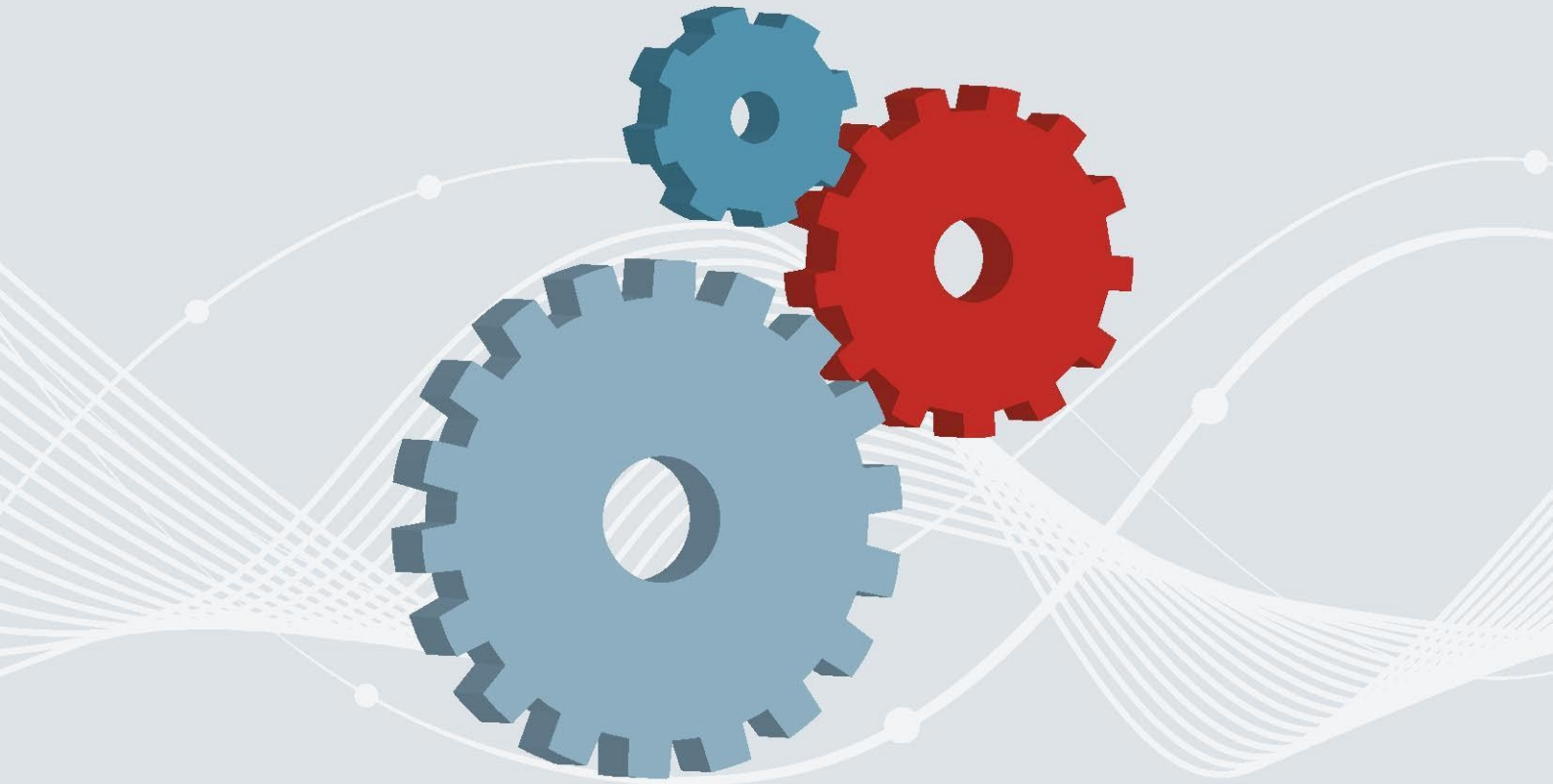
Bundesamt
für Sicherheit in der
Informationstechnik

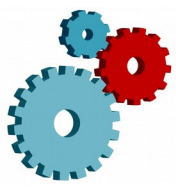


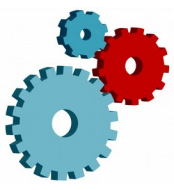
IT-Grundschutz-Kompendium

Änderungsdokumente zur Edition 2019

www.bsi.bund.de/grundschutz

Inhaltsverzeichnis





Einleitung

Für die Edition 2020 des IT-Grundschutz-Kompendiums wurden zahlreiche strukturelle Anpassungen an den IT-Grundschutz-Bausteinen vorgenommen, diese sind im Kapitel „Neues im IT-Grundschutz-Kompendium“ des Kompendiums beschrieben.

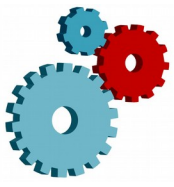
Zudem wurden alle Bausteine der Edition 2019 gesichtet und sprachlich sowie inhaltlich für die Edition 2020 in unterschiedlichem Umfang überarbeitet.

Die Änderungen sind wie folgt klassifiziert:

- **Umfangreiche Änderungen**, die Auswirkungen auf Zertifizierungsverfahren oder bestehende Sicherheitskonzepte haben können, sind im vorliegenden Dokument für alle betroffenen Bausteine aufgeführt.

- **Geringfügige sprachliche und redaktionelle Änderungen** sowie Überarbeitungen aus Gründen der besseren Verständlichkeit werden nicht separat aufgeführt. Für die Edition 2020 wurden alle Bausteine diesbezüglich überarbeitet.

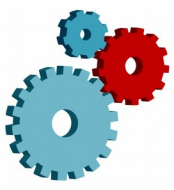
Stand: 18. Februar 2020



Verschobene und umbenannte Bausteine

Im Rahmen der Überarbeitung wurden einige Bausteine umbenannt bzw. in andere Schichten verschoben. Es handelt sich dabei um die folgenden Bausteine:

alt	**neu**
CON.5 *Entwicklung und Einsatz von Allgemeinen Anwendungen*	CON.5 *Entwicklung und Einsatz von Individualsoftware*
DER.3.2 *IS-Revision für Bundesbehörden*	DER.3.2 *Revisionen auf Basis des Leitfadens IS-Revision*
OPS.1.2.3 *Informations- und Datenträgeraustausch*	CON.9 *Informationsaustausch*
OPS.2.4 *Fernwartung*	OPS.1.2.5 *Fernwartung*
SYS.1.3 *Server unter Unix*	SYS.1.3 *Server unter Linux und Unix*
SYS.2.3 *Client unter Unix*	SYS.2.3 *Client unter Linux und Unix*
SYS.3.4 *Mobile Datenträger*	SYS.4.5 *Wechseldatenträger*

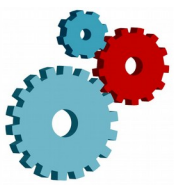


APP.1.1 *Office-Produkte*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

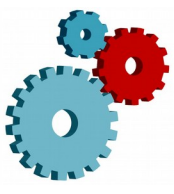
- APP.1.1.A2 *Einschränken von Aktiven Inhalten*: Benutzer als aktive Rolle entfernt.
- APP.1.1.A3 *Sicheres Öffnen von Dokumenten aus externen Quellen*: Benutzer als aktive Rolle hinzugefügt.
- APP.1.1.A7 *Installation und sichere Standardkonfiguration von Office-Produkten*: Freigabe der Standardkonfiguration wird nun explizit als SOLLTE-Anforderung gefordert.
- APP.1.1.A8 *Regelmäßige Versionskontrolle von Office-Produkten*: Teilanforderung zur Dokumentation der Konfiguration entfernt, da bereits durch APP.1.1.A7 abgedeckt.



APP.2.3 *OpenLDAP*

Kapitel 2: Gefährdungslage

- Die Gefährdung *Ausfall von Verzeichnisdiensten und Verschlüsselung* wurde entfernt, da sie bereits im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* enthalten ist.



APP.3.1 *Webanwendungen*

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Anwendung auf relevante Zielobjekte.

Kapitel 3: Anforderungen

Neue Anforderungen

- APP.3.1.A25 *Kryptografische Sicherung vertraulicher Daten*: Neue Anforderung, vertrauliche Daten sollten kryptographisch gesichert werden.

Änderungen an bestehenden Anforderungen

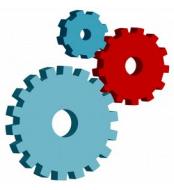
- APP.3.1.A1 *Authentisierung bei Webanwendungen*: Transportverschlüsselung aus Anforderung entfernt.
- APP.3.1.A2 *Zugriffskontrolle bei Webanwendungen*: Allgemeine Aspekte zu Zugriffsrechten aus Anforderung entfernt, die bereits aus anderen Anforderungen hervorgehen.
- APP.3.1.A8 *Systemarchitektur einer Webanwendung*: Aspekte zur Netzarchitektur aus Anforderung entfernt.
- APP.3.1.A11 *Sichere Anbindung von Hintergrundsystemen*: Aspekte zur Netzarchitektur aus Anforderung entfernt.
- APP.3.1.A13 *Restriktive Herausgabe sicherheitsrelevanter Informationen*: Aspekte zur Netzarchitektur aus Anforderung entfernt. Einzelheiten zu Sicherheitsmechanismen wurden entfernt, da eher Umsetzungshinweis als Anforderung.
- APP.3.1.A14 *Schutz vertraulicher Daten*: Kryptographische Sicherung vertraulicher Daten entfernt. Transportverschlüsselung aus Anforderung entfernt.
- APP.3.1.A15 *Verifikation essenzieller Änderungen*: Geeignete Authentisierung des Benutzer wird nun gefordert, wenn die Eingabe eines Passwortes nicht möglich ist.
- APP.3.1.A21 *Sichere HTTP-Konfiguration bei Webanwendungen*: Anforderung um weitere HTTP-Direktiven erweitert.
- APP.3.1.A23 *Verhinderung von Cross-Site-Request-Forgery*: Prüfung des HTTP-Referrer-Feldes entfernt.

Umsortierung von Anforderungen

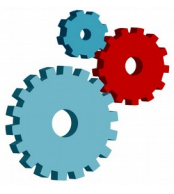
- APP.3.1.A14 *Schutz vertraulicher Daten*: Anforderung von Standard-Absicherung nach Basis-Absicherung verschoben.
- APP.3.1.A16 *Umfassende Eingabevalidierung und Ausgabekodierung*: Anforderung von Standard-Absicherung nach Basis-Absicherung verschoben.
- APP.3.1.A19 *Schutz vor SQL-Injection*: Anforderung von Standard-Absicherung nach Basis-Absicherung verschoben.

