Bundesamt
für Sicherheit in der
Informationstechnik

Änderungen in der Edition 2023 des IT-Grundschutz-Kompendiums

Inhaltsverzeichnis

Neues im IT-Grundschutz-Kompendium 4
Neue Bausteine 4
Entfallene Bausteine 4
Überarbeitete Bausteine 4
Überarbeitung von Rollen 5
Aktualisierungen aller Kreuzreferenztabellen und strukturelle Anpassung der Bausteine 6
Errata und überarbeitete Bausteine 6
Geschlechtergerechtere Sprache 7

Änderungsdokument zum Baustein ORP.1 Organisation 8
Kapitel 3: Anforderungen 8

Änderungsdokument zum Baustein CON.1 Kryptokonzept 9
Kapitel 1.3: Abgrenzung und Modellierung 9
Kapitel 2: Gefährdungslage 9
Kapitel 3: Anforderungen 9
Kapitel 4: Weiterführende Informationen 10

Änderungsdokument zum Baustein CON.2 Datenschutz 11
Kapitel 1.1: Einleitung 11
Kapitel 1.3: Abgrenzung und Modellierung 11

Änderungsdokument zum Baustein OPS.1.1.2 Ordnungsgemäße IT-Administration 12
Kapitel 3: Anforderungen 12

Änderungsdokument zum Baustein OPS.1.1.3 Patch- und Änderungsmanagement 13
Kapitel 1.3: Abgrenzung und Modellierung 13
Kapitel 3: Anforderungen 13

Änderungsdokument zum Baustein OPS.1.2.5 Fernwartung 14
Kapitel 1.3: Abgrenzung und Modellierung 14
Kapitel 2: Gefährdungslage 14
Kapitel 3: Anforderungen 14

Änderungsdokument zum Baustein APP.1.2 Webbrowser 15
Kapitel 3: Anforderungen 15

Änderungsdokument zum Baustein APP.2.1 Allgemeiner Verzeichnisdienst 16

Änderungsdokument zum Baustein APP.2.2 Active Directory Domain Service 17

Änderungsdokument zum Baustein APP.2.3 OpenLDAP 18
Kapitel 1.3: Abgrenzung und Modellierung 18
Kapitel 2: Gefährdungslage 18
Kapitel 3: Anforderungen 18

Änderungsdokument zum Baustein APP.5.3 Allgemeiner E-Mail-Client und -Server 19
Kapitel 3: Anforderungen 19

Änderungsdokument zum Baustein SYS.1.1 Allgemeiner Server 20
Kapitel 1.3: Abgrenzung und Modellierung 20
Kapitel 2: Gefährdungslage 20
Kapitel 3: Anforderungen 20

Änderungsdokument zum Baustein SYS.2.1 Allgemeiner Client 21
Kapitel 3: Anforderungen 21

Änderungsdokument zum Baustein SYS.2.2.3 Clients unter Windows 10 22

Kapitel 1.3: Abgrenzung und Modellierung 22
Kapitel 2: Gefährdungslage 22
Kapitel 3: Anforderungen 22

Änderungsdokument zum Baustein SYS.2.3 Clients unter Linux und Unix 23
Kapitel 3: Anforderungen 23

Änderungsdokument zum Baustein SYS.4.3 Eingebettete Systeme 24
Kapitel 2: Gefährdungslage 24
Kapitel 3: Anforderungen 24

Änderungsdokument zum Baustein SYS.4.5 Wechseldatenträger 25
Kapitel 2: Gefährdungslage 25
Kapitel 3: Anforderungen 25

Änderungsdokument zum Baustein IND.3.2 Fernwartung im industriellen Umfeld 26
Kapitel 1.3: Abgrenzung und Modellierung 26
Kapitel 2: Gefährdungslage 26
Kapitel 3: Anforderungen 26

Änderungsdokument zum Baustein INF.1 Allgemeines Gebäude 27
Kapitel 3: Anforderungen 27

Änderungsdokument zum Baustein INF.2 Rechenzentrum sowie Serverraum 28
Kapitel 3: Anforderungen 28

Änderungsdokument zum Baustein INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume 29
Kapitel 2: Gefährdungslage 29
Kapitel 3: Anforderungen 29

Neues im IT-Grundschutz-Kompendium

Die Edition 2023 des IT-Grundschutz-Kompendiums enthält insgesamt 111 IT-Grundschutz-Bausteine. Darunter sind zehn neue IT-Grundschutz-Bausteine sowie 101 Bausteine aus der Edition 2022. Drei Bausteine aus der Edition 2022 sind entfallen. Aus der Edition 2022 wurden 21 Bausteine für die Edition 2023 überarbeitet.

