.3: Abgrenzung und Modellierung

- Kapitel grundlegend überarbeitet.
- Konkretisierung der Abgrenzung: Ausführliche Hinweise hinzugefügt, die bei der Modellierung von NAS (Network Attached Storage (NAS), SAN (Storage Area Networks), Hybrid-Storage, Objekt-Storage und Cloud-Storage beachtet werden müssen.
- Abgrenzung zu ORP.4 *Identitäts- und Berechtigungsmanagemen*t ergänzt, da oftmals eine Vielzahl von Benutzerkonten Zugriff auf Speicherlösungen hat.
- Abgrenzung zu OPS.2.1 *Outsourcing für Kunden* ergänzt.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlende oder unzureichende Abgrenzung von Verantwortlichkeiten bei Speicherlösungen* wurde entfernt. Der zugrundeliegende Aspekt soll im übergeordneten Baustein ORP.1 *Organisation* beschrieben werden.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.1.8.A2 *Sichere Grundkonfiguration von Speicherlösungen:* Die Aspekte Benutzerkonten und Passwörter sind bereits durch die Anforderungen ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* bzw. ORP.4.A23 *Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme* im übergreifenden Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* abgedeckt.
- SYS.1.8.A6 *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen:* Die Anforderung wurde um den Aspekt einer möglichen Aktualisierung der Richtlinie erweitert.
- SYS.1.8.A11 *Sicherer Betrieb einer Speicherlösung:* Der Aspekt zu Änderungsmanagement ist bereits durch die Anforderungen OPS.1.1.3.A5 *Umgang mit Änderungsanforderungen* und OPS.1.1.3.A6 *Abstimmung von Änderungsanforderungen* im übergreifenden Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* abgedeckt.
- SYS.1.8.A13 *Überwachung und Verwaltung von Speicherlösungen:* Die letzte Teilanforderung wurde gestrichen. Der zugrundeliegende Aspekt wird im Baustein OPS.2.1 *Outsourcing für Kunden* behandelt.
- SYS.1.8.A16 *Sicheres Löschen in SAN-Umgebungen:* Die erste Teilanforderung wird bereits durch die Anforderung CON.6.A2 *Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen* im übergreifenden Baustein CON.6 *Löschen und Vernichten* abgedeckt.
- SYS.1.8.A17 *Dokumentation der Systemeinstellungen von Speichersystemen:* Die Aspekte Aktualiät der Dokumentation bezüglich Rechtevergabe sowie Verfügbarkeit der Dokumentation in Notfällen wurden gestrichen. Die Aktualität der Dokumentation bezüglich Rechtevergabe wird in ORP.4.A3 *Dokumentation der Benutzerkennungen und Rechteprofile* behandelt. Die Verfügbarkeit der Dokumentation in allen Notfallszenarien wird bereits ausreichend in SYS.1.8.A20 *Notfallvorsorge und Notfallreaktion für Speicherlösungen* adressiert.

Entfernung von Anforderungen

- SYS.1.8.A3 *Restriktive Rechtevergabe:* Diese Anforderung ist bereits durch die Anforderungen ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* sowie ORP.4.A15 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* abgedeckt.
- *SYS.1.8.A5 Protokollierung bei Speichersystemen:* Diese Anforderung ist bereits durch die Anforderung OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene* im übergreifenden Baustein OPS.1.1.5 *Protokollierung* abgedeckt.

- SYS.1.8.A12 *Schulung der Administratoren:* Diese Anforderung ist bereits durch die Anforderung OPS.1.1.2.A10 *Fortbildung und Information* im übergreifenden Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* abgedeckt.

Änderungsdokument zum Baustein: SYS.2.1 Allgemeiner Client

Kapitel 2: Gefährdungslage

- Die Gefährdung *Software-Schwachstellen oder -Fehler* wurde entfernt, da sie nicht spezifisch für Client-IT-Systeme ist.