Entfernung von Anforderungen

- APP.3.1.A6 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*: Anforderung entfallen, da nicht spezifisch für diesen Baustein.



- APP.3.1.A10 *Test und Freigabe von Webanwendungen*: Anforderung entfallen, da nicht spezifisch für diesen Baustein.



APP.3.2 *Webserver*

Kapitel 1.3: Abgrenzung und Modellierung

- Webinhalte werden nun explizit im Baustein betrachtet.
- Der Bereich Outsourcing wurde abgegrenzt.

Kapitel 2: Gefährdungslage

- Einige Gefährdungen wurden inhaltlich überarbeitet.

Kapitel 3: Anforderungen

Neue Anforderungen

- APP.3.2.A20 *Benennung von Ansprechpartnern*: Für Webangebote müssen Prozesse und Ansprechpartner festgelegt werden.

Änderungen an bestehenden Anforderungen

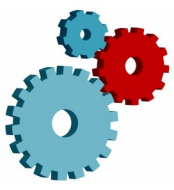
- APP.3.2.A2 *Schutz der Webserver-Dateien*: Anforderungen an den Zugriff auf Dateien und das WWW-Wurzelverzeichnis wurden spezifiziert. Verschlüsselte Übertragung von Daten wurde aus der Anforderung entfernt.
- APP.3.2.A3 *Absicherung von Datei-Uploads und -Downloads*: Speichern der abrufbaren Dateien auf einer separaten Partition wurde aus der Anforderung entfernt.
- APP.3.2.A5 *Authentisierung*: Sichere Verbindung aus Anforderung entfernt.
- APP.3.2.A10 *Auswahl eines geeigneten Webhosters*: Anforderungen, die in der Verantwortung des Webhoster liegen, wurden aus diesem Baustein entfernt.
- APP.3.2.A12 *Geeigneter Umgang mit Fehlern und Fehlermeldungen*: Anforderungen an die Ausgabe von Fehlermeldungen wurden spezifiziert.
- APP.3.2.A14 *Integritätsprüfungen und Schutz vor Schadsoftware*: Anforderung wurde spezifiziert.

Umsortierung von Anforderungen

- APP.3.2.A11 *Verschlüsselung über TLS*: Nach Basis verschoben. Eingegrenzt auf nicht vertrauenswürdige Netze.

Entfernung von Anforderungen

- APP.3.2.A6 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*: Anforderung entfallen, da nicht spezifisch für Webserver.
- APP.2.2.A19 *Einrichtung eines Internet-Redaktionsteams*: Anforderung entfallen, da Aspekte ausreichend in anderen Anforderungen berücksichtigt sind.



APP.3.3 *Fileserver*

Kapitel 2: Gefährdungslage

- Konkretisierung und Aktualisierung der Gefährdungslage.
- Die Gefährdung *Ungeeignete Aufstellung des Fileservers* wurde entfernt, da Aufstellung im Baustein SYS.1.1 *Allgemeiner Server* behandelt wird.
- Die Gefährdung *Fehlendes oder unzureichendes Datensicherungskonzept* wurde in *Datenverlust von auf Fileservern abgespeicherten Informationen* umbenannt.

Kapitel 3: Anforderungen

Neue Anforderungen

- APP.3.4.A15 *Planung von Fileservern*

Änderungen an bestehenden Anforderungen

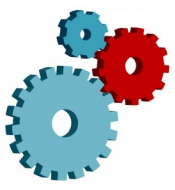
- APP.3.3.A3 *Einsatz von Antiviren-Programmen*: Redundante Teilanforderungen zu OPS.1.1.4 *Schutz vor Schadprogrammen* wurden entfernt.
- APP.3.3.A9 *Sicheres Speichermanagement*: Die Teilanforderung zur Katalogisierung von Speicherressourcen wurde entfernt.
- APP.3.3.A11 *Einsatz von Quotas*: Umbenennung in APP.3.3.A11 *Einsatz von Speicherbeschränkungen*
- *APP.3.3.A13 Replizieren zwischen Standorten*: Die Teilanforderung „Daten SOLLTEN zudem zwischen unabhängigen Geräten oder unabhängigen Standorten repliziert werden.“ wurde in „Daten SOLLTEN zudem zwischen unabhängigen Geräten, die sich zudem an unabhängigen Standorten befinden, repliziert werden.“ geändert, um bei einem erhöhten Schutzbedarf einen höheren Schutz zu erzielen.
- APP.3.3.A14 *Einsatz von Error-Correction-Codes*: Die Teilanforderung zu redundante Bits wurde entfernt

Umsortierung von Anforderungen

- APP.3.3.A14 *Einsatz von Error-Correction-Codes*: Die Anforderung wurde in eine Standard-Anforderung überführt (vorher Anforderung bei erhöhtem Schutzbedarf).

Entfernung von Anforderungen

- APP.3.3.A1 *Geeignete Aufstellung*: Die Anforderung ist bereits durch die Anforderung SYS.1.1.A1 *Geeignete Aufstellung* im übergreifenden Baustein SYS.1.1 *Allgemeiner Server* abgedeckt.
- APP.3.3.A4 *Regelmäßige Datensicherung*: Die Vorgaben dieser Anforderung gehen nicht über die Vorgaben des Bausteins *CON.3 Datensicherungskonzept* hinaus.
- APP.3.3.A10 *Regelmäßige Tests des Datensicherungs- bzw. Wiederherstellungskonzepts*: Die Anforderung ist bereits durch die Anforderung CON.3.A8 *Funktionstests und Überprüfung der Wiederherstellbarkeit* im übergreifenden Baustein CON.3 *Datensicherungskonzept* abgedeckt.



APP.3.4 *Samba*

Kapitel 2: Gefährdungslage

- Konkretisierung und Aktualisierung der Gefährdungslage.
- Die Gefährdung *Fehlerhafte Notfallvorsorge für Samba* wurde entfernt, da diese für jeden Dienst gilt.
- Die Gefährdung *Software-Schwachstellen oder -Fehler in Samba* wurde entfernt, da diese für jede Software gilt.

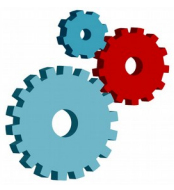
Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- APP.3.4.A1 *Planung des Einsatzes eines Samba-Servers:* Eine Teilanforderung zur Integration in das Konzept zum Schutz vor Schadprogrammen der Institution wurde aufgenommen.
- APP.3.4.A3 *Sichere Konfiguration des Betriebssystems für einen Samba-Server*: Anforderung wurde in *Sichere Konfiguration des Samba-Servers* umbenannt. Die Teilanforderung zu Netzports wurde präzisiert.
- APP.3.4.A4 *Sicherstellung der NTFS-Eigenschaften auf einem Samba-Server*: Anforderung wurde in *Vermeidung der NTFS-Eigenschaften auf einem Samba-Server* umbenannt.
- APP.3.4.A6 *Sichere Konfiguration von Winbind unter Samba*: Die Teilanforderung „Der Einsatz von Winbind SOLLTE sorgfältig geplant und geregelt werden." wurde entfernt.
- APP.3.4.A7 *Sichere Konfiguration von DNS unter Samba*: Die Teilanforderung „Wird Samba als primärer AD DC verwendet, SOLLTE der DNS-Dienst auf dem Samba-Server installiert und sorgfältig konfiguriert werden." wurde gestrichen.
- APP.3.4.A11 *Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers*: Die Teilanforderung zu Netware wurde entfernt.
- APP.3.4.A13 *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers*: Die Teilanforderung „Die Konfigurationsdaten, Statusinformationen und Systemdateien SOLLTEN kompatibel zueinander sein." wurde entfernt.

Entfernung von Anforderungen

- APP.3.4.A14 *Erstellen eines Notfallplans für den Ausfall von Samba-Servern*: Diese Anforderung ist bereits durch den übergreifenden Baustein DER.4 *Notfallmanagement* abgedeckt.



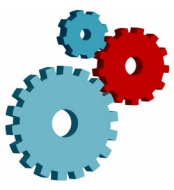
APP.3.6 *DNS-Server*

Änderungen an bestehenden Anforderungen

- APP.3.6.A10 *Auswahl eines geeigneten DNS-Server-Produktes:* Der Schulungsaspekt wurde gestrichen, da dies bereits in APP.3.6.A12 *Schulung der Verantwortlichen* adressiert wird.

Entfernung von Anforderungen

- APP.3.6.A5 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates:* Die Vorgaben dieser Anforderung gehen nicht über die Vorgaben des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* hinaus.



APP.5.1 *Allgemeine Groupware*

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung gegenüber den Bausteinen OPS.1.1.5 *Protokollierung* und OPS.1.2.2 *Archivierung*.

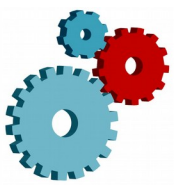
Kapitel 3: Anforderungen

Neue Anforderungen

- APP.5.1.A22 *Spam- und Virenschutz auf dem E-Mailserver*: Neue Basis-Anforderung zum Spam- und Virenschutz auf dem E-Mailserver.