Neue Bausteine

Die folgenden zehn neuen IT-Grundschutz-Bausteine sind in fünf unterschiedlichen Schichten hinzugekommen:

- CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)*
- OPS.1.1.1 *Allgemeiner IT-Betrieb*
- OPS.2.3 *Nutzung von Outsourcing*
  Dieser Baustein ersetzt OPS.2.1 *Outsourcing für Kunden*.
- OPS.3.2 *Anbieten von Outsourcing*
  Dieser Baustein ersetzt OPS.3.1 *Outsourcing für Dienstleister*.
- APP.5.4 *Unified Communications und Collaboration (UCC)*
- SYS.1.2.3 *Windows Server*
- SYS.1.9 *Terminalserver*
- SYS.2.5 *Client-Virtualisierung*
- SYS.2.6 *Virtual Desktop Infrastructure*
- NET.3.4 *Network Access Control*

Entfallene Bausteine

Die folgenden Bausteine sind in der Edition 2023 entfallen:

- SYS.2.2.2 *Clients unter Windows 8.1*
  Der Support für das Betriebssystem endete am 10.01.2023. Windows 8.1 sollte daher nicht mehr eingesetzt werden.
- OPS.2.1 *Outsourcing für Kunden*
  Der Baustein wird durch OPS.2.3 *Nutzung von Outsourcing* ersetzt.
- OPS.3.1 *Outsourcing für Dienstleister*
  Der Baustein wird durch OPS.3.2 *Anbieten von Outsourcing* ersetzt.

Überarbeitete Bausteine

Nach der Veröffentlichung der letzten Edition des IT-Grundschutz-Kompendiums im Februar 2022 hat das IT-Grundschutz-Team zahlreiche wertvolle Rückmeldungen von IT-Grundschutz-Anwendern und -Anwenderinnen erhalten. Hinweise zu einzelnen Aspekten und Erfahrungswerte aus der beruflichen Praxis von Informationssicherheitsbeauftragten sowie weiteren erfahrenen Anwendenden tragen dazu bei, die Inhalte noch aktueller und praxistauglicher aufzubereiten. Die einzelnen Bausteintexte wurden daraufhin gesichtet und überarbeitet, sodass in der Edition 2023 insgesamt 21 IT-Grundschutz-Bausteine aktualisiert wurden.

Die IT-Grundschutz-Bausteine sind in einem unterschiedlichen Umfang überarbeitet worden. Die Änderungen sind wie folgt klassifiziert:

- **Umfangreiche Änderungen**, die Auswirkungen auf Zertifizierungsverfahren oder bestehende Sicherheitskonzepte haben können, sind vorliegend in separaten Änderungsdokumenten aufgeführt. Dies betrifft 21 Bausteine aus der Edition 2022.
- **Geringfügige sprachliche und redaktionelle Änderungen** sowie Überarbeitungen aus Gründen der besseren Verständlichkeit werden nicht in einem separaten Änderungsdokument aufgeführt. Bei IT-Grundschutz-Bausteinen, die entsprechend geringfügig bearbeitet wurden, ist lediglich das Datum in der Fußzeile auf die aktuelle Edition gesetzt worden. Dies betrifft alle Bausteine aus der Edition 2022, die nicht umfangreich geändert wurden.

IT-Grundschutz-Bausteine aus der Edition 2022, die überarbeitet wurden und zu denen ein Änderungsdokument verfügbar ist:

- ORP.1 *Organisation*
- CON.1 *Kryptokonzept*
- CON.2 *Datenschutz*
- OPS.1.1.2 *Ordnungsgemäße IT-Administration*
- OPS.1.1.3 *Patch- und Änderungsmanagement*
- OPS.1.2.5 *Fernwartung*
- APP.1.2 *Webbrowser*
- APP.2.1 *Allgemeiner Verzeichnisdienst*
- APP.2.2 *Active Directory*
  Der Baustein wurde in "Active Directory Domain Services" umbenannt.
- APP.2.3 *OpenLDAP*
- APP.5.3 *Allgemeiner E-Mail-Client und -Server*
- SYS.1.1 *Allgemeiner Server*
- SYS.2.1 *Allgemeiner Client*
- SYS.2.3 *Clients unter Linux und Unix*
- SYS.2.2.3 *Clients unter Windows 10*
  Der Baustein wurde in "Clients unter Windows" umbenannt und behandelt nun mit Windows 10 und 11 die einzigen beiden Versionen von Windows für Client-Systeme, die durch Microsoft Support erhalten.
- SYS.4.3 *Eingebettete Systeme*
- SYS.4.5 *Wechseldatenträger*
- IND.3.2 *Fernwartung im industriellen Umfeld*
- INF.1 *Allgemeines Gebäude*
- INF.2 *Rechenzentrum sowie Serverraum*
- INF.10 *Besprechungs-, Veranstaltungs- und Schulungsraum*

Überarbeitung von Rollen

Folgende Rollen wurden mit der Edition 2023 umbenannt:

Alte Rollenbezeichnung	Neue Rollenbezeichnung
Anforderungsmanager (Compliance Manager)	Compliance-Beauftragte
Bauleiter	Bauleitung

Benutzer	Benutzende
Bereichssicherheitsbeauftragter	Bereichssicherheitsbeauftragte
Brandschutzbeauftragter	Brandschutzbeauftragte
Datenschutzbeauftragter	Datenschutzbeauftragte
Entwickler	Entwickelnde
ICS-Informationssicherheitsbeauftragter	ICS-Informationssicherheitsbeauftragte
Informationssicherheitsbeauftragter (ISB)	Informationssicherheitsbeauftragte (ISB)
Mitarbeiter	Mitarbeitende
Notfallbeauftragter	Notfallbeauftragte
OT-Leiter	OT-Leitung
Planer	Planende
Tester	Testende

Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

Aktualisierungen aller Kreuzreferenztabellen und strukturelle Anpassung der Bausteine

Alle Bausteine der Edition 2022 wurden für die Edition 2023 strukturell überarbeitet.