Kapitel 3: Anforderungen

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.A1 *Sichere Benutzerauthentisierung*: Nutzung von Bildschirmsperre und Abmelden von Benutzern aus SYS.2.1.A5 *Verwendung einer Bildschirmsperre* sowie SYS.2.1.A22 *Abmelden nach Aufgabenerfüllung* ergänzt. Allgemeiner Verweis zu Passwörtern entfernt, dies wird umfassend in ORP.4 *Identitäts- und Berechtigungsmanagement* und insbesondere in ORP.4.A8 *Regelung des Passwortgebrauchs* und ORP.4.A9 *Identifikation und Authentisierung* behandelt.
- SYS.2.1.A6 *Einsatz von Schutzprogrammen gegen Schadsoftware*: Die Anforderung wurde mit Fokus auf Client-Systeme neu konzipiert. Allgemeine Aspekte zum Thema finden sich in OPS.1.1.4 *Schutz vor Schadprogrammen*, insbesondere in OPS.1.1.4.A3 *Auswahl eines Virenschutzprogrammes* und OPS.1.1.4.A5 *Betrieb und Konfiguration von Virenschutzprogrammen*.
- SYS.2.1.A10 *Planung des Einsatzes von Clients*: Planung von Authentisierung und Benutzerverwaltung entfernt. Dies ist Teil des Identitäts- und Berechtigungsmanagement, insbesondere ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen*.
- SYS.2.1.A14 *Updates und Patches für Firmware, Betriebssystem und Anwendungen*: Allgemeine Aspekte bezüglich Patches entfernt, da diese in OPS.1.1.3.A15 *Regelmäßige Bewertung und Implementierung von Sicherheitskorrekturen* und OPS.1.1.3.A16 *Regelmäßige Suche nach Informationen zu Patches und Schwachstellen* behandelt werden. Die Anforderung beschreibt nun schwerpunktmäßig den Einsatz von Software abhängig vom verfügbaren Support.
- SYS.2.1.A15 *Sichere Installation und Konfiguration von Clients*: Zeitliche Reihenfolge der Schritte bei Installation und Konfiguration präzisiert.
- 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, dies ist über den Baustein APP.1.2 *Webbrowser* zu regeln und insbesondere abgedeckt in APP.1.2.A2 *Unterstützung sicherer Verschlüsselung der Kommunikation*.
- 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 zur Sicherung von verschlüsselten Daten entfernt, dies ist behandelt in CON.3.A13 *Einsatz kryptografischer Verfahren bei der Datensicherung*. 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.
- SYS.2.1.A34 *Einsatz von Anwendungsisolation*: Umbenannt in *Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten*. Es wird nun sowohl der Ausbruch aus einer Anwendung als auch der Zugriff von Betriebssystemkomponenten auf Daten in Anwendungen behandelt.
- SYS.2.1.A39 *Unterbrechungsfreie und stabile Stromversorgung*: Weiterführende inhaltliche Anforderungen an die unterbrechungsfreie Stromversorgung und den Überspannungsschutz entfernt. Diese sind abgedeckt durch INF.2.A3 *Einsatz einer unterbrechungsfreien Stromversorgung* sowie INF.3.A6 *Überspannungsschutz*.
- SYS.2.1.A41 *Verhinderung der Überlastung der lokalen Festplatte*: Die Anforderung wurde umbenannt in *Verwendung von Quotas für lokale Datenträger*, um den Inhalt besser zu erfassen.

Entfernung von Anforderungen

- SYS.2.1.A2 *Rollentrennung*: Entfallen. Die Aspekte dieser Anforderung sind in den Bausteinen OPS.1.1.2 *Ordnungsgemäße IT-Administration* sowie ORP.4 *Identitäts- und Berechtigungsmanagement* zu finden, insbesondere in den Anforderungen OPS.1.1.2.A6 *Schutz administrativer Tätigkeiten* sowie ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen*.
- SYS.2.1.A4 *Regelmäßige Datensicherung*: Entfallen. Eine umfassende Darstellung aller Aspekte dieser Anforderung, wie ein Datensicherungskonzept aufgebaut wird, ist im Baustein CON.3 *Datensicherungskonzept* zu finden.
- SYS.2.1.A5 *Verwendung einer Bildschirmsperre*: Entfallen, da inhaltlich nun in SYS.2.1.A1 *Sichere Benutzerauthentisierung* integriert.
- SYS.2.1.A7 *Protokollierung auf Clients*: Entfallen, da das Thema umfassend in OPS.1.1.5 *Protokollierung* behandelt wird, insbesondere ist OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene* relevant.
- SYS.2.1.A12 *Kompatibilitätsprüfung von Software*: Entfallen, da die beschriebenen Aspekte umfassend durch den im Baustein APP.6 *Allgemeine Software* beschriebenen Lebenszyklus von Software sowie speziell durch OPS.1.1.3.A9 *Test- und Abnahmeverfahren für neue Hard- und Software* abgedeckt sind.
- SYS.2.1.A17 *Einsatzfreigabe für Clients*: Entfallen. Die Aspekte dieser Anforderung werden durch OPS.1.1.3.A9 *Test- und Abnahmeverfahren für neue Hardware* sowie OPS.1.1.6.A4 *Freigabe der Software* behandelt.
- SYS.2.1.A19 *Restriktive Rechtevergabe*: Entfallen, da redundant zu ORP.4 *Identitäts- und Berechtigungsmanagement*, insbesondere ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* sowie ORP.4.A3 *Dokumentation der Benutzerkennungen und Rechteprofile*.
- SYS.2.1.A22 *Abmelden nach Aufgabenerfüllung*: Entfallen, da inhaltlich nun in SYS.2.1.A1 *Sichere Benutzerauthentisierung* integriert.
- SYS.2.1.A25 *Mitarbeiterrichtlinie zur sicheren IT-Nutzung*: Entfallen. Diese Anforderung duplizierte Inhalte von ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*.