Änderungen an bestehenden Anforderungen

- APP.5.1.A1 *Sichere Installation von Groupware-Systemen*: Schutz von Installationsquellen entfernt.
- APP.5.1.A2 *Sichere Konfiguration der Groupware-Clients*: Konfiguration der Clients besser beschrieben. Größenbeschränkungen für Postfächer entfernt.
- APP.5.1.A3 *Sicherer Betrieb von Groupware-Systemen*: Explizite Anforderung zur Transportverschlüsselung ergänzt. Größenbeschränkung für Postfächer ergänzt. Anforderungen an das Betriebssystem entfernt.
- APP.5.1.A4 *Datensicherung und Archivierung bei Groupware*: Allgemeine Aspekte der Archivierung entfernt, die aus anderen Bausteinen hervorgehen.
- APP.5.1.A6 *Festlegung von Vertretungsregelungen bei E-Mail-Nutzung*: Einhaltung datenschutzrechtlicher Aspekte und Benachrichtigung des Absenders ergänzt.
- APP.5.1.A7 *Planung des sicheren Einsatzes von Groupware-Systemen*: Sichere Dimensionierung des Systems ergänzt. Festlegung der übermittelten Informationen entfernt. Durchzuführende Planungen detaillierter beschrieben.
- APP.5.1.A8 *Festlegung einer Sicherheitsrichtlinie für Groupware*: Regelungen für Newsgroups und Mailinglisten ergänzt. Regelungen für den Umgang mit Dateianhängen und HTML-E-Emails ergänzt.
- APP.5.1.A12 *Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer*: Entfernung allgemeiner Schulungsanforderungen. Bessere Bezugnahme auf bestehende Schulungsmaßnahmen.
- APP.5.1.A16 *Umgang mit SPAM*: Regelungen für Newsgroups und Mailinglisten entfernt.
- APP.5.1.A17 *Auswahl eines Groupware- oder Mail-Providers*: Anforderung zur Vereinbarung von SLAs ergänzt.
- APP.5.1.A18 *Spam- und Virenschutz durch Einsatz eines E-Mail-Scanners auf dem Mailserver*: Anforderungstitel geändert zu *Erweiterter Spamschutz auf dem E-Mailserver*. Anforderung befasst sich nun mit Sender Policy Framework, DomainKeys und Domain-based Message Authentication, Reporting and Conformance.

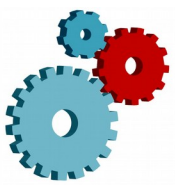


Umsortierung von Anforderungen

- APP.5.1.A7 *Planung des sicheren Einsatzes von Groupware-Systemen*: Die Anforderung wurde in eine Basis-Anforderung überführt (vorher Standard-Anforderung), da Planungsanforderungen für einen sicheren Betrieb grundsätzlich immer umgesetzt werden müssen.

Entfernung von Anforderungen

- APP.5.1.A5 *Festlegung der Kommunikationspartner*: Anforderung entfernt, da redundant mit Baustein CON.9 *Informationsaustausch*
- APP.5.1.A9 *Sichere Administration von Groupware-Systemen*: Anforderung entfernt, da keine groupwarespezifischen Inhalte vorhanden waren.
- APP.5.1.A10 *Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren*: Anforderung entfernt, da keine groupwarespezifischen Inhalte vorhanden waren.
- APP.5.1.A11 *Berechtigungsverwaltung für Groupware-Systeme*: Anforderung entfernt, da keine groupwarespezifischen Inhalte vorhanden waren.
- APP.5.1.A13 *Verifizierung der zu übertragenden Daten vor Weitergabe und Beseitigung von*
  Restinformationen: Anforderung entfernt, da redundant mit Baustein CON.9 *Informationsaustausch*.
- APP.5.1.A14 *Vermeidung problematischer Dateiformate*: Anforderung entfernt, da Inhalte nicht groupwarespezifisch bzw. redundant zu anderen Anforderungen waren.
- APP.5.1.A15 *Protokollierung von Groupware-Systemen*: Anforderung entfernt, da keine groupwarespezifischen Inhalte vorhanden waren.
- APP.5.1.A19 *Verschlüsselung von Groupware*: Anforderung entfernt, da Transportverschlüsselung nun als Basisanforderung in APP.5.1.A3 *Sicherer Betrieb von Groupware-Systemen* gefordert wird.
- APP.5.1.A20 *Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen*: Anforderung entfernt, da Inhalte durch den Baustein DER.4 *Notfallmanagement* abgedeckt werden.



APP.5.2 *Microsoft Exchange und Outlook*

Kapitel 3: Anforderungen

Neue Anforderungen

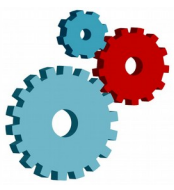
- APP.5.2.A19 *Erstellung einer Sicherheitsrichtlinie für Microsoft Exchange*: Neue Standard-Anforderung zur Sicherheitsrichtlinie für Microsoft Exchange und Outlook.

Änderungen an bestehenden Anforderungen

- Die Anforderungen des Bausteins wurden umfangreich überarbeitet. Insbesondere wurden Redundanzen beseitigt.

Entfernung von Anforderungen

- APP.5.2.A4 *Zugriffsrechte auf Microsoft Exchange-Objekte*: Entfallen, da keine spezifische Anforderung.
- APP.5.2.A6 *Sichere Installation eines Microsoft Exchange-Systems*: Entfallen, da keine spezifische Anforderung.
- APP.5.2.A8 *Sicherer Betrieb von Microsoft Exchange*: Entfallen, da keine spezifische Anforderung.
- APP.5.2.A13 *Schulung von Administratoren*: Entfallen, da keine spezifische Anforderung.
- APP.5.2.A16 *Erstellung eines Notfallplans für den Ausfall von Microsoft Exchange und Outlook*: Entfallen, da keine spezifische Anforderung.
- APP.5.2.A18 *Regelmäßige Sicherheitsprüfungen für Microsoft Exchange-Systeme*: Entfallen, da keine spezifische Anforderung.



CON.1 *Kryptokonzept*

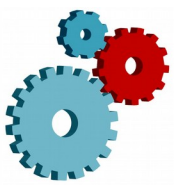
Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung gegenüber den Schichten APP *Anwendungen*, SYS *IT-Systeme* und NET *Netze und Kommunikation*.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- CON.1.A5 *Sicheres Löschen und Vernichten von kryptografischen Schlüsseln*: Die Teilanforderung zum Aspekt der sicheren Schlüsselablage ist entfernt worden, da diese in CON.1.A9 *Auswahl eines geeigneten kryptografischen Produkts verschoben wurde*.

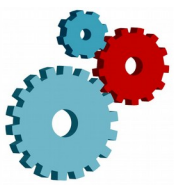


CON.2 *Datenschutz*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- CON.2.A1 *Umsetzung Standard-Datenschutzmodell*: Die Formulierung der Anforderung wurde verallgemeinert. Die Einhaltung gesetzlicher Vorgaben zum Datenschutz ist nun eine zwingende Anforderung („MUSS“). Wird das SDM nicht verwendet, so ist dies zu begründen („SOLLTE“).



CON.3 *Datensicherungskonzept*

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung gegenüber weiteren Bausteinen, die das Datensicherungskonzept um systemspezifische Anforderungen ergänzen.
- Entfernung des Verweises auf die Protokollierung und den damit verbundenen weiteren Bausteinen.

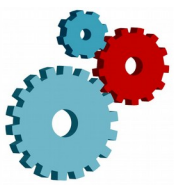
Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- CON.3.A1 *Erhebung der Einflussfaktoren für Datensicherungen*: Die Anforderung wurde um konkrete Rahmenbedingungen, die mindestens beachtet werden müssen, ergänzt.
- CON.3.A4 *Erstellung eines Minimaldatensicherungskonzeptes*: Die Anforderung wurde um konkrete Vorgaben an den Inhalt eines Minimaldatensicherungskonzepts ergänzt.
- CON.3.A6 *Entwicklung eines Datensicherungskonzepts*: Die Anforderung wurde um konkrete Vorgaben an den Inhalt eines Datensicherungskonzepts ergänzt.

Entfernung von Anforderungen

- CON.3.A3 *Ermittlung von rechtlichen Einflussfaktoren auf die Datensicherung:* Diese Anforderung ist bereits durch die Anforderung *CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen* abgedeckt.
- CON.3.A8 *Funktionstests und Überprüfung der Wiederherstellbarkeit:* Diese Anforderung ist bereits durch die Anforderung CON.3.A5 *Regelmäßige Datensicherung* abgedeckt.



CON.4 *Auswahl und Einsatz von Standardsoftware*

Kapitel 1.3: Abgrenzung und Modellierung

- Entfernung des Verweises auf OPS.1.2.6 *Verkauf und Aussonderung von IT*.

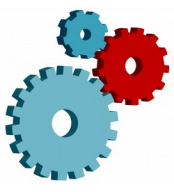
Kapitel 2: Gefährdungslage

- Die Gefährdung 2.4 *Manipulation von Daten durch Benutzer* wurde entfernt, da dieser Aspekt hinreichend durch die elementaren Gefährdungen abgedeckt wird.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- CON.4.A1 *Sicherstellen der Integrität von Standardsoftware*: Anpassung der Formulierung und Ergänzung des Verweises auf das Datensicherungskonzept.
- CON.4.A8 *Lizenzverwaltung und Versionskontrolle von Standardsoftware*: Die Anforderung wurde um den Aspekt der konkreten Nutzeranzahl und des korrekten Einsatzzwecks erweitert.



CON.5 *Entwicklung und Einsatz von* Individualsoftware

Der Baustein wurde von *Entwicklung und Einsatz von Allgemeinen Anwendungen* zu *Entwicklung und Einsatz von Individualsoftware* umbenannt, um die Abgrenzung zur Standardsoftware und dem damit verbundenen Baustein CON.4 *Auswahl und Einsatz von Standardsoftware* schon im Namen deutlich zu machen.

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung der Abgrenzung gegenüber dem Baustein CON.4: *Auswahl und Einsatz von Standardsoftware*, sowie dem Baustein CON.8 *Software-Entwicklung* und Fokussierung des Anwendungsbereichs des Bausteins auf Individualsoftware.
- Ergänzung der Abgrenzung gegenüber dem Baustein OPS.1.1.6. *Software-Tests und -Freigaben.*
- Ergänzung der Abgrenzung gegenüber dem Baustein *OPS.2.1 Outsourcing für Kunden bzw. OPS 3.1 Outsourcing für Dienstleister.*

Kapitel 2: Gefährdungslage

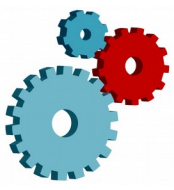
- Die Gefährdung *Verlust der Vertraulichkeit oder Integrität in Fachanwendungen* wurde entfernt, da dieser Aspekt hinreichend durch die elementaren Gefährdungen abgedeckt wird.
- Die Gefährdung *Softwareschwachstellen* wurde entfernt, da dieser Aspekt hinreichend durch die elementaren Gefährdungen abgedeckt wird.