Die Kreuzreferenztabellen, die die Anforderungen jedes Bausteins den elementaren Gefährdungen gegenüberstellen, wurden geprüft und überarbeitet. Zukünftig zeigen diese nur noch direkte Gefährdungen, die unmittelbar auf das Zielobjekt einwirken und die durch die Anforderungen aus dem Baustein behandelt werden. Hierbei werden nur noch direkte Beziehungen zwischen Elementaren Gefährdungen und Anforderungen aufgeführt. Indirekte Beziehungen, die aus direkten Beziehungen folgen, wurden entfernt. Dadurch steigt die Übersicht und der eindeutige Fokus wird auf die für das Zielobjekt relevanten Gefährdungen gesetzt. Durch die Überarbeitung entsteht weniger Aufwand, wenn die Kreuzreferenztabellen für eine Risikoanalyse genutzt werden.

Die Elementaren Gefährdungen, die für den jeweiligen Baustein relevant sind, werden nun nur noch in den Kreuzreferenztabellen aufgeführt. Diese werden separat auf den Webseiten des BSI veröffentlicht. Die Anlage "Kreuzreferenztabelle zu elementaren Gefährdungen" wurde in den einzelnen Bausteinen entfernt.

Errata und überarbeitete Bausteine

Trotz einer sorgfältigen, mehrstufigen Qualitätssicherung lassen sich Fehler und Unschärfen bei einem Werk vom Umfang des IT-Grundschutz-Kompendiums nicht immer vermeiden. Auch können aufgrund der schnellen Entwicklungszyklen in der Informationstechnik Konzepte und Anforderungen aus dem IT-Grundschutz zum Erscheinungsdatum der jeweiligen Edition nicht mehr vollständig zutreffen.

Anwendende, denen Fehler oder Probleme auffallen, sind dazu eingeladen, diese an *it-grundschutz@bsi.bund.de* zu melden. Alle Anmerkungen werden durch das IT-Grundschutz-Team geprüft und fließen geeignet in die nächste Edition des IT-Grundschutz-Kompendiums ein.

Im Jahresverlauf können außerdem Drafts von überarbeiteten Bausteinen erscheinen, die bereits entsprechend aktualisiert sind.

Notwendige Korrekturen, die nach Redaktionsschluss der aktuellen Edition auftreten, werden (falls vorhanden) in den „Errata zur Edition 2023“ auf den IT-Grundschutz-Webseiten unter https://bsi.bund.de/grundschutz in der Rubrik „IT-Grundschutz-Kompendium“ veröffentlicht. Sie ersetzen anderslautende Aussagen im IT-Grundschutz-Kompendium.

Geschlechtergerechtere Sprache

Im Sinne der Gleichbehandlung wurden für die Edition 2023 alle Bausteine des IT-Grundschutz-Kompendiums in eine geschlechtergerechtere Sprache überführt.

Änderungsdokument zum Baustein ORP.1 Organisation

Kapitel 3: Anforderungen

Neue Anforderungen

- ORP.1.A17 *Mitführverbot von Mobiltelefonen (H)*: Diese Anforderung wurde in diesen Baustein verschoben aus INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume*.

Änderungsdokument zum Baustein CON.1 Kryptokonzept

Kapitel 1.3: Abgrenzung und Modellierung

- Anpassung des Wordings: Anstelle des unspezifisches Begriffs "Krytpomodul" werden die konkreteren Begriffe Hardware und Software mit kryptografischen Funktionen verwendet.

Kapitel 2: Gefährdungslage

- Gefährdung 2.2 *Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptografischen Verfahren:* Verfahren wurde um weitere rechtliche Aspekte ergänzt und in *Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptografischen Verfahren in Hard- oder Software mit kryptografischen Funktionen* umbenannt.
- Gefährdung 2.4 *Software-Schwachstellen oder -Fehler in Kryptomodulen:* Umbenennung in *Schwachstellen oder Fehler in Hardware oder Software mit kryptografischen Funktione*n und mit 2.8 *Unautorisierte Nutzung eines Kryptomoduls* zusammengefasst.
- Gefährdung 2.5 *Ausfall eines Kryptomoduls:* Umbenennung in *Ausfall von Hardware mit kryptografischen Funktionen.*
- Gefährdung 2.7 *Fehler in verschlüsselten Daten oder kryptografischen Schlüsseln:* Ergänzung um Angriffe auf die Chiffrate.
- Gefährdung 2.8 *Unautorisierte Nutzung eines Kryptomoduls* wurde gestrichen.

Kapitel 3: Anforderungen

Neue Anforderungen

- CON.1.A19 *Erstellung eines Krypto-Katasters (S):* Neue Anforderung zur Dokumentation der eingesetzten kryptografischen Verfahren in einer Gesamtübersicht.
- CON.1.A20 *Manipulationserkennung für Hard- und Software mit kryptografischen Funktionen (H):* Neue Anforderung zur Vermeidung und Identifikation von Manipulation an kryptografischer Hardware.