Änderungsdokument zum Baustein: SYS.2.2.2 Clients unter Windows 8.1

Kapitel 3: Anforderungen

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.A5 *Lokale Sicherheitsrichtlinien für Windows 8.1*: Deaktivierung nicht benötigter Anwendungen und Komponenten entfernt, da bereits abgedeckt durch SYS.2.1.A16 *Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen*.
- SYS.2.2.2.A18 *Aktivierung des Last-Access-Zeitstempels*: Mögliche Auswirkungen dieser Einstellung konkretisiert.

Entfernung von Anforderungen

- SYS.2.2.2.A6 *Datei- und Freigabeberechtigungen unter Windows 8.1*: Entfallen, da bereits abgedeckt durch ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen*.

Änderungsdokument zum Baustein: SYS.2.2.3 Clients unter Windows 10

Kapitel 3: Anforderungen

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.

Entfernung von Anforderungen

- SYS.2.2.3.A7 *Lokale Sicherheitsrichtlinien für Windows 10*: Diese Anforderung ist nun für alle Betriebssysteme verallgemeinert zu finden als SYS.2.1.A43 *Lokale Sicherheitsrichtlinien für Clients*.
- SYS.2.2.3.A8 *Zentrale Verwaltung der Sicherheitsrichtlinien von Clients*: Diese Anforderung ist nun für alle Betriebssysteme verallgemeinert zu finden als SYS.2.1.A44 *Verwaltung der Sicherheitsrichtlinien von Clients*.
- SYS.2.2.3.A10 *Konfiguration zum Schutz von Anwendungen unter Windows 10*: Diese Anforderung ist bereits durch SYS.2.1.A26 *Schutz vor Ausnutzung von Schwachstellen in Anwendungen* abgedeckt.

Änderungsdokument zum Baustein: SYS.2.3 Clients unter Linux und Unix

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.2.3.A1 *Authentisierung von Administratoren und Benutzern*: Der allgemeine Aspekt, dass Benutzer sich authentisieren müssen, wurde entfernt. Er ist bereits durch SYS.2.1.A1 *Sichere Benutzerauthentisierung* abgedeckt.
- SYS.2.3.A2 *Auswahl einer geeigneten Distribution*: Die Aspekte zu Rolling Releases und zur Verfügbarkeit von Updates und Support wurden entfernt. Sie sind unabhängig vom Betriebssystem abgedeckt in SYS.2.1.A14 *Updates und Patches für Firmware, Betriebssystem und Anwendungen*.
- SYS.2.3.A4 *Einspielen von Updates und Patches auf unixartigen Systemen*: Grundsätzliche Aspekte zu Updates und Patches entfernt, da redundant zu OPS.1.1.3 *Patch- und Änderungsmanagement*. Die Anforderung wurde entsprechend in *Kernel-Aktualisierungen auf unixartigen Systemen* umbenannt.
- SYS.2.3.A5 *Sichere Installation von Software-Paketen*: Allgemeine Anforderungen zu Software aus sicheren Quellen entfernt, da bereits durch APP6.A3 *Sichere Beschaffung von Software* gefordert.
- SYS.2.3.A7 *Restriktive Rechtevergabe auf Dateien und Verzeichnisse*: Anforderung zu minimalen Berechtigungen entfernt, da dies in ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* behandelt wird.