Änderungen an bestehenden Anforderungen

- CON.5.A1 *Festlegung benötigter Sicherheitsfunktionen der Individualsoftware:* Anpassung des Anforderungstitels und Umformulierung der Anforderung im Zuge der Umbenennung des Bausteins.
- CON.5.A3 *Sichere Installation von Individualsoftware:* Anpassung des Anforderungstitels und Umformulierung der Anforderung im Zuge der Umbenennung des Bausteins.
- CON.5.A4 *Heranführen von Benutzerinnen und Benutzern an Individualsoftware:* Anpassung des Anforderungstitels und Umformulierung der Anforderung im Zuge der Umbenennung des Bausteins.
- CON.5.A6 *Dokumentation der Anforderungen an die Individualsoftware:* Anpassung des Anforderungstitels und Umformulierung der Anforderung im Zuge der Umbenennung des Bausteins.
- CON.5.*A9 Außerbetriebnahme von Individualsoftware:* Anpassung des Anforderungstitels und Umformulierung der Anforderung im Zuge der Umbenennung des Bausteins.

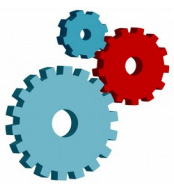
Umsortierung von Anforderungen

- CON.5.A11 *Geeignete und rechtskonforme Beschaffung*: Die Anforderung wurde in eine Standard-Anforderung überführt (vorher erhöhter Schutzbedarf), da eine geeignete und geregelte Beschaffung auch für den normalen Schutzbedarf erfolgen sollte.



Entfernung von Anforderungen

- CON.5.A2 *Test und Freigabe von Fachanwendungen:* Diese Anforderung ist bereits durch die Anforderungen im übergreifenden Baustein OPS.1.1.6 *Software-Tests und -Freigaben* abgedeckt.
- CON.5.A5 *Sicherer Betrieb von Individualsoftware*: Diese Anforderung ist bereits durch die Anforderungen in den übergreifenden Bausteinen OPS.1.1.3 *Patch- und Änderungsmanagement,* OPS.1.1.5 *Protokollierung*, CON.3 *Datensicherungskonzept* und ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt.
- CON.5.A7 *Erstellung eines Mandantenkonzeptes:* Diese Anforderung ist bereits durch die Anforderung OPS.3.1.A7 *Erstellung eines Mandantenkonzeptes durch den Outsourcing-Dienstleister* im übergreifenden Baustein OPS.3.1 *Outsourcing für Dienstleister* abgedeckt.
- CON.5.A10 *Notfallvorsorge für Anwendungen*: Diese Anforderung ist bereits durch die Anforderungen im übergreifenden Baustein DER.4 *Notfallmanagement* abgedeckt.



CON.7 *Informationssicherheit auf Auslandsreisen*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- CON.7.A1 *Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen:* Teilanforderung zur regelmäßigen Überprüfung der Umsetzung hinzugefügt.
- CON.7.A2 *Sensibilisierung der Mitarbeiter zur Informationssicherheit auf Auslandsreisen*: Präzisierung der Aufgaben des ISB als Teilanforderung.
- CON.7.A3 *Identifikation länderspezifischer Regelungen, Reise- und Umgebungsbedingungen*: Präzisierung der Berücksichtigung der Reise- und Umgebungsbedingungen als Teilanforderung.
- CON.7.A14 *Kryptografisch abgesicherte E-Mail-Kommunikation*: Präzisierung möglicher Sicherheitsmechanismen des Providers als Teilanforderung.

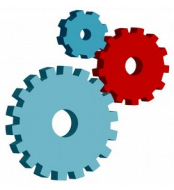
DER.1 *Detektion von sicherheitsrelevanten Ereignissen*

Kapitel 2: Gefährdungslage

- Die Gefährdung *Unzureichende Qualifikation der Verantwortlichen* wurde in *Unzureichende Qualifikation der Mitarbeiter* umbenannt und anhand von Beispielen konkretisiert.
- Die Gefährdung *Fehlende oder unzureichende Protokollierung* wurde in Bezug auf Prüfung von Protokollinformationen konkretisiert.

Änderungen an bestehenden Anforderungen

- DER.1.A5 *Einsatz von mitgelieferten Systemfunktionen zur Detektion:* Die Anforderung wurde geschärft.
- DER.1.A14 *Auswertung der Protokolldaten durch spezialisiertes Personal:* Die Anforderung wurde geschärft.



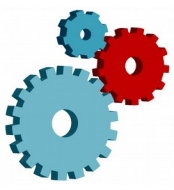
DER.2.1 *Behandlung von Sicherheitsvorfällen*

Kapitel 2: Gefährdungslage

- Die Gefährdung *Ungeeigneter Umgang mit Sicherheitsvorfällen* wurde um den Aspekt Einbruchdiebstahl erweitert.
- Die Gefährdung *Nicht erkannte Sicherheitsvorfälle* wurde entfernt und nach DER.1 *Detektion von sicherheitsrelevanten Ereignissen* verschoben.

Änderungen an bestehenden Anforderungen

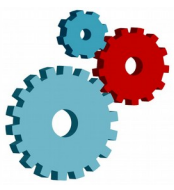
- DER.2.1.A3 *Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen:* Die Anforderung wurde geschärft.
- DER.2.1.A7 *Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen:* Die Anforderung wurde geschärft.
- DER.2.1.A8 *Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen:* Die Anforderung wurde geschärft.
- DER.2.1.A17 *Nachbereitung von Sicherheitsvorfällen:* Die Teilanforderung zum Aspekt „Unterrichtung der Leitungsebene bei sofortigem Handlungsbedarf“ ist nun eine MUSS-Teilanforderung, da hier die Dringlichkeit gegeben ist.
- DER.2.1.A18 *Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen:* Die Anforderung wurde geschärft.
- DER.2.1.A21 *Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen*: Die Anforderung wurde geschärft.



DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*

Änderungen an bestehenden Anforderungen

- DER.2.3.A8 *Etablierung sicherer, unabhängiger Kommunikationskanäle:* Die Anforderung wurde geschärft und um den Aspekt „Kommunikationsdienste Dritter“erweitert.

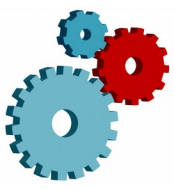


DER.3.1 *Audits und Revisionen*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- DER.3.1.A20 *Abschlussbesprechung*: Schärfung durch Umbenennung in *Durchführung einer Abschlussbesprechung.*
- DER.3.1.A22 *Erstellung eines Auditberichts*: Präsentation entfernt, da dies eher ein Umsetzungshinweis ist.
- DER.3.1.A20 *Nachbereitung und Einleitung des Follow-up*: Anforderungstitel geändert zu *Nachbereitung.*

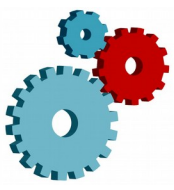


DER.3.2 *Revisionen auf Basis des Leitfadens IS-Revision*

Der Baustein wurde umbenannt (vorher: *IS-Revision für Bundesbehörden*), da er für alle Anwender des *Leitfadens IS-Revision* des BSI gültig ist.

Kapitel 1.3: Abgrenzung und Modellierung

- Hinweise auf UP Bund 2017 entfernt.
- Abgrenzung zum Geheimschutz ergänzt.



DER.4 *Notfallmanagement*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

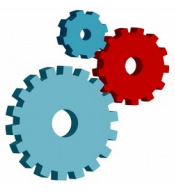
- DER.4.A14 *Regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen:* Diese Anforderung wurde um Aspekte aus der entfernten Anforderung DER.4.A11 *Überprüfung und Aufrechterhaltung der Maßnahmen zur Notfallvorsorge und -reaktion* erweitert.
- DER.4.A10 *Tests und Notfallübungen:* Diese Anforderungen wurde konkretisiert.
- DER.4.A15 *Bewertung der Leistungsfähigkeit des Notfallmanagement-Systems:* In dieser Anforderung wurde der Bewertungszeitraum erweitert, so dass auch mehrere Bewertungen innerhalb eines Jahres berücksichtigt werden.

Entfernung von Anforderungen

- DER.4.A11 *Überprüfung und Aufrechterhaltung der Maßnahmen zur Notfallvorsorge und -reaktion*: Diese Anforderung wurde mit Anforderung DER.4.A14 *Regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen* zusammengeführt.

Kapitel 5: Anlage Kreuzreferenztabelle zu elementaren Gefährdungen

- Es wurden 3 weitere elementaren Gefährdungen identifiziert:
  - G 0.11 Ausfall oder Störung von Dienstleistern
  - G 0.19 Offenlegung schützenswerter Informationen
  - G 0.29 Verstoß gegen Gesetze oder Regelungen
- Die Gefährdung G 0.33 Personalausfall wurde entfernt, da sie nicht direkt auf die Anforderungen wirkt.



INF.2 *Rechenzentrum sowie Serverraum*

Kapitel 3: Anforderungen

Neue Anforderungen

- INF.2.A29 *Vermeidung und Überwachung nicht erforderlicher Leitungen.*
- INF.2.A30 *Anlagen zur Erkennung, Löschung oder Vermeidung von Bränden.*

Änderungen an bestehenden Anforderungen

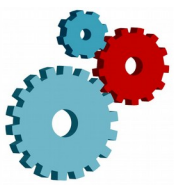
- INF.2.A1 *Festlegung von Anforderungen:* Vorgaben zu Wasser- und sonstigen Leitungen wurden hier gestrichen und sind nun in der neuen Anforderungen INF.2.A29 *Vermeidung und Überwachung nicht erforderlicher Leitungen* zu finden.
- INF.2.A3 *Einsatz einer unterbrechungsfreien Stromversorgung:* Die Anforderung wurde geschärft.
- INF.2.A9 *Einsatz einer Lösch- oder Brandvermeidungsanlage*: Die vorhandene Anforderung zum Einsatz einer Lösch- oder Brandvermeidungsanlage wurde grundlegend überarbeitet und aufgeteilt:
  - INF.2.A9 *Einsatz einer Lösch- oder Brandvermeidungsanlage* (Basis-Anforderung)
  - INF.2.A30 *Anlagen zur Erkennung, Löschung oder Vermeidung von Bränden* (neue Standard-Anforderung).
- INF.2.A10 *Inspektion und Wartung der Infrastruktur:* Die Anforderung wurde geschärft.
- INF.2.A11 *Automatische Überwachung der Infrastruktur:* Sprachliche Anpassung des Anforderungstitels und der Anforderung.
- INF.2.A12 *Perimeterschutz für das Rechenzentrum:* Sprachliche Anpassung des Anforderungstitels. Zudem wurde die Anforderung um Maßnahmen zur Beweissicherung (bspw. Videoaufzeichnung) sowie um den Aspekt der automatischen Alarmierung erweitert.
- INF.2.A14 *Einsatz einer Netzersatzanlage:* Die Anforderung wurde geschärft.
- INF.2.A15 *Überspannungsschutzeinrichtung:* Der letzte Absatz wurde gestrichen. Der zugrundeliegende Aspekt soll im übergeordneten Baustein INF.3 *Elektrotechnische Verkabelung* behandelt werden.
- INF.2.A16 *Klimatisierung im Rechenzentrum:* Die Anforderung wurde geschärft.
- INF.2.A21 *Ausweichrechenzentrum:* Die Anforderung wurde um die Aspekte „Schwenk auf das Notfallrechenzentrum“ sowie „Übertragungswege in das Ausweichrechenzentrum“ erweitert.