Änderungen an bestehenden Anforderungen

- CON.1.A1 *Auswahl geeigneter kryptografischer Verfahren (B):* Ergänzung um den Zusammenhang zwischen Schlüssellänge und Einsatzdauer.
- CON.1.A2 *Datensicherung beim Einsatz kryptografischer Verfahren (B):* Anpassung an das aktualisierte Wording.
- CON.1.A4 *Geeignetes Schlüsselmanagement (B):* Die Anforderung wurde nach Basis verschoben. Ergänzung um Behandlung von voreingestellten Schlüsseln.
- CON.1.A5 *Sicheres Löschen und Vernichten von kryptografischen Schlüsseln* (S): Verweis auf Dokumentation im Kryptokonzept ergänzt.
- CON.1.A9 *Auswahl eines geeigneten kryptografischen Produkts (S)*: Die Anforderung wurde nach Standard verschoben und in *Festlegung von Kriterien für die Auswahl von Hard- oder Software mit kryptografischen Funktionen* umbenannt. Ergänzung um Aspekte aus CON.1.A8 *Erhebung der Einflussfaktoren für kryptografische Verfahren und Produkte*, um die wachsende Bedeutung der Kryptografie zu berücksichtigen.
- CON.1.A10 *Entwicklung eines Kryptokonzepts (S):* Die Anforderung wurde nach Standard verschoben, um die wachsende Bedeutung der Kryptografie zu berücksichtigen. Sammlung

aller wesentlichen Aspekte zur Kryptografie im Kryptokonzept als zentrales Dokument. Zusammenführung mit der Sicherheitsrichtlinie.

- CON.1.A15 *Reaktion auf praktische Schwächung eines Kryptoverfahrens (S):* Die Anforderung wurde nach Standard verschoben. Bezug zum Dokument "Kryptokonzept" ergänzt.
- CON.1.A16 *Physische Absicherung von Kryptomodulen (H):* Umbenennung in CON.1.A16 *Physische Absicherung von Hardware mit kryptografischen Funktionen.*
- CON.1.A17 *Abstrahlsicherheit (H)*: Um den Bezug zum Dokument Kryptokonzept ergänzt.
- CON.1.A18 *Kryptografische Ersatzmodule:* Umbenennung in CON.1.A18 *Kryptografische Ersatzhardware (H)* und Anpassung an Hardware mit kryptografischen Funktionen.

Umsortierung von Anforderungen

- CON.1.A4 *Geeignetes Schlüsselmanagement:* Die Anforderung wurde nach Basis verschoben.
- CON.1.A9 *Auswahl eines geeigneten kryptografischen Produkts*: Die Anforderung wurde nach Standard verschoben
- CON.1.A10 *Entwicklung eines Kryptokonzepts:* Die Anforderung wurde nach Standard verschoben.
- CON.1.A15 *Reaktion auf praktische Schwächung eines Kryptoverfahrens:* Die Anforderung wurde nach Standard verschoben.

Entfernung von Anforderungen

- CON.1.A3 *Verschlüsselung der Kommunikationsverbindungen*: Diese Anforderung ist entfallen, da die in CON.1.A3 geforderten Inhalte bereits in den konkreteren Bausteinen der NET, APP und SYS-Schicht behandelt werden.
- CON.1.A6 *Bedarfserhebung für kryptografische Verfahren und Produkte*: Die Inhalte dieser Anforderungen wurden überführt nach CON.1.A9 *Festlegung von Kriterien für die Auswahl von Hard- oder Software mit kryptografischen Funktionen,* um die Anforderungserhebung für Hard- oder Software mit kryptografischen Funktionen gebündelt zu behandeln.
- CON.1.A7 *Erstellung einer Sicherheitsrichtlinie für den Einsatz kryptografischer Verfahren und Produkte*: Die Inhalte dieser Anforderungen wurden nach CON.1.A10 *Erstellung des Kryptokonzepts* verschoben, um alle Aspekte hinsichtlich der Kryptografie gebündelt in einem Dokument zu dokumentieren.
- CON.1.A8 *Erhebung der Einflussfaktoren für kryptografische Verfahren und Produkte*: Entfallen und mit CON.1.A9 Auswahl eines geeigneten kryptografischen Produkts zusammengefasst.
- CON.1.A12 *Sichere Rollenteilung beim Einsatz von Kryptomodulen*: Diese Anforderung wurde entfernt, da der ehemalige Fokus des Bausteins auf Kryptomodule verworfen wurde und die Inhalte bereits von ORP.4.A4 *Aufgabenverteilung und Funktionstrennung* abgedeckt werden.
- CON.1.A13 *Anforderungen an die Betriebssystemsicherheit beim Einsatz von Kryptomodulen*: Diese Anforderung wurde im Zuge der Fokusverschiebung von kryptografischen Modulen auf Hard- und Software mit kryptografischen Funktionen entfernt.
- CON.1A.14 *Sensibilisierung und Schulung*: Die Anforderung wurde entfernt, da die Inhalte dieser Anforderung nicht über die generischen Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* hinausgehen.

Kapitel 4: Weiterführende Informationen

- Verweis auf den Leitfaden "Erstellung von Kryptokonzepten" entfernt, da dieser nicht mehr aktuell ist.

Änderungsdokument zum Baustein CON.2 Datenschutz

Kapitel 1.1: Einleitung

- Konzentrierung aller erläuternder Texte zum SDM in der Einleitung.
- Weitere Ausführung der rechtlichen Hintergründe und der Risikotypen im Bereich des Datenschutzes.

Kapitel 1.3: Abgrenzung und Modellierung

- Verschiebung der Informationen zum SDM in die Einleitung.
- Schärfung der Modellierungshinweise, sodass der Baustein auf den gesamten Informationsverbund anzuwenden ist.