Entfernung von Anforderungen

- SYS.2.3.A3 *Nutzung von Cloud- und Online-Funktionen*: Entfallen. Die Anforderung wurde allgemeingültig in den Baustein SYS.2.1 *Allgemeiner Client* überführt und ist dort als SYS.2.1.A42 unter gleichem Titel zu finden.
- SYS.2.3.A16 *Zusätzliche Absicherung des Bootvorgangs*: Entfallen, da bereits durch SYS.2.1.A36 *Selbstverwalteter Einsatz von SecureBoot und TPM* abgdeckt.

Änderungsdokument zum Baustein: SYS.2.4 Clients unter macOS

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.2.4.A1 *Planung des sicheren Einsatzes von macOS*: Generische Anforderungen zu allgemeinen Administrationsaspekten entfernt. Die Themen Benutzerverwaltung, Administration und Protokollierung werden umfassend in den Bausteinen ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.2 *Ordnungsgemäße IT-Administration* und OPS.1.1.5 *Protokollierung* behandelt. Der Schutz vor Schadprogrammen wird für Clients in SYS.2.1.A6 *Einsatz von Viren-Schutzprogrammen* sowie für macOS in SYS.2.4.A9 *Verwendung von zusätzlichen Schutzprogrammen unter macOS* behandelt.

Änderungsdokument zum Baustein: SYS.3.1 Laptops

Kapitel 2: Gefährdungslage

- *Fehler bei der Synchronisation*: Gestrichen, da die beschriebenen Fehler bei der Synchronisation von Daten nicht spezifisch für Laptops sind.
- *Datenverlust bei mobilem Einsatz*: Gestrichen, da bereits durch Diebstahl und Verlust von Laptops abgedeckt und ein leerer Akku keinen Datenverlust erzwingt.
- *Datendiebstahl mithilfe von Laptops:* Gestrichen, da diese Gefährdung lediglich unspezifische Gefährdungen z. B. zur Nutzung drahtloser Netze dupliziert.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.3.1.A8 *Sicherer Anschluss von Laptops an Datennetze*: Allgemeine Aspekte zu Aspekten wie Schutz vor Schadprogrammen oder regelmäßige Aktualisierungen entfernt, die bereits durch spezifische Anforderungen zu den Themen abgedeckt sind.
- SYS.3.1.A9 *Sicherer Fernzugriff*: Allgemeine Forderung zur Absicherung des Laptops selbst entfernt, dies ergibt sich aus den übrigen 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.

Entfernung von Anforderungen

- SYS.3.1.A2 *Zugriffsschutz am Laptop*: Entfallen, da diese Anforderung auf Ebene des Betriebssystems umzusetzen ist und bereits durch SYS.2.1.A1 *Sichere Benutzerauthentisierung* abgedeckt wird.
- SYS.3.1.A4 *Einsatz von Antivirenprogrammen*: Entfallen, da diese Anforderung auf Ebene des Betriebssystems umzusetzen ist und bereits durch SYS.2.1.A6 *Einsatz von Viren-Schutzprogrammen* abgedeckt wird.
- SYS.3.1.A5 *Datensicherung*: Entfallen, da das Thema umfassend in CON.3 *Datensicherungskonzept* behandelt wird. Hier sind insbesondere CON.3.A4 *Erstellung eines Minimaldatensicherungskonzeptes* und CON.3.A5 *Regelmäßige Datensicherung* zu nennen.

Änderungsdokument zum Baustein: SYS.3.2.1 Allgemeine Smartphones und Tablets

Kapitel 2: Gefährdungslage

- Die Gefährdung *Rechteerhöhung durch Schwachstellen* wurde aus dem Baustein SYS.3.2.4 *Android* in den Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* verschoben.

Kapitel 3: Anforderungen

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 *Konfiguration des verwendeten DNS-Servers*
- SYS.3.2.1.A34 *Verwendung einer Firewall*: Die Anforderung wurde aus dem Baustein SYS.3.2.4 *Android* hierher verschoben.

Änderungen an bestehenden Anforderungen

- SYS.3.2.1.A3 *Sichere Grundkonfiguration für mobile Geräte*: Der Aspekt zum Thema MDM wurde entfernt, da dieser redundant zur Anforderung SYS.3.2.2.A5 *Installation des MDM Clients* ist.
- SYS.3.2.1.A5 *Updates von Betriebssystem und Apps*: Allgemeine Anforderungen an Updates entfernt, da dies redundant zur Anforderung OPS.1.1.3.A9 *Test- und Abnahmeverfahren für neue Hard- und Software* ist.
- SYS.3.2.1.A6 *Datenschutzeinstellung und Berechtigungen*: Die Anforderung wurde umbenannt. Aspekte zum Umgang mit Berechtigungseinstellungen wurden ergänzt.
- SYS.3.2.1.A7 *Verhaltensregeln bei Sicherheitsvorfällen*: Allgemeine Aspekte zu Sicherheitsvorfällen entfernt, da diese redundant zu den Anforderungen DER.1.A4 *Sensibilisierung der* Mitarbeiter und DER.2.1.A5 *Behebung von Sicherheitsvorfällen* sind.
- 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.