Umsortierung von Anforderungen

- INF.2.A17 *Brandfrüherkennung:* Vorgaben zur Brandfrüherkennung wurden in eine Basis-Anforderung überführt (vorher Standard-Anforderung), da dies nach Rücksprache mit Fachanwendern unerlässlich ist.

Entfernung von Anforderungen

- INF.2.A18 *Schutz vor Wasseraustritt:* Die bisherige INF.2.A18 *Schutz vor Wasseraustritt* ist nun durch die neue Anforderung INF.2.A29 *Vermeidung und Überwachung nicht erforderlicher Leitungen* abgedeckt und wurde daher gestrichen.



INF.3 *Elektrotechnische Verkabelung*

Kapitel 1.3: Abgrenzung und Modellierung

- Schärfung der Abgrenzung zum Baustein INF:1 *Allgemeines Gebäude*.

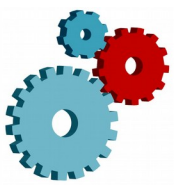
Kapitel 2: Gefährdungslage

- Konsolidierung der Gefährdungen mit dem Baustein INF.4 *IT-Verkabelung*.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- INF.3.A1: Konsolidierung mit der entsprechenden Anforderung aus dem Baustein INF.4 *IT-Verkabelung*.



INF.4 *IT-Verkabelung*

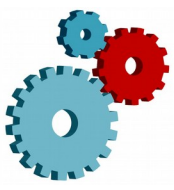
Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung in Bezug auf die Abgrenzung zu den Bausteinen der Schicht NET und der Anwendbarkeit des Bausteins INF.1 *Allgemeines Gebäude.*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- INF.4.A6*: Laufende Fortschreibung und Revision der Netzdokumentation:* Entfernung des Anforderungsteils „Die Dokumentation der IT-Verkabelung SOLLTE als ein elementarer Bestandteil jeder Veränderung im Netz betrachtet und behandelt werden.“ Dieser lieferte keinen Mehrwert und war nicht überprüfbar.



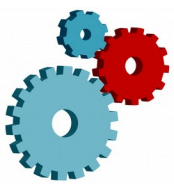
NET.1.2 *Netzmanagement*

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung der Abgrenzung. Verweise auf weitere Themen wie z. B. Management der passiven Netzinfrastruktur oder Outsourcing wurden entfernt.

Änderungen an bestehenden Anforderungen

- NET.1.2.A4 *Grundlegende Authentisierung für den Netzmanagement-Zugriff:* Der Aspekt „regelmäßige Änderung von Passwörtern“ wurde im Zuge der inhaltlichen Konsolidierung mit dem übergreifenden Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* gestrichen.
- NET.1.2.A9 *Absicherung der Netzmanagement-Kommunikation:* Die Anforderung wurde geschärft.
- NET.1.2.A10 *Beschränkung der SNMP-Kommunikation:* Die Anforderung wurde geschärft.
- NET.1.2.A11 *Festlegung einer Sicherheitsrichtlinie für das Netzmanagement:* Die Teilanforderung „Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.“ ist nun eine SOLLTE-Teilanforderung, da die Dringlichkeit hier nicht gegeben ist.
- NET.1.2.A20 *Absicherung des Zugangs zu Netzmanagement-Lösungen:* Die Anforderung wurde geschärft.
- NET.1.2.A26 *Umfassende Protokollierung, Alarmierung und Logging von Ereignissen:* Die Anforderung wurde geschärft.



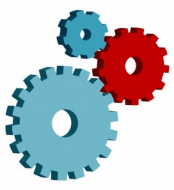
NET.2.1 *WLAN-Betrieb*

Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlende oder unzureichende Planung des WLAN-Einsatzes* wurde um den Aspekt WLAN-Abdeckung erweitert.

Änderungen an bestehenden Anforderungen

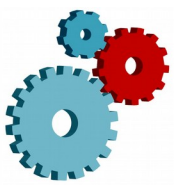
- NET.2.1.A1 *Festlegung einer Strategie für den Einsatz von WLANs*: Die Anforderung wurde geschärft.
- NET.2.1.A2 *Auswahl eines geeigneten WLAN-Standards*: Die Teilanforderung „Geräte, die von anerkannt sicheren Verfahren auf unsichere zurückgreifen müssen, DÜRFEN in der Planung NICHT mehr berücksichtigt werden.“ wurde geschärft.
- NET.2.1.A3 *Auswahl geeigneter Kryptoverfahren für WLAN:* Die Teilanforderung „Außerdem MUSS dieser regelmäßig gewechselt werden.“ wurde im Zuge der inhaltlichen Konsolidierung mit dem übergreifenden Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* gestrichen.
- NET.2.1.A4 *Geeignete Aufstellung von Access Points:* Die Anforderung wurde um den Aspekt Diebstahlsicherheit erweitert.



NET.2.2 *WLAN-Nutzung*

Änderungen an bestehenden Anforderungen

- NET.2.2.A3 *Absicherung der WLAN-Nutzung in unsicheren Umgebungen:* Die Anforderung wurde geschärft.



NET.3.2 *Firewall*

Die Begriffe *Firewall* und *Firewall-System* wurden im Baustein synonym verwendet. Dies wurde zur besseren Verständlichkeit angepasst. Der Baustein spricht jetzt nur noch von *Firewall*.

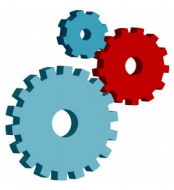
Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung der Abgrenzung. Der Baustein ist auf jede Firewall anzuwenden.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.3.2.A2 *Festlegen der Firewall-Regeln:* Korrektur des Modalverbs von SOLLTE zu MUSS im Satz „Es MUSS beachtet werden, dass mögliche Ausnahmen zu dieser Anforderung in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.“, da es sich bei der Anforderung um eine Basis-Anforderung handelt.
- NET.3.2.A3 *Einrichten geeigneter Filterregeln am Paketfilter*: Korrektur des Modalverbs von SOLLTE zu MUSS im Satz „Auch für die verbindungslosen Protokolle UDP und ICMP MÜSSEN zustandsbehaftete Filterregeln konfiguriert werden.“, da es sich bei der Anforderung um eine Basis-Anforderung handelt.
- NET.3.2.A4 *Sichere Konfiguration der Firewall*: Korrektur der Modalverben von SOLLTE zu MUSS in den Sätzen „Die Integrität der Konfigurationsdateien MUSS geeignet geschützt werden. Zugangspasswörter MÜSSEN verschlüsselt gespeichert werden.“ und „Auch MUSS begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden.“, da es sich bei der Anforderung um eine Basis-Anforderung handelt.
- NET.3.2.A11 *Einspielen von Updates und Patches*: Korrektur des Modalverbs von SOLLTE zu MUSS im Satz „Vorab MUSS auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen.“, da es sich bei der Anforderung um eine Basis-Anforderung handelt.



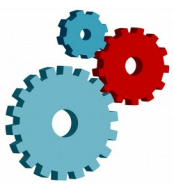
NET.3.3 *VPN*

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung der Abgrenzung. Verweise auf weitere Themen wie z. B. Patch- und Änderungsmanagement, Sensibilisierung und Schulung zur Informationssicherheit oder Notfallmanagement wurden entfernt.

Änderungen an bestehenden Anforderungen

- NET.3.3.A11 *Sichere Anbindung eines externen Netzes:* Die Anforderung wurde geschärft.



NET.4.1 *TK-Anlage*

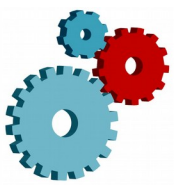
Kapitel 1.3: Abgrenzung und Modellierung

- Streichung der Verweise auf noch nicht erstellte Bausteine.

Kapitel 3: Anforderungen

Umsortierung von Anforderungen

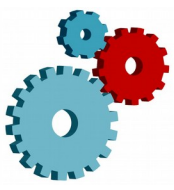
- NET.4.1.A17 *Wartung von TK-Anlagen*: Anforderung wurde aufgrund ihrer Relevanz von einer Anforderung bei erhöhtem Schutzbedarf zu einer Standard-Anforderung verschoben.



NET.4.2 *VoIP*

Kapitel 1.3: Abgrenzung und Modellierung

- Streichung von noch nicht erstellten Bausteinen.
- Schärfung der Abgrenzung zum Baustein NET.4.1 *TK-Anlagen*.



NET.4.3 *Faxgeräte und Faxserver*

Kapitel 2: Gefährdungslage

- In der Gefährdung *Unbefugtes Lesen von Faxsendungen* wurde der zweite Absatz gestrichen, da er redundant zur vorherigen Gefährdung war.
- In der Gefährdung *Auswertung von Restinformationen in Faxgeräten und Faxservern* wurde der letzte Absatz gestrichen, da er sich nicht auf Faxgeräte und -server bezog.

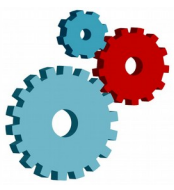
Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- NET.4.3.A7 *Geeignete Kennzeichnung ausgehender Faxsendungen:* Streichung des Satzes „Alle Informationen, die auf dem Deckblatt einzutragen sind, SOLLTEN in geeigneter Weise ausgewählt werden“. Dieser Satz lieferte keinen Mehrwert.

Entfernung von Anforderungen

- NET.4.3.A5 *Ernennung eines Fax-Verantwortlichen:* Der Fax-Verantwortliche sollte, wie alle Rollen innerhalb des IT-Grundschutz-Kompendiums, unabhängig vom Baustein ernannt werden.



OPS.1.1.2 *Ordnungsgemäße IT-Administration*

Kapitel 2: Gefährdungslage

- Die Gefährdung *Erleichterung von Angriffen* wurde in *Mangelhafte Berücksichtigung von administrative Aufgaben* umbenannt.

