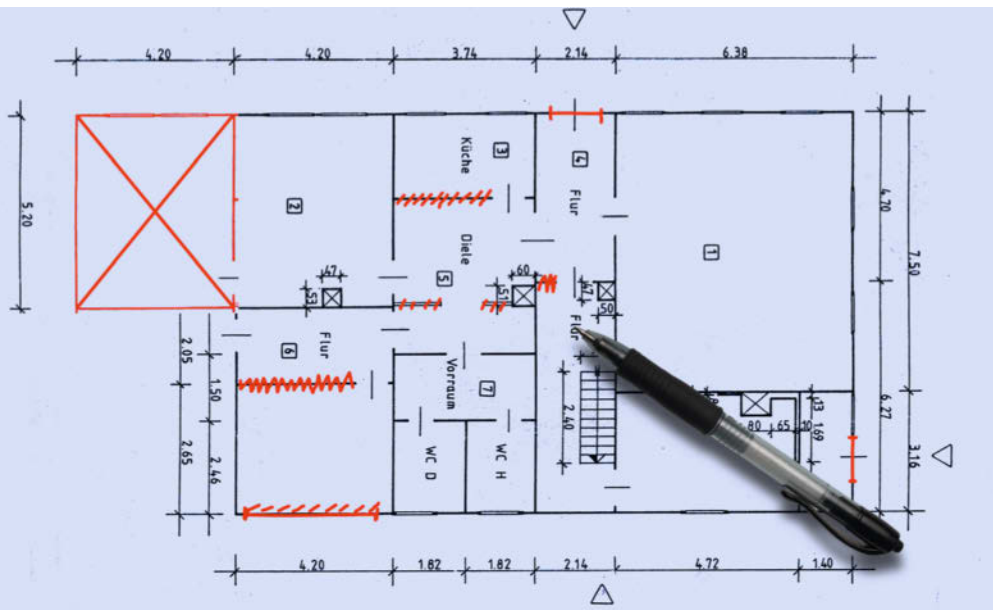




BSI-IT-Grundschutz-Kompendium
Edition 2021 veröffentlicht

Saniert und angebaut

Ronny Frankenstein

Das BSI hat sein IT-Grundschutz-Kompendium turnusmäßig aktualisiert. Die Version 2021 wartet mit zwei komplett neuen Bausteinen zur Entwicklung von Webanwendungen und zu IT in Fahrzeugen auf. Darüber hinaus gibt es zahllose Änderungen in den vorhandenen Bausteinen.

Auch dieses Jahr hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) an den versprochenen Turnus der jährlichen Veröffentlichung überarbeiteter IT-Grundschutz-Kataloge gehalten. Diesmal gibt es vor allem Änderungen vorhandener Bausteine. Formulierungen in den Anforderungen wurden erneut geschärft, um die Anwender für das Umsetzen von Maßnahmen zu gewinnen. Nur zwei gänzlich neue Bausteine kamen hinzu.

Mit seinem IT-Grundschutz-Kompendium will das BSI bewährte und praxistaugliche Empfehlungen zur Absicherung von IT-Infrastrukturen und Informationen,

zum Aufbau eines Managementsystems zur Informationssicherheit (ISMS) und zum Schutz besonders wertvoller Bereiche geben.

Mehrere Bausteine wurden umbenannt und in eine andere Schicht verschoben. Die Bausteine IT- und Elektrotechnische Verkabelung wurden zu einem Baustein Verkabelung zusammengefasst (siehe Tabelle „Versionsvergleich: Struktur des IT-Grundschutz-Kompendiums“ und Abbildung).

Bei den Rollenbezeichnungen gibt es vier neue Rollen, mehrere Zusammenfassungen ursprünglich unterschiedlicher Bezeichnungen, und eine Rolle fiel ganz weg

(siehe Tabelle „Änderung der Rollenbezeichnungen“).

Änderungen unterschiedlich relevant

Fast 2300 Änderungen fanden innerhalb des Kompendiumtextes der Anforderungen statt. Für existierende Managementsysteme der Informationssicherheit (ISMS) und IT-Sicherheitskonzepte sind diese Änderungen unterschiedlich kritisch. Sie müssen daher in der Regel einer Einzelbewertung unterzogen werden. Hier können Tools enorm unterstützen, da sie die Aktualisierungen kenntlich machen. Eine Liste solcher Tools ist über ix.de/zaxj zu finden.