Entfernung von Anforderungen

- SYS.3.2.1.A14 *Schutz vor Phishing und Schadprogrammen im Browser*: Die Anforderung wurde entfernt, da sie redundant zur Anforderung APP.1.2.A11 *Überprüfung auf schädliche Inhalte* ist.
- SYS.3.2.1.A15 *Deaktivierung von Download-Boostern*: Die Anforderung ist entfallen, da diese für Allgemeine Smartphones und Tablets irrelevant ist.
- SYS.3.2.1.A17 *Verwendung der SIM-Karten-PIN*: Die Anforderung wurde entfernt, da sie redundant zur Anforderung SYS.3.3.A5 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen* ist.
- SYS.3.2.1.A20 *Auswahl und Freigabe von Apps*: Die Anforderung ist entfallen, da sie redundant zur Anforderung APP.6.A1 *Planung des Software-Einsatzes* ist.
- SYS.3.2.1.A21 *Definition der erlaubten Informationen und Applikationen auf mobilen Geräten*: Die Anforderung ist entfallen, da sie redundant zu den Anforderungen APP.6.A1 *Planung des Software-*

Einsatzes und APP.6.A3 *Sichere Beschaffung von Software ist.*

- SYS.3.2.1.A23 *Zusätzliche Authentisierung für vertrauliche Anwendungen*: Die Anforderung wurde entfernt, das sie redundant zur Anforderung APP.1.4.A14 *Unterstützung zusätzlicher Authentisierungsmerkmale bei Apps* ist.
- SYS.3.2.1.A24 *Einsatz einer geschlossenen Benutzergruppe*: Die Anforderung ist entfallen, da sie redundant zur Anforderung ORP.4.*A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen* ist.

Änderungsdokument zum Baustein: SYS.3.2.2 Mobile Device Management

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung, dass BYOD nicht im Fokus des Bausteins liegt, wurde eingefügt.
- Ergänzung zur Abgrenzung zum Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* wurde eingefügt.

Kapitel 3: Anforderungen

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.A5 *Sichere Konfiguration für mobile Endgeräte*: Anforderungstitel wurde in *Installation des MDM Clients* umbenannt. Allgemeine Aspekte zur Konfiguration wurden entfernt, da sie zur Anforderung SYS.3.2.1.A3 *Sichere Grundkonfiguration für mobile Geräte* redundant sind.
- SYS.3.2.2.A6 *Protokollierung des Gerätestatus*: Allgemeine Anforderungen an die Protokollierung wurden entfernt, da sie redundant zur Anforderung OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene* sind.
- SYS.3.2.2.A7 *Installation von Apps*: Allgemeine Anforderungen an die Auswahl und Freigabe von Apps wurden entfernt, da sie redundant zu den Anforderungen APP.6.A1 *Planung des Software-Einsatzes,* APP.6A2 *Erstellung eines Anforderungskatalogs für Software* und APP.6.A9 *Inventarisierung von Software* sind.
- *SYS.3.2.2.A12 Absicherung der MDM-Betriebsumgebung:* Allgemeine Anforderungen zur Patcheinspielung und Konfiguration wurden entfernt, da sie bereits aus den Anforderungen OPS.1.1.3.A15 *Regelmäßige Aktualisierung von IT-Systemen und Software* und ORP.4.A15 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* in Verbindung mit ORP.4.A2 *Einrichtung, Änderung und Entzug von Berechtigungen* hervorgehen.
- 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.