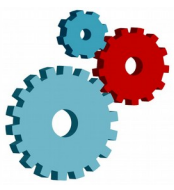
Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- OPS.1.1.2.A1 *Personalauswahl für administrative Tätigkeiten*: Teilanforderung "Diese Anforderungen MÜSSEN auch dann erfüllt werden, wenn administrative Aufgaben an Dritte übertragen werden." gestrichen, weil im Baustein OPS.2.1 *Outsourcing* dies schon gefordert ist.
- OPS.1.1.2.A4 *Beendigung der Tätigkeit als IT-Administrator*: Teilanforderung "Diese Anforderungen MÜSSEN auch dann erfüllt werden, wenn administrative Aufgaben an Dritte übertragen wurden und die dort beschäftigten Mitarbeiter aus ihrer Tätigkeit ausscheiden." gestrichen, weil im Baustein OPS.2.1 *Outsourcing* dies schon gefordert ist.
- OPS.1.1.2.A5 *Nachweisbarkeit von administrativen Tätigkeiten:* Anforderungstitel umbenannt und Anforderung komplett überarbeitet:
  Die Institution MUSS jederzeit nachweisen können, welcher Administrator welche Aktion durchgeführt hat. Dazu SOLLTE jeder Administrator über eine eigene Benutzerkennung verfügen. Auch Vertreter von Administratoren SOLLTEN eigene Benutzerkennungen erhalten. Jeder Anmeldevorgang über eine Administrationskennung (Login) MUSS protokolliert werden.
- OPS.1.1.2.A6 *Schutz administrativer Kennungen*: Teilanforderung "Für Administrationszugriffe MÜSSEN sichere Protokolle verwendet werden, wenn dies nicht über eine lokale Konsole erfolgt. Diese MÜSSEN sicherstellen, dass die Kommunikation nach dem Stand der Technik verschlüsselt ist." gestrichen, weil dies durch OPS.1.2.5 *Fernwartung* ausreichend abgedeckt ist.

Entfernung von Anforderungen

- OPS.1.1.2.A13 *Absicherung von Fernwartung*: Das Thema wird im separaten Baustein OPS.1.2.5 *Fernwartung* behandelt.



OPS.1.1.6 *Software-Tests und -Freigaben*

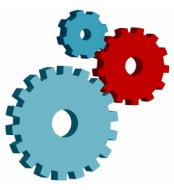
Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Abgrenzung gegenüber der Bausteine der Schicht APP.
- Entfernung des Verweises auf Penetrationstests.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- OPS.1.1.6.A5 *Durchführung nicht-funktionaler Software-Tests*: In der Teilanforderung zu sicherheitsspezifischen Software-Tests und deren Dokumentation wurde „SOLLTE“ in „MUSS“ geändert.
- OPS.1.1.6.A7 *Personalauswahl der Software-Teste*r: Die Teilanforderung zur Rollentrennung wurde ergänzt.



OPS.1.2.2 *Archivierung*

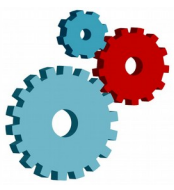
Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- OPS.1.2.2.A6 *Schutz der Integrität der Indexdatenbank von Archivsystemen:* Teilanforderung „Mittlere und große Archive MÜSSEN über redundante Indexdatenbanken verfügen.“ wurde zu „Mittlere und große Archive SOLLTEN über redundante Indexdatenbanken verfügen.“ angepasst, da „mittlere und große“ recht unbestimmte Begriffe sind.
- OPS.1.2.2.A12 *Überwachung der Speicherressourcen von Archivmedien:* Korrektur eines Fehlers im ersten Satz der Standard-Anforderung, „MUSS“ wurde zu „SOLLTE“ geändert.

OPS.1.2.3 *Informations- und Datenträgeraustausch*

Dieser Baustein wurde aufgeteilt und verschoben. Die Aspekte zum Thema Informationsaustausch finden sich nun im neuen Baustein CON.9 *Informationsaustausch*. Die Aspekte zum Thema Datenträgeraustausch wurden, sofern nicht bereits vorhanden, mit den Inhalten des Bausteins SYS.3.4 *Mobile Datenträger* im neuen Baustein SYS.4.5 *Wechseldatenträger* zusammengeführt.



OPS.1.2.5 *Fernwartung*

Der Baustein wurde aus der Teilschicht OPS.2 *Betrieb von Dritten* nach OPS.1.2 *Weiterführende Aufgaben* unter OPS.1 *Eigener Betrieb* verschoben, da er nicht nur bei der Fernwartung durch Dritte anzuwenden ist.

Kapitel 1.3: Abgrenzung und Modellierung

- Ergänzung der Anwendung auf relevante Zielobjekte.

Kapitel 2: Gefährdungslage

- Konkretisierung bestehender Gefährdungen.
- Entfernung von Gefährdungen, die aus anderen Gefährdungen hervorgehen.
- Ergänzung der Gefährdung *Unbekannte Fernwartungskomponenten*.

Kapitel 3: Anforderungen

Neue Anforderungen

- OPS.1.2.5.A24 *Absicherung integrierter Fernwartungssysteme*: Standard-Anforderung zum Umgang mit integrierten Fernwartungskomponenten ergänzt.

Änderungen an bestehenden Anforderungen

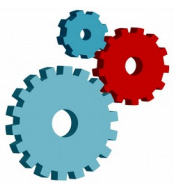
- Die Anforderungen des Bausteins wurden umfangreich überarbeitet. Insbesondere wurden Redundanzen beseitigt.

Umsortierung von Anforderungen

- OPS.1.2.5.A5 *Einsatz von Online-Diensten*: Die Anforderung wurde in eine Standard-Anforderung überführt (vorher Basis-Anforderung), da die Nutzung von Onlinediensten nicht mehr dem Stand der Technik widerspricht.
- OPS.1.2.5.A21 *Erstellung eines Notfallplans für den Ausfall der Fernwartung*: Die Anforderung wurde in eine Standard-Anforderung überführt (vorher erhöhter Schutzbedarf), da der Ausfall von Fernwartungszugängen in einigen Fällen auch bei normalem Schutzbedarf zum völligen Ausfall von Systemen führen kann.

Entfernung von Anforderungen

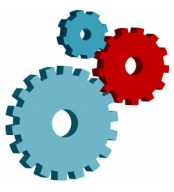
- OPS.1.2.5.A11 *Einsatz von kryptografischen Verfahren bei der Fernwartung*: Anforderung entfernt, da redundant.
- OPS.1.2.5.A12 *Patch- und Änderungsmanagement bei der Fernwartung*: Anforderung entfernt, da redundant.
- OPS.1.2.5.A13 *Datensicherung bei der Fernwartung*: Anforderung entfernt, da redundant.
- OPS.1.2.5.A15 *Absicherung der Fernwartung*: Anforderung entfernt, da redundant.
- OPS.1.2.5.A16 *Schulungen zur Fernwartung*: Anforderung entfernt, da redundant.
- OPS.1.2.5.A18 *Passwortsicherheit bei der Fernwartung*: Anforderung entfernt, da redundant.



OPS.2.2 *Cloud-Nutzung*

Kapitel 1.3: Abgrenzung und Modellierung

- Konkretisierung der Abgrenzung gegenüber dem Baustein *OPS.2.1 Outsourcing für Kunden*.
- Konkretisierung der Modellierung in Bezug auf Nutzung unterschiedlicher Cloud-Diensteanbieter.

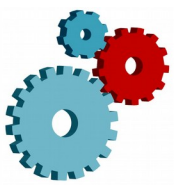


ORP.1 *Organisation*

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- ORP.1.A9 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln:* Diese Anforderung ist bereits durch Anforderung CON.6.A2 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen* im Baustein CON.6 *Löschen und Vernichten* abgedeckt.

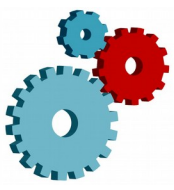


ORP.2 *Personal*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- ORP.2.A2 *Geregelte Verfahrensweise beim Weggang von Mitarbeitern:* Der Satz „Die IT-Administration MUSS außerdem dafür Sorge tragen, dass ehemaligen Mitarbeitern sämtliche Zugriffsberechtigungen auf IT-Systeme entzogen bzw. diese bei Aufgabenwechseln angepasst werden." wurde gestrichen, da diese Anforderung bereits durch die Anforderung ORP.4.A2 *Regelung für Einrichtung, Änderung und Entzug von Berechtigungen* im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* abgedeckt ist.

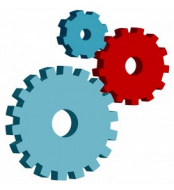


ORP.3 *Sensibilisierung und Schulung*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- ORP.3.A6 *Planung und Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit:* Die Anforderung wurde um den Aspekt des Austausches mit anderen Bereichen wie Gesundheitsschutz, Arbeitsschutz usw. ergänzt.



ORP.4 *Identitäts- und Berechtigungsmanagement*

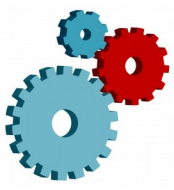
Kapitel 3: Anforderungen

Neue Anforderungen

- ORP.4.A22 *Regelung zur Passwortqualität.*
- ORP.4.A23 *Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme.*

Änderungen an bestehenden Anforderungen

- ORP.4.A1 *Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen*: Ergänzung von Titel und Anforderung um den Aspekt „Löschung“ von Benutzern und Benutzergruppen.
- ORP.4.A3 *Dokumentation der Benutzerkennungen und Rechteprofile*: Sprachliche Anpassung des Anforderungstitels und der Anforderung.
- ORP.4.A4 *Aufgabenverteilung und Funktionstrennung*: Schärfung der Anforderung mit Hinweis auf die unvereinbaren Funktionen, die in Baustein ORP.1 *Organisation* definiert werden.
- ORP.4.A5 *Vergabe von Zutrittsberechtigungen*: Sprachliche Anpassung der Anforderung.
- ORP.4.A7 *Vergabe von Zugriffsrechten*: Sprachliche Anpassung der Anforderung.
- ORP.4.A8 *Regelung des Passwortgebrauchs*: Sprachliche Überarbeitung der Anforderung und thematische Aufteilung nach Regelung des Passwortgebrauchs, Regelung zur Passwortqualität (neue Anforderung) und Regelung für passwortverarbeitende Anwendungen und IT-Systeme (neue Anforderung).
- ORP.4.A10 *Schutz von Benutzerkennungen mit weitreichenden Berechtigungen*: Sprachliche Anpassung des Anforderungstitels und der Anforderung.
- ORP.4.A14 *Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. Anwendung*: Sprachliche Anpassung des Anforderungstitels und der Anforderung.
- ORP.4.A20 *Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System*: Sprachliche Anpassung der Anforderung.