Um die Kompatibilität mit bestehender Dokumentation zu ermöglichen, lässt das BSI absichtlich Lücken in der Nummerierung von Bausteinen und Anforderungen. Sie werden ausschließlich fortgeschrieben und so kann ein Delta zu den großen Veränderungen – beim Wegfall oder Hinzukommen von Anforderungen – leichter erkannt und migriert werden. Einen Auszug einer Änderungsdokumentation zeigt die Tabelle „Abgleich GS-Kompendium 2021 mit 2020“.

Webanwendungen sollen sicher(er) werden

Der neu hinzugekommene Baustein „CON.10 Entwicklung von Webanwendungen“ im Bereich „Konzeption und Vorgehensweisen“ hat zum Ziel, die Entwicklung sicherer Webanwendungen zu unterstützen und Anforderungen an den Schutz der Informationsverarbeitung durch Webanwendungen zu definieren. Im Gegensatz dazu geht es im alten Baustein „APP.3.1 Webanwendungen“ um den sicheren Einsatz. Die allgemeinen Anforderungen an die sichere Softwareentwicklung behandelt der Baustein „CON.8 Softwareentwicklung“.

Im Baustein erfolgt eine kurze Darstellung der für das Thema spezifischen Gefährdungsaspekte, zum Beispiel die Umgehung der Autorisierung, unzureichende Eingabvalidierung und Ausgabecodierung, fehlende oder mangelhafte Fehlerbehandlung, unzureichende Protokollierung sicherheitsrelevanter Ereignisse, Missbrauch einer Webanwendung durch automatisierte Nutzung und Offenlegung sicherheitsrelevanter Informationen und unzureichendes Session-Management. Bei Webanwendungen sind diese Punkte besonders schwerwiegend, da sie in der Regel auch für Unbefugte grundsätzlich von außen zu erreichen sind. Daher füh-

ren Schwachstellen immer wieder dazu, dass Unternehmen und Behörden Schaden entsteht.

Entsprechend lauten die Basis-Anforderungen Authentisierung, Zugriffskontrolle, sicheres Session-Management, kontrolliertes Einbinden von Inhalten, Upload-Funktionen, Schutz vor unerlaubter automatisierter Nutzung, Schutz vertraulicher Daten, umfassende Eingabvalidierung und Ausgabecodierung, Schutz vor SQL-Injection und restriktive Herausgabe sicherheitsrelevanter Informationen. Entwickler sind angehalten, ihre Hausaufgaben zu machen.

Die Standard-Anforderungen sind dann eher auf die Aufrechterhaltung des Sicherheitsniveaus ausgerichtet und bestehen aus dem Management der Softwarearchitektur, der Verifikation essenzieller Änderungen, der Fehlerbehandlung, der sicheren HTTP-Konfiguration, der Verhinderung von Cross-Site-Request-Forgery und wann immer möglich der Nutzung der Mehrfaktor-Authentisierung.

Für einen erhöhten Schutzbedarf nennt das Kompendium die beiden Anforderungen Verhinderung der Blockade von Ressourcen – im Wesentlichen bezieht sich das auf DDoS-Angriffe (Denial of Service) und das Volllaufen der Protokolldateien – sowie kryptografische Absicherung vertraulicher Daten, bei der es um den Einsatz sicherer Verschlüsselungsalgorithmen geht.

Autos mit speziellen Gefahren

Der Baustein „INF.11 Allgemeines Fahrzeug“ klärt zunächst über die speziellen Gefahren auf, denen IT im Fahrzeug, also in einem besonderen Umfeld, ausgesetzt ist. Davon werden dann Anforderungen abgeleitet, die Fahrzeugnutzer und -halter erfüllen sollten, um den optimalen Fahrzeugbetrieb unter Berücksichtigung der Informationssicherheit zu gewährleisten.

Bei der im Baustein umfangreich geschilderten Abgrenzung und Modellierung

Versionsvergleich: Struktur des IT-Grundschutz-Kompends

Ausgabe 2020	Ausgabe 2021
APP.5.1 Allgemeine Groupware	APP.5.3 Allgemeiner E-Mail-Client und -Server
CON.4 Auswahl und Einsatz von Standard-Software	APP.6 Allgemeine Software
CON.5 Entwicklung und Einsatz von Individualsoftware	APP.7 Entwicklung von Individualsoftware
IND.1 Betriebs- und Steuerungstechnik	IND.1 Prozessleit- und Automatisierungstechnik
INF.3 Elektrotechnische Verkabelung	INF.12 Verkabelung
INF.4 IT-Verkabelung	
ORP.3 Sensibilisierung und Schulung	ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

im gleichnamigen Kapitel ist ersichtlich, dass dies der erste von mehreren Bausteinen sein wird. Er umfasst Fahrzeuge, die von Menschen gefahren werden, sowie ihre Besitzer.