Entfernung von Anforderungen

- SYS.3.2.2.A8 *Festlegung erlaubter Informationen auf mobilen Endgeräten*: Entfallen, da redundant zu den Anforderungen SYS.3.2.1.A1 *Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets* und SYS.3.2.1.A26 *Nutzung von PIM-Containern.*
- SYS.3.2.2.A9 Auswahl und Installation von Sicherheits-Apps: Entfallen, da redundant zur Anforderung SYS.3.2.1.A33 *Auswahl und Installation von Sicherheits-Apps.*
- SYS.3.2.2.A10 *Sichere Anbindung der mobilen Endgeräte an die Institution*: Entfallen, da redundant zur Anforderung SYS.3.2.1.A28 *Verwendung der Filteroption für Webseiten.*
- SYS.3.2.2.A11 *Berechtigungsmanagement im MDM*: Entfallen, da redundant zu APP.6.A4 *Regelung für die Installation und Konfiguration von Software.*

Kapitel 4: Weiterführende Informationen

- Der "Mindeststandard des BSI für Mobile Device Management nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 11.05.2017" zum Thema MDM wurde als weitere Literatur ergänzt.

Änderungsdokument zum Baustein: SYS.3.2.3 iOS (for Enterprise)

Kapitel 2: Gefährdungslage

- Konkretisierung und Aktualisierung der Gefährdungslage.
- Die Gefährdung *Fehlende oder schlechte Qualität des Zugangsschutzes* wurde entfernt, da die dagegen wirkende Anforderung in den übergeordneten Baustein SYS.3.2.1 *Allgemeines Smartphone und Tablet* verschoben wurde.
- *Die Gefährdung Software-Schwachstellen in Apps* wurde entfernt, da die dagegen wirkende Anforderung in den übergeordneten Baustein SYS.3.2.1 *Allgemeines Smartphone und Tablet* verschoben wurde.
- Die Gefährung *Missbrauch biometrischer Authentisierung* wurde entfernt, da das Thema in ORP.4.A13 *Geeignete Auswahl von Authentisierungsmechanismen* behandelt wird.
- *Die Gefährdung Missbrauch vertraulicher Daten im gesperrten Zustand* wurde entfernt, da die dagegen wirkende Anforderung in den übergeordneten Baustein SYS.3.2.1 *Allgemeines Smartphone und Tablet* verschoben wurde.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.3.2.3.A21 *Freigabe von Apps und Einbindung des Apple App Stores*: Allgemeine Anforderungen an Apps entfernt, da redundant zu APP.1.4.A8 *Verhinderung von Datenabfluss.*

Entfernung von Anforderungen

- SYS.3.2.3.A10 *Verwendung biometrischer Authentisierung*: Die Anforderung ist entfallen, da sie redundant zur Anforderung *ORP.4.A13 Geeigente Auswahl von Authentisierungsmechanismen* ist.
- SYS.3.2.3.A11 *Verwendung nicht personalisierter Gerätename*: Die Anforderung ist entfallen, da sie redundant zur Anforderung SYS.3.2.1.*A12 Verwendung nicht personalisierter Gerätenamen* ist.
- SYS.3.2.3.A20 *Einbindung der Geräte in die interne Infrastruktur via VPN*: Die Anforderung ist entfallen, da sie redundant zur Anforderung SYS.3.2.1.A22 *Einbindung mobiler Geräte in die interne Infrastruktur via VPN* ist.

Änderungsdokument zum Baustein: SYS.3.2.4 Android

Kapitel 2: Gefährdungslage

- Konkretisierung und Aktualisierung der Gefährdungslage.
- Die Gefährdung *Deaktivieren von Sicherheitsfunktionen* wurde neu aufgenommen.
- Die Gefährdung *Rechteerhöhung durch Schwachstellen* wurde in den übergeordneten Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* verschoben.

Neue Anforderungen

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

Entfernung von Anforderungen

- SYS.3.2.4.A1 *Auswahl von Android-basierten Geräten*: Entfallen, da die Anforderung redundant zur Anforderung SYS.3.2.1.A5 *Updates von Betriebssystem und Apps* ist.
- SYS.3.2.4.A4 *Regelung und Konfiguration von Cloud-Print*: Entfallen, da der Dienst von Google eingestellt wurde und die Anforderung somit irrelevant ist.
- SYS.3.2.4.A6 *Einsatz eines Produkts zum Schutz vor Schadsoftware*: Entfallen, da die Anforderung redundant zur Anforderung SYS.3.2.1.A33 *Auswahl und Installation von Sicherheits-Apps* ist.
- SYS.3.2.4.A7 *Verwendung einer Firewall*: Die Anforderung wurde in den übergeordneten Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* nach SYS.3.2.1.A35 *Verwendung einer Firewall* verschoben.

Änderungsdokument zum Baustein: SYS.3.3 Mobiltelefon

Kapitel 1.3: Abgrenzung und Modellierung

- In der Abgrenzung wurde der Hinweis auf den Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* aufgenommen.

Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.3.3.A5 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*: Die Teilanforderung zur Nutzung von PIN/PUK wurde auf aufgenommen.

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.
- SYS.3.3.A5 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*: Hinweis auf Benutzerschulung entfernt, da dieser redundant zu SYS.3.3.A3 *Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen* ist.
- SYS.3.3.A12 *Einrichtung eines Mobiltelefon-Pools*: Hinweis zur Aufbewahrung wurde entfernt, da dieser redundant zu SYS.3.3.A3 *Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen* ist.

Umsortierung von Anforderungen

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

Änderungsdokument zum Baustein: SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung in Bezug auf Leasing, Tausch, Instandsetzung und Rückgabe von Geräten.
- Ergänzung der Abgrenzung gegenüber der Bausteinen der Schicht NET *Netze und Kommunikatio*n.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Unberechtigtes Kopieren und Scannen von Informationen* wurde in *Unkontrollierter Datenaustausch über Speicherschnittstellen bei Druckern, Kopierern und Multifunktionsgeräten* umbenannt und um den Aspekt Datenaustausch erweitert.
- Die Gefährdung *Fehlende Netztrennung* wurde in *Ungenügend abgesicherte Netzzugänge von Druckern, Kopierern und Multifunktionsgeräten* umbenannt und um den Aspekt Proxies erweitert.

Kapitel 3: Anforderungen

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.A2 *Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte*: Die Teilanforderung zu Passwörtern wurde entfernt, da redundant zu der Anforderung ORP.4.A8 *Regelung des Passwortgebrauchs* des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement*.
- 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* unbenannt.
- SYS.4.1.A18 K*onfiguration 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, der Aspekt zum SNMP Set Community Name wurde entfernt.
- SYS.4.1.A20 *Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten*: Die Teilanforderung zur verschlüsselten Übertragung wurde entfernt, da diese redundant zu Anforderung SYS.4.1.A15 *Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten* ist.
- SYS.4.1.A21 *Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten*: Zuständigkeit zum IT-Betrieb wurde hervorgehoben.

Entfernung von Anforderungen

- SYS.4.1.A12 *Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln*: Die Vorgaben dieser Anforderung gehen nicht über die Vorgaben der Anforderung CON.6.A2 *Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen* des Bausteins CON.6 *Löschen und Vernichten* hinaus.
- SYS.4.1.A19 *Sicheres Löschen von Informationen bei Druckern, Kopierern und Multifunktionsgeräten*: Die Vorgaben dieser Anforderung gehen nicht über die Vorgaben der Anforderung CON.6.A2 *Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen* des Bausteins CON.6 *Löschen und Vernichten* hinaus.

Änderungsdokument zum Baustein: SYS.4.3 Eingebettete Systeme

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.4.3.A1 *Regelungen zum Umgang mit eingebetteten Systemen:* Die Teilanforderung zum Thema Schulung wurde entfernt, da sie redundant zur Anforderung ORP.3.A3 *Einweisung des Personals in den sicheren Umgang mit IT* ist.
- SYS.4.3.A4 *Erstellung von Beschaffungskriterien für eingebettete Systeme*: Der Aspekt zum Thema Trusted Plattform Module (TPM) wurde eingefügt.

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* Si*cherheitszonen* 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.*

- INF.1.A21 *Unabhängige elektrische Versorgungsstränge:* Entfallen, da redundant zu INF.12.A14 *A-B-Versorgung.*
- INF.1.A28 *Klimatisierung durch raumlufttechnische Anlagen*: Entfallen, da kein Bezug zur Informationssicherheit besteht, sondern dies Aspekte der Arbeitsstättenrichtlinie beinhaltet.
- INF.1.A29 *Organisatorische Vorgaben für die Gebäudereinigung*: Entfallen, da redundant zu ORP.1.A3 *Beaufsichtigung oder Begleitung von Fremdpersonen* und ORP.2.A4. *Festlegung von Regelungen für den Einsatz von Fremdpersonal.*
- INF.1.A33 *Anordnung schützenswerter Gebäudeteile*: Entfallen, da redundant zu Anforderung INF.1.A9 *Sicherheitskonzept für die Gebäudenutzung*.