Änderungsdokument zum Baustein OPS.1.1.2 Ordnungsgemäße IT-Administration

Dieser Baustein wurde komplett überarbeitet. Daher wird in diesem Dokument nur im Überblick aufgezeigt, wo sich die entfallenen Anforderungen wiederfinden, bzw. ab welcher Nummer die Anforderungen neu sind.

Kapitel 3: Anforderungen

Neue Anforderungen

Alle Anforderungen ab OPS.1.1.2.A21 *Regelung der IT-Administrationsrollen* sind neu.

Entfernung von Anforderungen

- OPS.1.1.2.A3 *Geregelte Einstellung von IT-Administratoren (B):* Diese Anforderung ist bereits durch die Bausteine ORP.2 *Personal* (A1 und A14) sowie OPS.1.1.1 *Allgemeiner IT-Betrieb* (A2) ausreichend abgedeckt.
- OPS.1.1.2.A9 *Ausreichende Ressourcen für den IT-Betrieb (S):* Diese Anforderung wurde verschoben nach OPS.1.1.1 *Allgemeiner IT-Betrieb (A5).*
- OPS.1.1.2.A10 *Fortbildung und Information (S):* Diese Anforderung ist bereits durch die Bausteine ORP.2 *Personal (A15)*, ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und ORP.1.1.1 *Allgemeiner IT-Betrieb* (A17) ausreichend abgedeckt.
- OPS.1.1.2.A12 *Regelungen für Wartungs- und Reparaturarbeiten (S):* Diese Anforderung wurde verschoben nach OPS.1.1.1 *Allgemeiner IT-Betrieb (A20).*
- OPS.1.1.2.A14 *Sicherheitsüberprüfung von Administratoren (H):* Diese Anforderung ist bereits durch den Baustein ORP. 2 *Personal* (A7 und A13) ausreichend abgedeckt
- OPS.1.1.2.A15 *Aufteilung von Administrationstätigkeiten (H):* Diese Anforderung wurde auf die Anforderungen OPS.1.1.2.A21 *Regelung der IT-Administrationsrollen* und OPS.1.1.2.A7 *Regelung der IT-Administrationstätigkeit* aufgeteilt.
- OPS.1.1.2.A20 *Verwaltung und Inbetriebnahme von Geräten (S):* Diese Anforderung wurde verschoben nach OPS.1.1.1 *Allgemeiner IT-Betrieb*. Der Aspekt Verwaltung wird dort in A7 und die Inbetriebnahme von Geräten in A8 betrachtet.

Änderungsdokument zum Baustein OPS.1.1.3 Patch- und Änderungsmanagement

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung in Bezug auf die Bedeutung der Begriffe "Patch" und "Änderung".

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- OPS.1.1.3.A15 *Regelmäßige Aktualisierung von IT-Systemen und Software (B):* Die Anforderung wurde um die Prüfung auf bekannte Schwachstellen in Patches und um den Aspekt Software- oder Hardwareprodukte ohne Herstellersupport erweitert.

Entfernung von Anforderungen

- OPS.1.1.3.A16 *Regelmäßige Suche nach Informationen zu Patches und Schwachstellen (B):* Diese Anforderung wurde verschoben in den neuen Baustein OPS.1.1.1 *Allgemeiner IT-Betrieb* (Anforderung A20).

Änderungsdokument zum Baustein OPS.1.2.5 Fernwartung

Kapitel 1.3: Abgrenzung und Modellierung

- Der Baustein OPS.1.1.7 *Systemmanagement* wurde in die Abgrenzung aufgenommen.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Unsichere und unkontrollierte Fremdnutzung der Fernwartungszugänge* wurde in *Fehlende Regelungen zur Fremdnutzung der Fernwartungszugänge* umbenannt.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- OPS.1.2.5.A10 *Verwaltung der Fernwartungswerkzeuge (S):* Anforderung umbenannt in *Umgang mit Fernwartungswerkzeugen*.
- OPS.1.2.5.A14 *Dedizierte Clients bei der Fernwartung (H)*: Die Anforderung wurde umbenannt in *Dedizierte Clients und Konten bei der Fernwartung*. Die Anforderung sieht nun ebenfalls vor, dedizierte Konten für die Fernwartung zu verwenden.

Änderungsdokument zum Baustein APP.1.2 Webbrowser

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.1.2.A9 *Einsatz einer isolierten Webbrowser-Umgebung (H)*: Die Formulierung der Anforderung wurde geschärft.
- APP.1.2.A13 *Nutzung von DNS-over-HTTPS (B)*: Die Anforderung wurde zielgenauer ausgerichtet.

Änderungsdokument zum Baustein APP.2.1 Allgemeiner Verzeichnisdienst

Der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* wurde zusammen mit dem Baustein APP.2.2 *Active Directory Domain Services* (ehemals Active Directory) komplett überarbeitet und neu aufgebaut, um der aktuellen Gefährdungslage und dem Stand der Technik gerecht zu werden.

Änderungsdokument zum Baustein APP.2.2 Active Directory Domain Service

Der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* wurde zusammen mit dem Baustein APP.2.2 *Active Directory Domain Services* (ehemals Active Directory) komplett überarbeitet und neu aufgebaut, um der aktuellen Gefährdungslage und dem Stand der Technik gerecht zu werden. Der Fokus des Bausteins APP.2.2 liegt nun auf der Serverrolle Active Directory Domain Services (AD DS), die die Funktionen eines Verzeichnisdienstes aggregiert.