Der Baustein möchte zunächst für die folgenden Gefährdungen sensibilisieren: fehlende oder unzureichende Regelungen, fehlendes Sicherheitsbewusstsein und Sorglosigkeit beim Umgang, ungeregelte Datenübertragung an Dritte und unsichere Kommunikationsschnittstellen, unsachgemäße Veränderungen, Manipulation, unbefugten Zutritt und Diebstahl, Gefahren im Zusammenhang mit Wartung, Reparatur und Updates, Gefahren bei der Aussonderung und unzulässige Temperatur und Luftfeuchte.

Die Basis-Anforderungen verlangen auch die notwendigen Prozesse wie Planung und Beschaffung, Wartung, Inspektion und Updates und das Erstellen von Regelungen für die Fahrzeugbenutzung. Die Standard-Anforderungen setzen darauf auf und unterstützen das ISMS mit dem Erstellen einer Sicherheitsrichtlinie zu diesem Spezialthema und einer Inventarliste, mit Handlungsanweisungen, mit dem Festlegen eines sachgerechten Umgangs mit Fahrzeugen und schützenswerten Informationen, dem Schutz vor witterungsbedingten Einflüssen, dem Sicherstellen der Versorgung und geregelter Aussonderung.

Zu den Anforderungen bei erhöhtem Schutzbedarf kommen Ersatzvorkehrungen. Sie betreffen Ausfälle, Diebstahlsicherung in Form von Bewachung,

Maßnahmen gegen schädigende Fremdeinwirkung, Schutz vertraulicher Informationen vor unbefugtem Zugriff und Kenntnisnahme, physische Absicherung der Schnittstellen, Vorhandensein einer Brandlöschanlage und die Netztrennung des In-Vehicle-Network mit einem Sonderfahrzeugnetz über Gateways.

Übersicht über Änderungen

Für die Edition 2021 wurden alle Bausteine sprachlich und redaktionell aus Gründen der besseren Verständlichkeit überarbeitet. Diese Änderungen weist das BSI ebenso wenig wie in der Vorgängerversion gesondert aus.

Da die inhaltlichen Änderungen jedoch Auswirkungen auf das ISMS, eine mögliche Zertifizierung oder Sicherheitskonzepte haben können, liefert die Behörde stets eine umfangreiche Änderungsdokumentation mit, in der sie alle Änderungen grundsätzlich benennt. Der Autor empfiehlt hier für den ISMS-Prozess (also die Umsetzung eines Informationsmanagementsystems) über mehrere Jahre den Einsatz entsprechender Tools. Das BSI hat eine unverbindliche Liste mit Herstellern kompatibler Tools veröffentlicht (zu finden über [ix.de/zaxj](https://www.ix.de/zaxj)).

Von besonderer Bedeutung sind in jeder Grundschutzaktualisierung die in den vorhandenen Bausteinen ergänzten neuen Anforderungen, die nachfolgend für die 2021er-Edition dargestellt sind. Denn sie bedeuten für manche Unternehmen eine besondere Herausforderung oder auch großen Aufwand beim Integrieren in das ISMS. Änderungen oder Streichungen dagegen sind weitgehend unkritisch.

Noch immer bedeutend: der menschliche Faktor

Im Baustein „ORP.1 Organisation“ wurden die Basis-Anforderungen „ORP.1.A15 Ansprechpartner zu Sicherheitsfragen“ und die Standard-Anforderung „ORP.1.A16 Mitarbeiterrichtlinie zur sicheren IT-Nut-



- Pünktlich veröffentlichte das BSI die Edition 2021 der BSI-IT-Grundschutz-Kataloge. Wie bei der Aktualisierung im vergangenen Jahr sind die meisten Änderungen innerhalb der Bausteine zu finden.
- Zwei neue Bausteine präzisieren die Anforderungen für die Entwicklung von Webanwendungen und die IT in Fahrzeugen.
- Die umfangreichen Änderungen erfordern von den Grundschutzverantwortlichen im Unternehmen Bewertungen in großem Umfang, um alles Wesentliche einzuordnen und zu planen – zum Glück gibt es inzwischen passende Tools.

zung“ hinzugefügt. Bei ORP.1.A15 wurde nachgeschärft, dass es unbedingt einen Ansprechpartner für Sicherheitsfragen geben muss, dieser bekannt ist und diese Information allen Mitarbeitern leicht zugänglich sein muss. ORP.1.A16 schlägt vor, im Rahmen des ISMS eine IT-Nutzerrichtlinie zu erstellen, damit den Benutzern eine sinnvolle Zusammenfassung aller Maßnahmen zur Verfügung steht.