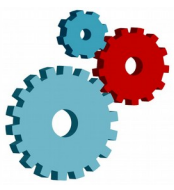


ORP.5 *Compliance Management (Anforderungsmanagement)*

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- ORP.5.A7 *Aufrechterhaltung der Informationssicherheit:* Diese Anforderung ist bereits durch die Anforderung ISMS.1.A11 *Aufrechterhaltung der Informationssicherheit* im Baustein ISMS.1 *Sicherheitsmanagement* abgedeckt.
- ORP.5.A9 *Schutz gegen nachträgliche Veränderungen von Informationen* ist kein Thema des Compliance Management.
- ORP.5.A10 *Klassifizierung von Informationen* ist kein Thema des Compliance Management.
- ORP.5.A11 *Erhebung der rechtlichen Rahmenbedingungen für kryptografische Verfahren und Produkte* ist keine spezielle Anforderung für den erhöhten Schutzbedarf und bereits in ORP.5.A1 *Identifikation der rechtlichen Rahmenbedingungen* inbegriffen.



SYS.1.1 *Allgemeiner Server*

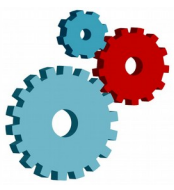
Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.1.1.A34 *Festplattenverschlüsselung*

Änderungen an bestehenden Anforderungen

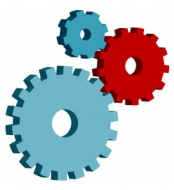
- SYS.1.1.A1 *Geeignete Aufstellung*: Teilanforderungen zur Nutzung von Servern als Arbeitsplatz und zum Anschluss von externen Geräten wurden nach SYS.1.1.A5 *Schutz der Administrationsschnittstellen* verschoben.
- SYS.1.1.A2 *Benutzerauthentisierung an Servern*: Die Anforderung wurde verallgemeinert, um „Authentisierungsverfahren“ statt „Passwörter“ zu behandeln.
- SYS.1.1.A3 *Restriktive Rechtevergabe*: Früheres Beispiel zur Vergabe von Schreibrechten ist nun eine SOLLTE-Anforderung.
- SYS.1.1.A10 *Protokollierung*: Teilanforderung zur zentralen Speicherung von Protokolldaten ergänzt.



SYS.1.2.2 *Windows Server 2012*

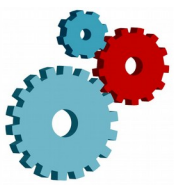
Kapitel 2: Gefährdungslage

- Die Gefährdung *Software-Schwachstellen oder -Fehler* wurde entfernt, da sie bereits in SYS.1.1 *Allgemeiner Server* betriebssystemübergreifend beschrieben wird.



SYS.1.3 *Server unter Linux und Unix*

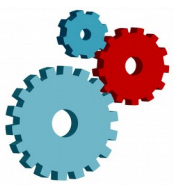
Der Baustein wurde umbenannt (vorher: *Server unter Unix*), da der Schwerpunkt der Inhalte auf Linux liegt.



SYS.1.5 *Virtualisierung*

Änderungen an bestehenden Anforderungen

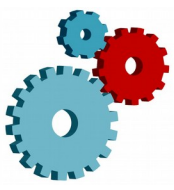
- SYS.1.5.A5 *Schutz der Administrationsschnittstellen:* Die Anforderung wurde geschärft.



SYS.1.8 *Speicherlösungen*

Änderungen an bestehenden Anforderungen

- SYS.1.8.A3 *Restriktive Rechtevergabe:* Die Anforderung wurde geschärft.
- SYS.1.8.A4 *Schutz der Administrationsschnittstellen:* Die Anforderung wurde geschärft.



SYS.2.1 *Allgemeiner Client*

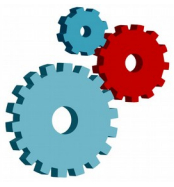
Kapitel 2: Gefährdungslage

- Die Gefährdungen *Unstrukturierte lokale Datenhaltung* sowie *Datenverlust* wurden zu *Datenverlust durch lokale Datenhaltung* zusammengefasst.
- Die Gefährdung *Fehlerhafte Administration oder Nutzung von Geräten und Systemen* wurde hinzugefügt.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.2.1.A4 *Regelmäßige Datensicherung*: Die Anforderung wurde vollständig überarbeitet und geschärft.
- SYS.2.1.A7 *Protokollierung auf Clients*: Anforderung zur zentralen Speicherung von Protokolldaten ergänzt.
- SYS.2.1.A22 *Abmelden nach Aufgabenerfüllung*: Teilanforderung zur automatischen Aktivierung der Bildschirmsperre entfernt, da bereits durch SYS.2.1.A5 *Verwendung einer Bildschirmsperre* abgedeckt.



SYS.2.2.2 *Clients unter Windows 8.1*

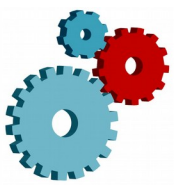
Kapitel 2: Gefährdungslage

- Die Gefährdung *Auf Windows ausgerichtete Schadprogramme* wurde inhaltlich stärker an ihren Titel angepasst.
- Die Gefährdung *Software-Schwachstellen oder -Fehler* wurde entfernt, da sie bereits in SYS.2.1 *Allgemeiner Client* betriebssystemübergreifend beschrieben wird.
- Die Gefährdung *Fehlerhafte Administration oder Nutzung von Geräten und Systemen* wurde entfernt, da sie bereits in SYS.2.1 *Allgemeiner Client* betriebssystemübergreifend beschrieben wird.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.2.2.2.A10 *Integration von Online-Konten in das Betriebssystem*: Benutzer als aktive Rolle hinzugefügt.



SYS.2.2.3 *Clients unter Windows 10*

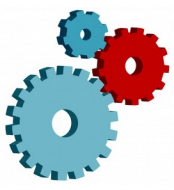
Kapitel 2: Gefährdungslage

- Die Gefährdung *Software-Schwachstellen in Windows 10* wurde entfernt, da sie bereits in SYS.2.1 *Allgemeiner Client* betriebssystemübergreifend beschrieben wird.
- Die Gefährdung *Telemetrie-Funktionen von Windows 10* wurde neu hinzugefügt.

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- SYS.2.2.3.A3 *Geeignetes Patch- und Änderungsmanagement*: Die Anforderung ist entfallen, da das Thema nicht betriebssystemspezifisch ist und bereits durch SYS.2.1 *Allgemeiner Client* sowie OPS.1.1.3 *Patch- und Änderungsmanagement* behandelt wird.



SYS.2.3 *Clients unter Linux und Unix*

Der Baustein wurde umbenannt (vorher: *Clients unter Unix*), da der Schwerpunkt der Inhalte auf Linux liegt.

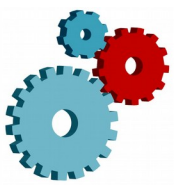
Kapitel 2: Gefährdungslage

- Die Gefährdung *Schadprogramme* wurde entfernt, da sie bereits in SYS.2.1 *Allgemeiner Client* betriebssystemübergreifend beschrieben wird.
- Die Gefährdung *Software-Schwachstellen oder -Fehler* wurde entfernt, da sie bereits in SYS.2.1 *Allgemeiner Client* betriebssystemübergreifend beschrieben wird.

Kapitel 3: Anforderungen

Entfernung von Anforderungen

- SYS.2.3.A13 *Schutz vor unbefugten Anmeldungen*: Entfallen, da bereits abgedeckt durch SYS.2.1.A37 *Verwendung von Mehr-Faktor-Authentisierung*.



SYS.2.4 *Clients unter macOS*

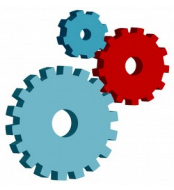
Kapitel 2: Gefährdungslage

- Die Gefährdung *Betriebssystem-integrierte Funktionalität von Drittanbietern* wurde entfernt, da sie in dieser Form unter aktuellen macOS-Versionen nicht mehr zutrifft.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.2.4.A4 *Verwendung einer Festplattenverschlüsselung*: Verweis auf institutionelle Wiederherstellungsschlüssel für FileVault ergänzt.
- SYS.2.4.A12 *Firmware-Kennwort und Boot-Schutz auf Macs*: Berücksichtigung des T2-Sicherheitschips im Kontext von Firmware-Passwörtern.

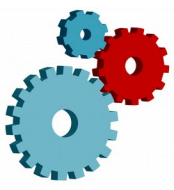


SYS.3.1 *Laptops*

Kapitel 3: Anforderungen

Umsortierung von Anforderungen

- SYS.3.1.A15 *Geeignete Auswahl von Laptops*: Die Anforderung ist nun eine Standard-Anforderung (vorher: Erhöhter Schutzbedarf).

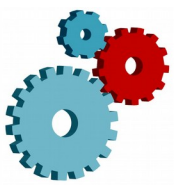


SYS.3.2.1 *Allgemeine Smartphones und Tablets*

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.3.2.1.A1 *Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets*: Zur Vereinheitlichung mit anderen Bausteinen nun Forderung einer „Richtlinie“ statt „Strategie“
- SYS.3.2.1.A6 *Datenschutzeinstellungen*: Ergänzung von Ortungs-, Gesundheits- und Fitnessdaten



SYS.3.2.3 *iOS (for Enterprise)*

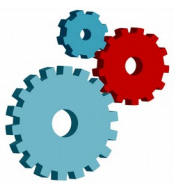
Kapitel 2: Gefährdungslage

- Die Gefährdung *Fehlende Betriebssystem-Updates bei alten Geräten* wurde entfernt, da sie nicht iOS-spezifisch ist und bereits in SYS.3.2.1 *Allgemeine Smartphones und Tablets* allgemeingültig beschrieben wird.
- Die Gefährdung *Missbrauch von Fitness-, Gesundheits- oder Ortungsdaten unter iOS* wurde entfernt, da sie nicht iOS-spezifisch ist und bereits in SYS.3.2.1 *Allgemeine Smartphones und Tablets* allgemeingültig beschrieben wird.
- Die Gefährdung *Webbasierte Angriffe auf Browser* wurde entfernt, da sie nicht iOS-spezifisch ist und bereits in SYS.3.2.1 *Allgemeine Smartphones und Tablets* allgemeingültig beschrieben wird.
- Die Gefährdung *Unzureichende Vorgaben zum Lizenz-Management* wurde entfernt, da sie nicht iOS-spezifisch ist und das Thema in ORP.5 *Compliance Management (Anforderungsmanagement)* behandelt wird.

Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.3.2.3.A1 *Strategie für die iOS-Nutzung*: Der Aspekt „Jailbreaks“ wurde ergänzt.
- SYS.3.2.3.A2 *Planung des Einsatzes von Cloud-Diensten*: Verweis auf „Device Enrollment Program“ wurde durch „Apple Business Manager“ ersetzt.
- SYS.3.2.3.A12 *Verwendung von Apple-IDs*: Vorgabe einer anonymisierten statt einer institutionsbezogenen Apple-ID. Verweis auf „Volume Purchasing Program“ wurde durch „Apple Business Manager“ ersetzt.
- SYS.3.2.3.A21 *Freigabe von Apps und Einbindung des Apple App Stores*: Anforderung zur Freigabe von Apps ist nun SOLLTE statt MUSS. Verweis auf „Volume Purchasing Program“ wurde durch „Apple Business Manager“ ersetzt.



SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte*

Kapitel 2: Gefährdungslage

- Konkretisierung und Aktualisierung der Gefährdungslage.
- Die Gefährdung *Manipulation des Betriebssystems* wurde entfernt, da das Thema Softwareupdates zentral im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* behandelt wird.

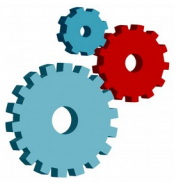
Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.4.1.A22 *Ordnungsgemäße Entsorgung ausgedruckter Dokumente*, da Inhalte aus SYS.4.1.A12 *Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln* nun in eigene Anforderung verschoben wurden.

Änderungen an bestehenden Anforderungen

- SYS.4.1.A1 *Erstellung eines Basis-Konzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten*: Umbenennung in *Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*. Teilsatz: "und wie sie vor Angriffen geschützt werden sollen." wurde gestrichen, da zu generisch. Ergebnisse sollten nun in ein Basis-Konzept festgehalten werden.
- SYS.4.1.A2 *Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte*: Teilanforderung "Nicht benötigte Gerätefunktionen SOLLTEN abgeschaltet werden. " wurde in SYS.4.1.A18 *Konfiguration von Druckern, Kopierern und Multifunktionsgeräten* verschoben. Explizite Anforderung zum Wechsel von Passwörtern wurde hier gestrichen, da dieses Thema im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* behandelt wird, dafür wird Integration in das Identitäts- und Berechtigungsmanagement der Institution gefordert.
- SYS.4.1.A4 *Erstellung eines Sicherheitskonzeptes für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten*: Erstellung von Administrationsrichtlinie wurde aufgenommen.
- SYS.4.1.A5 *Erstellung von Benutzer- und Administrationsrichtlinie für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*: Administrationsrichtlinie wurde an dieser Stelle entfernt und in SYS.4.1.A4 aufgenommen. Umbenennung der Anforderung in *Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*.
- SYS.4.1.A11 *Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten*: Netzseparierung wird nun gefordert.
- SYS.4.1.A12 *Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln*. Ausgedruckte Papierdokumente wurden aus dieser Anforderung entfernt und in neue Anforderung SYS.4.1.A22 *Ordnungsgemäße Entsorgung ausgedruckter Dokumente* überführt. Folgende Teilanforderungen wurden geändert
  - "Bevor die Institution Altgeräte entsorgt oder zurückgibt, MÜSSEN alle sensiblen Daten auf den Geräten sicher gelöscht werden." geändert in "SOLLTEN".



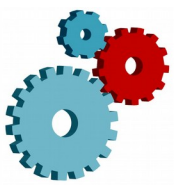
    - "Ist das nicht möglich, SOLLTEN die Massenspeicher ausgebaut und durch geeignete Prozesse vernichtet werden." geändert in MÜSSEN.
- SYS.4.1.A17 *Schutz von Nutz- und Metadaten*: Es sollte nicht nur *darauf geachtet werden*, dass Metadaten nicht sichtbar sind, sondern es sollte nun *sichergestellt* werden.
- SYS.4.1.A18 *Konfiguration von Druckern, Kopierern und Multifunktionsgeräten*: Teilanforderung "Nicht benötigte Gerätefunktionen SOLLTEN abgeschaltet werden." wurde aus SYS.4.1.A2 *Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte* hierher verschoben.
- SYS.4.1.A20 *Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten*: Teilanforderung „Alternativ SOLLTEN die Geräte so eingestellt werden, dass sich eingescannte Dokumente nur an eine fest eingetragene Adresse senden lassen“ gestrichen.

Entfernung von Anforderungen

- SYS.4.1.A3 *Regelmäßige Aktualisierung von Druckern, Kopieren und Multifunktionsgeräten*: Diese Anforderung ist bereits durch den übergreifenden Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* abgedeckt. Aspekt wurde auch in Kapitel *Abgrenzung* aufgenommen.

Kapitel 5: Anlage Kreuzreferenztabelle zu elementaren Gefährdungen

- Die elementare Gefährdung G 0.22 *Manipulationen von Informationen* wurde ergänzt.
- Die elementare Gefährdung *G 0.14 Ausspähen von Informationen (Spionage)* wurde entfernt.
- Die elementare Gefährdung *G 0.20 Informationen aus unzuverlässiger Quelle* wurde entfernt.
- Die elementare Gefährdung *G 0.32 Missbrauch von Berechtigungen* wurde entfernt.
- Die elementare Gefährdung *G 0.39 Schadprogramme* wurde entfernt.



SYS.4.4 *Allgemeines IoT-Gerät*

Kapitel 1.3: Abgrenzung und Modellierung

- Aufnahme, dass IoT-Geräte im Identitäts- und Berechtigungsmanagement zu berücksichtigen sind. Hierfür ist der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* umzusetzen.

Kapitel 2: Gefährdungslage

- Die Überschrift der Gefährdung *Schäden Dritter* wurde an den fachlichen Inhalt des angepasst. Sie heißt nunmehr *Distributed Denial of Service (DDoS)*.

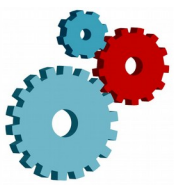
Kapitel 3: Anforderungen

Änderungen an bestehenden Anforderungen

- SYS.4.4.A5 *Einschränkung des Netzzugriffs:* Hinweis auf Intrusion-Prevention-Systeme (IPS) wurde entfernt.
- SYS.4.4.A7 *Planung des Einsatzes von IoT-Geräten*: Die Teil-Anforderung, dass die Vorgaben zur Authentisierung, Update-Mechanismen und Netzanbindung definiert werden sollen, wurde entfernt.
- SYS.4.4.A8 *Beschaffungskriterien für IoT-Geräte*: Die Teil-Anforderung, dass IoT-Geräte mit einem Cloud-Konzept nicht beschafft werden sollten, wurde entfernt.
- SYS.4.4.A11 *Verwendung von verschlüsselter Datenübertragung*: Die Teil-Anforderungen, dass die IoT-Geräte auf Verschlüsselung basierende Protokolle unterstützen sollen oder alternativ in einem VPN eingesetzt werden, wurde entfernt.
- SYS.4.4.A19 *Schutz der Administrationsschnittstellen*: Die Teil-Anforderungen zur Einschränkung der Administrationsschnittstellen wurde entfernt.

Entfernung von Anforderungen

- SYS.4.4.A4 *Aktivieren von Autoupdate* wurde aufgrund von Redundanz entfernt.



SYS.4.5 *Wechseldatenträger*

Der Baustein wurde umbenannt (vorher: *Mobile Datenträger*) und aus der Teilschicht SYS.3 *Mobile Devices* in die Teilschicht SYS.4 *Sonstige Systeme* verschoben. Außerdem wurden die themenspezifischen Aspekte aus dem früheren Baustein OPS.1.2.3 *Informations- und Datenträgeraustausch* integriert.

Kapitel 1.3: Abgrenzung und Modellierung

- Der Baustein ist auf alle Wechseldatenträger des Informationsverbundes anzuwenden.
- Die Abgrenzung zum neuen Baustein CON.9 *Informationsaustausch* (ehemals OPS.1.2.3 *Informations- und Datenträgertausch*) wurde geschärft.

Kapitel 2: Gefährdungslage

- Die Gefährdungslage wurde umfangreich überarbeitet. Es werden nur noch Gefährdungen betrachtet, die auf Wechseldatenträger wirken.

Kapitel 3: Anforderungen

Neue Anforderungen

- SYS.4.5.A12 *Schutz vor Schadsoftware*: Neue Basisanforderung zum Schutz vor Schadsoftware auf Wechseldatenträgern.
- SYS.4.5.A13 *Angemessene Kennzeichnung der Datenträger beim Versand*: Neue Standard-Anforderung, die regelt wie Datenträger gekennzeichnet werden sollen, bevor sie versendet werden.
- SYS.4.5.A14 *Sichere Versandart und Verpackung*: Neue Anforderung für erhöhten Schutzbedarf, die regelt wie Wechseldatenträger beim Versand geschützt werden können.
- SYS.4.5.A15 *Zertifizierte Produkte*: Neue Anforderung für erhöhten Schutzbedarf zur Nutzung von zertifizierten Produkten.
- SYS.4.5.A16 *Nutzung dedizierter Systeme zur Datenprüfung*: Neue Anforderung für erhöhten Schutzbedarf. Um Datenträger vor der Nutzung zu überprüfen, sollten gesonderte Systeme eingesetzt werden.

Änderungen an bestehenden Anforderungen

- Generell wurde alle Anforderungen sprachlich überarbeitet, insbesondere wurde die Bezeichnung „mobiler Datenträger“ durch „Wechseldatenträger“ ersetzt.
- SYS.4.5.A2 *Verlustmeldung mobiler Datenträger*: Anforderung umbenannt in *Verlust- bzw. Manipulationsmeldung*. Anforderung betrachtet jetzt auch Manipulation von Datenträgern.

Entfernung von Anforderungen

- SYS.3.4.A3 *Sicherungskopie der übermittelten Daten*: Anforderung entfernt, da der Inhalt der Anforderung nicht der Abgrenzung des Bausteins entspricht.