Änderungsdokument zum Baustein APP.2.3 OpenLDAP

Kapitel 1.3: Abgrenzung und Modellierung

- Die Auflistung der Bausteine, in denen OpenLDAP mit betrachtet werden sollte, wurde an APP.2.1 *Allgemeiner Verzeichnisdienst* angeglichen.

Kapitel 2: Gefährdungslage

- Konkretisierung und Aktualisierung der Gefährdungslage.

Kapitel 3: Anforderungen

3.2. Änderungen an bestehenden Anforderungen

- APP.2.3.A6 *Sichere Authentisierung gegenüber OpenLDAP (B):* Der Aspekt zur Speicherung von Passwörtern wurde von DÜRFEN NUR auf SOLLTEN geändert.
- APP.2.3.A9 *Partitionierung und Replikation bei OpenLDAP (S)*: Die erste Teilanforderung wurde sprachlich neu formuliert, um Widersprüche zu vermeiden.
- APP.2.3.A10 *Sichere Aktualisierung von OpenLDAP (S)*: Ergänzung um zwei zusätzliche Teilanforderungen zur Prüfung von Overlays und Backends bei der Migration.
- APP.2.3.A11 *Einschränkung der OpenLDAP-Laufzeitumgebung (S)*: Überarbeitung der Anforderung mit Blick auf den Baustein SYS.1.6 *Containerisierung.*

Änderungsdokument zum Baustein APP.5.3 Allgemeiner E-Mail-Client und -Server

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.5.3.A1 *Sichere Konfiguration der E-Mail-Clients (B)*: Änderung eines Modalverbs (SOLLTE statt MUSS für die Änderung von Konfigurationen durch Benutzende) und Entfernung einer unnötigen Einschränkung.
- APP.5.3.A2 *Sicherer Betrieb von E-Mail-Servern (B)*: Schärfung der Anforderung im Bezug auf die Nutzung von Transportverschlüsselung. Neue Einschränkung zur Nutzung von unverschlüsselten Verbindungen. Die Struktur der Anforderung wurde überarbeitet.
- APP.5.3.A6 *Festlegung einer Sicherheitsrichtlinie für E-Mail (S)*: Entfernung eines redundanten Aufzählungspunktes.
- APP.5.3.A9 *Erweiterte Sicherheitsmaßnahmen auf dem E-Mail-Server (S)*: DomainKeys mit DKIM abgekürzt. Genauere Beschreibung, wie SPF verwendet werden soll.
- APP.5.3.A10 *Ende-zu-Ende-Verschlüsselung (H)*: Anforderung umbenannt in *Ende-zu-Ende-Verschlüsselung und Signatur*.
- APP.5.3.A12 *Überwachung öffentlicher Blacklists (H)*: Anforderung umbenannt in *Überwachung öffentlicher Block-Listen*.

Änderungsdokument zum Baustein SYS.1.1 Allgemeiner Server

Kapitel 1.3: Abgrenzung und Modellierung

- Modellierung des Bausteins verdeutlicht: Wenn für ein Server-Zielobjekt kein spezifischer Baustein existiert, müssen die Anforderungen aus SYS.1.1 *Allgemeiner Server* geeignet für das Zielobjekt konkretisiert und es muss eine ergänzende Risikobetrachtung für das Zielobjekt durchgeführt werden, um Eigenschaften zu betrachten, die nicht in SYS.1.1 behandelt werden. Dieses Vorgehen ergibt sich bereits aus der IT-Grundschutz-Methodik gemäß BSI-Standard 200-2, wurde aber häufig missverstanden. SYS.1.1 *Allgemeiner Server* ist für *jeden* Server zu modellieren, reicht aber *allein* nicht aus.
- Ergänzung, dass Benutzersitzungen auf Terminalservern als Dienst zu betrachten und durch den entsprechenden Baustein zu modellieren sind. Solche Sitzungen können also z. B. wie ein Client genutzt werden und unterliegen *nicht* den Einschränkungen, die für das zugrunde liegende Server-Betriebssystem gelten.

Kapitel 2: Gefährdungslage

- Die Gefährdung *Unzureichende Planung* wurde hinzugefügt. Sie stammt ursprünglich aus dem Community Draft zu SYS.1.2.3 *Windows Server 2019* (nun: SYS.1.2.3 *Windows Server*), ist aber gültig für alle Server.
- Die Gefährdung *Fehlerhafte Administration von Servern* wurde hinzugefügt. Sie stammt ursprünglich aus dem Community Draft zu SYS.1.2.3 *Windows Server 2019* (nun: SYS.1.2.3 *Windows Server*), ist aber gültig für alle Server.
- Die Gefährdung *Unberechtigtes Erlangen oder Missbrauch von Administratorrechten* wurde hinzugefügt. Sie stammt ursprünglich aus dem Community Draft zu SYS.1.2.3 *Windows Server 2019* (nun: SYS.1.2.3 *Windows Server*), ist aber gültig für alle Server.

Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.1.1.A39 *Zentrale Verwaltung der Sicherheitsrichtlinien von Servern (S)*: Die Anforderung stammt ursprünglich aus dem Community Draft zu SYS.1.2.3 *Windows Server 2019* (nun: SYS.1.2.3 *Windows Server*), ist aber gültig für alle Server.