Änderungsdokument zum Baustein: INF.2 Rechenzentrum sowie Serverraum

Kapitel 1.3: Abgrenzung und Modellierung

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

Kapitel 2: Gefährdungslage

- Sprachliche Anpassungen im Zusammenhang mit der Unterscheidung des Betriebsbereichs ggü. dem gesamten Rechenzentrum.
- Umbenennung von der Gefährdung *Unberechtigter Zutritt* in *Fehlende oder fehlerhafte Zutrittskontrollen,* um den Fokus des Beispiels zu verdeutlichen.
- *Unzureichende Trassendimensionierung* ist entfallen, da eher für Gebäude relevant.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- Sprachliche Anpassungen im Zusammenhang mit der Unterscheidung des Betriebsbereichs ggü. dem gesamten Rechenzentrum.
- INF.2.A6 *Zutrittskontrolle*: Sprachliche Anpassungen zum besseren Verständnis. Teilanforderungen entfallen, die redundant sind zu ORP.4.A5 *Vergabe von Zutrittsberechtigungen*.
- 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.
- 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.A24 *Einsatz von Videoüberwachungsanlagen*: Redundante Teilanforderungen zum Aufbau wurden entfernt. Sprachliche Schärfung der Teilanforderungen zur Abstimmung mit dem Datenschutzbeauftragten.
- INF.2.A25 *Redundante Auslegung von unterbrechungsfreien Stromversorgungen:* Neuformulierung der Anforderung zur besseren Vereinbarkeit mit der A-B-Versorgung.

- INF.2.A29 *Vermeidung und Überwachung nicht erforderlicher Leitungen*: Sprachliche Anpassung der Teilanforderung zur Minimierung des von Leitungen ausgehenden Risikos.
- INF.2.A30 *Anlagen zur Erkennung, Löschung oder Vermeidung von Bränden*: Die Teilanforderungen zur Brandfrüherkennung wurden nach INF.2.A17 *Brandfrüherkennung* verschoben.

Entfernung von Anforderungen

- INF.2.A20 *Regelmäßige Aktualisierungen der Dokumentation*: Entfallen, da redundant zu INF.1.A36 *Regelmäßige Aktualisierungen der Dokumentation.*
- INF.2.A27 *Durchführung von Alarmierungs- und Branschutzübungen*: Entfallen, da redundant zu INF.1.A20 *Alarmierungsplan und Brandschutzübungen*.

Kapitel 4: Weiterführende Informationen

- Das Kapitel wurde um Verweise auf weitere BSI-Publikationen ergänzt.

Änderungsdokument zum Baustein: INF.5 Raum sowie Schrank für technische Infrastruktur

Kapitel 3: Anforderungen

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 *Stormversorgung*: Die Anforderung wurde in eine Basis-Anforderung überführt (vorher Standard-Anforderung), da sie entsprechend konkretisiert wurde.

Entfernung von Anforderungen

- INF.5.A21 *Redundante Leitungstrassen*: Entfallen, da redundant zu Baustein INF.12 Verkabelung, speziell INF.12.A10 *Dokumentation der Verkabelung,* INF.12.A14 *A-B-Versorgung* und INF.12.A17 *Redundanzen für die IT-Verkabelung.*

Änderungsdokument zum Baustein: INF.7 Büroarbeitsplatz

Kapitel 2: Gefährdungslage

- Die Gefährdung *Vandalismus* wurde entfernt, da sie nicht weiter relevant für den Baustein ist.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

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

Entfernung von Anforderungen

- INF.7.A4 *Zutrittsregelungen und -kontrolle*: Entfallen, da redundant zu INF.1.A7 *Zutrittsregelung und -kontrolle.*

Änderungsdokument zum Baustein: INF.8 Häuslicher Arbeitsplatz

Kapitel 2: Gefährdungslage

- Die Gefährdung *Gefährdung durch Reinigungs oder Fremdpersonal* wurde entfernt, da sie nicht weiter relevant für den Baustein ist.

Änderungsdokument zum Baustein: INF.9 Mobiler Arbeitsplatz

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlendes Sicherheitsbewusstsein und Sorglosigkeit im Umgang mit Informationen* wurde entfernt, da sie nicht weiter im Baustein thematisiert wird.

Kapitel 3: Anforderungen

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.

Neue Anforderungen

- INF.9.A12 *Nutzung eines Bildschirmschutzes*

Änderungsdokument zum Baustein: INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- INF.10.A2 *Beaufsichtigung von Besuchern*: Entfallen, da redundant zu ORP.1.A3 *Beaufsichtigung oder Begleitung von Fremdpersonen.*

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.