Änderungen an bestehenden Anforderungen

- SYS.1.1.A1 *Geeignete Aufstellung (B)*: Die Anforderung wurde umbenannt in "Zugriffsschutz und Nutzung". Die Anforderung behandelt nun sowohl physische als auch virtualisierte Server. Es wurden Aspekte ergänzt, die sich mit dem Verbot der Nutzung als Arbeitsplatzrechner beschäftigen. Diese stammen ursprünglich aus dem Community Draft zu SYS.1.2.3 *Windows Server 2019* (nun: SYS.1.2.3 *Windows Server*), sind aber gültig für alle Server.
- SYS.1.1.A6 *Deaktivierung nicht benötigter Dienste (B)*: Konkretisierung der zu deaktivierenden Dienste.
- SYS.1.1.A16 *Sichere Grundkonfiguration von Servern (S)*: Die Anforderung wurde neu strukturiert und umfassend erweitert. Die Ergänzungen stammen ursprünglich aus dem Community Draft zu SYS.1.2.3 *Windows Server 2019* (nun: SYS.1.2.3 *Windows Server*), sind aber gültig für alle Server. In diesem Zuge wurde sie umbenannt in "Sichere Installation und Grundkonfiguration von Servern".

Änderungsdokument zum Baustein SYS.2.1 Allgemeiner Client

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.2.1.A11 *Beschaffung von Clients (S):* Teilanforderung bezüglich Rolling Releases ergänzt.

Entfernung von Anforderungen

- SYS.2.1.A14 *Updates und Patches für Firmware, Betriebssystem und Anwendungen (S):* Die Teilanforderung zu Rolling Releases wurde nach SYS.2.1.A11 verschoben (siehe oben). Die Teilanforderung zum notwendigen Herstellersupport bei der Beschaffung ist bereits durch APP.6.A3 *Sichere Beschaffung von Software* abgedeckt. Die Teilanforderung bezüglich Weiterbetrieb beim Entfall des Herstellersupports ist bereits durch OPS.1.1.3.A16 *Regelmäßige Suche nach Informationen zu Patches und Schwachstellen* abgedeckt.

Änderungsdokument zum Baustein SYS.2.2.3 Clients unter Windows 10

Der Baustein wurde umbenannt in SYS.2.2.3 *Clients unter Windows*. Entsprechend wurden alle Bezüge zu Windows 10 innerhalb des Bausteins in "Windows" verallgemeinert.

Mit dem Ende des erweiterten Supports für Windows 8.1 ist der Baustein SYS.2.2.2 *Clients unter Windows 8.1* entfallen, SYS.2.2.3 deckt neben Windows 10 nun auch Windows 11 und damit alle durch Microsoft unterstützten Client-Versionen des Betriebssystems ab.

Kapitel 1.3: Abgrenzung und Modellierung

- Der Baustein ist nun auch auf Clients mit dem Betriebssystem Windows 11 anzuwenden.

Kapitel 2: Gefährdungslage

- Aus der Gefährdung "Schadprogramme auf Windows-Clients" wurden allgemeine Ausführungen zu Auswirkungen von Schadprogrammen entfernt, da diese nicht spezifisch für Windows-Clients waren.

Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.2.2.3.A26 *Nutzung des Virtual Secure Mode (VSM) (H)*: Diese Anforderung entspricht der gleichnamigen Anforderung SYS.1.2.3.A8 aus dem Baustein SYS.1.2.3 *Windows Server*.

Änderungen an bestehenden Anforderungen

- SYS.2.2.3.A4 *Telemetrie und Datenschutzeinstellungen unter Windows (B)*: Präzisierung der Formulierung. In der Enterprise-Edition von Windows 10 oder 11 muss der Telemetrie-Level 0 konfiguriert werden. Andernfalls, insbesondere auch bei anderen Editionen des Betriebssystems, muss die Telemetrie durch andere Maßnahmen blockiert werden.

Änderungsdokument zum Baustein SYS.2.3 Clients unter Linux und Unix

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.2.3.A8 *Einsatz von Techniken zur Rechtebeschränkung von Anwendungen (S)*: Präzisierung, dass Rechte grundsätzlich entzogen und explizit erteilt werden sollten.
- SYS.2.3.A14 *Absicherung gegen Nutzung unbefugter Peripheriegeräte (H)*: Verallgemeinerung auf die Notwendigkeit zur Freigabe von Peripheriegeräten, um weitere Anwendungsszenarien abzudecken.

Änderungsdokument zum Baustein SYS.4.3 Eingebettete Systeme

Kapitel 2: Gefährdungslage

- Die Gefährdung *Hardwareausfall und Hardwarefehler bei eingebetteten Systemen* wurde um Aspekte der rauen Umgebungseinflüsse erweitert.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.4.3.A1 *Regelungen zum Umgang mit eingebetteten Systemen (B):* Die Anforderung wurde um die Erfassung und Dokumentation aller eingebetteten Systeme und Schnittstellen erweitert.
- SYS.4.3.A2 *Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen (B)*: Die Anforderung wurde um das Deaktivieren aller nicht benötigter Schnittstellen erweitert.
- SYS.4.3.A5 *Schutz vor schädigenden Umwelteinflüssen bei eingebetteten Systemen (S):* Die schädigenden Umwelteinflüsse wurden erweitert.
- SYS.4.3.A11 *Sichere Aussonderung eines eingebetteten Systems (S)*: Die Anforderung wurde teilweise umformuliert.

Änderungsdokument zum Baustein SYS.4.5 Wechseldatenträger

Kapitel 2: Gefährdungslage

- Die Gefährdung *Verbreitung von Schadprogrammen* wurde in *Verbreitung von Schadsoftware* umbenannt.

Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.4.5.A17 *Gewährleistung der Integrität und Verfügbarkeit bei Langzeitspeichern (S)*: Neue Standard-Anforderung mit dem Fokus auf langfristige Datenhaltung.

Änderungen an bestehenden Anforderungen

- SYS.4.5.A2 *Verlust- bzw. Manipulationsmeldung (B)*: Die Anforderung wurde umbenannt in *Verlust- und Manipulationsmeldung*. Es wurden Ergänzungen zum Umgang mit wiedergefundenen Wechseldatenträgern aufgenommen.
- SYS.4.5.A4 *Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern (S)*: Regelungen zum Anschließen von Wechseldatenträgern an fremde IT-Systeme wurden in der Aufzählung ergänzt. Das Verbot, private Wechseldatenträger zu nutzen, wurde ergänzt.
- SYS.4.5.A7 *Sicheres Löschen der Datenträger vor und nach der Verwendung (S)*: Die Anforderung wurde umbenannt in *Sicheres Löschen der Wechseldatenträger vor und nach der Verwendung*.
- SYS.4.5.A13 *Angemessene Kennzeichnung der Datenträger beim Versand (S)*: Die Anforderung wurde umbenannt in *Kennzeichnung der Wechseldatenträger beim Versand.*
- SYS.4.5.A15 *Zertifizierte Produkte (H)*: Anforderung umbenannt in *Verwendung zertifizierter Wechseldatenträger*.
- SYS.4.5.A16 *Nutzung dedizierter Systeme zur Datenprüfung (H)*: Anforderung umbenannt in *Nutzung dedizierter IT-Systeme zur Datenprüfung.*

Änderungsdokument zum Baustein IND.3.2 Fernwartung im industriellen Umfeld

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung des Verweises auf Baustein IND.2.7 *Safety Instrumented Systems*.

Kapitel 2: Gefährdungslage

- Die Gefährdung 2.5 *Direkte technische Zugriffsmöglichkeiten auf ICS aus unsicheren Zonen* wurde umbenannt in 2.5 *Direkte IP-basierte Zugriffsmöglichkeiten auf ICS aus unsicheren Zonen.*
- Die Gefährdung 2.7 *Unsichere technische Konzeption von OT-Fernwartungszugängen* wurde umbenannt in 2.7 *Unsichere Konzeption von OT-Fernwartungszugängen*.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- IND.3.2.A1 *Planung des Einsatzes der Fernwartung in der OT (B)*: Die Anforderung wurde um den Aspekt der gesetzlichen Vorgabe des Schutzes von Personen erweitert.
- IND.3.2.A3 *Regelmäßige Prüfungen sowie OT-Fernwartungszugänge (B)*: Die Teilanforderung zum Aspekt des Genehmigungsprozesses für Abweichungen vom Fernwartungskonzept ist nun eine MUSS-Anforderung, da Abweichungen in der Praxis zwar unvermeidbar sind, aber beobachtet und kontrolliert werden müssen.
- IND.3.2.A4 *Verbindliche Regelung der OT-Fernwartung durch Dritte (B)*: Die Anforderung wurde um den Aspekt des Schutzes von Personen erweitert.
- IND.3.2.A7 *Technische Entkopplung von Zugriffen (S)*: Die Teilanforderung zum Aspekt der Terminierung wurde dahingehend geändert, dass nach der Terminierung nicht zwingend ein anderes Protokoll verwendet werden muss als vor der Terminierung.
- IND.3.2.A10 *Beobachtung und Kontrolle von OT-Fernwartungssitzungen (S)*: Die Teilanforderung zum Aspekt des Personenschutzes wurde erweitert um den Schutz vor Sachschäden an Anlagen und Maschinen.

Änderungsdokument zum Baustein INF.1 Allgemeines Gebäude

Kapitel 3: Anforderungen

Umsortierung von Anforderungen

- INF.1.A3 *Einhaltung von Brandschutzvorschriften (B)*: Die Teilanforderung des IT-bezogenen Brandschutzkonzeptes wurde in eine Standard-Anforderung (INF.1.A9 *Sicherheitskonzept für die Gebäudenutzung*) überführt (vorher Basis-Teilanforderung: INF.1.A3 *Einhaltung von Brandschutzvorschriften*) .

Änderungsdokument zum Baustein INF.2 Rechenzentrum sowie Serverraum

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- INF.2.A9 *Einsatz einer Lösch- oder Brandvermeidungsanlage (B)*: Die Formulierung "In einem Rechenzentrum MUSS eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik installiert sein. Ist dies nicht möglich [...]" wurde angepasst und konkretisiert. Es wir nun eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik gefordert oder alternativ andere technische Maßnahmen wie eine flächendeckende Brandfrüherkennung mit entsprechenden organisatorischen Maßnahmen.

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

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlende oder unzureichende Regelungen* wurde um den Aspekt der vorhandenen Arbeitsmittel im Besprechungsraum konkretisiert.
- Die Gefährdung *Gefährdung durch Besucher* wurde entfernt, da diese bereits im übergreifenden Baustein ORP.1 *Organisation* behandelt wird.

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- INF.10.A10 *Mitführverbot von Mobiltelefonen (H)*: Diese Anforderung wurde verschoben nach ORP.1 *Organisation*.