Der Baustein „ORP.2 Personal“ wurde um zwei Basis-Anforderungen ergänzt. Die „ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitern“ wünscht die Verpflichtungserklärung und Kenntnis der gesetzlichen Rahmenbedingungen durch

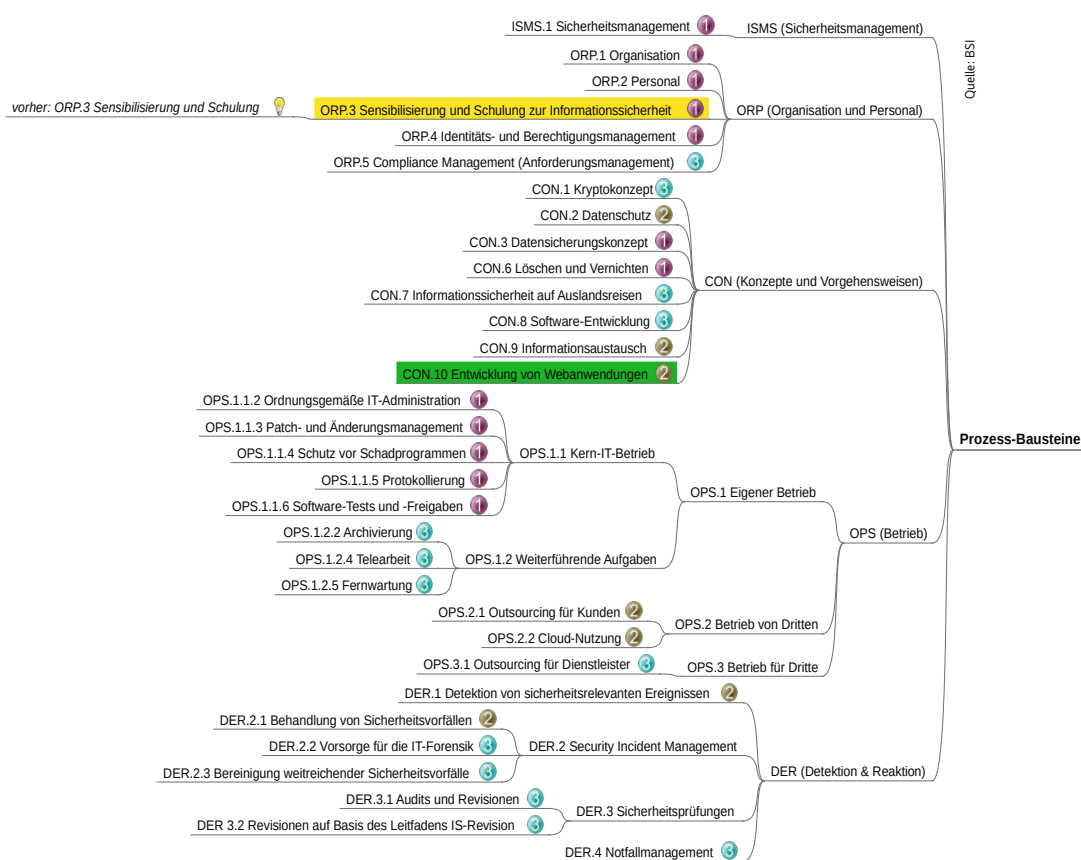
die Mitarbeiter einerseits und fordert andererseits eine geeignete Dokumentierung der Aufgaben und der Zuständigkeiten. Ferner sollen Mitarbeiter durch die Umsetzung der Maßnahmen auf Geheimhaltung verpflichtet und sensibilisiert werden. Die „ORP.2.A15 Auswahl von Personal nach Qualifikation“ fordert die stetige Weiterbildung des Personals und die sorgfältige Auswahl neuer Mitarbeiter.

Die nächste Änderung erwartet den Anwender im Baustein „ORP.4 Identitäts- und Berechtigungsmanagement“. Die dortige neue Anforderung bei erhöhtem Schutzbedarf ORP.4.A24 empfiehlt das Vieraugenprinzip für administrative Tä-

tigkeiten, also das Zerlegen von Passwörtern und das Verteilen auf mindestens zwei Personen und bei der Mehr-Faktor-Authentisierung das Zerlegen der Faktoren in mindestens zwei Teile.

Sicherheit konzeptionell vorbereiten

Im „Baustein CON.6 Löschen und Vernichten“ werden die in der Basis-Anforderung „CON.6.A12 Mindestanforderungen an Verfahren zur Löschung und Vernichtung“ genannten Vorgaben für solche Verfahren konkretisiert. Einige Aspekte werden dabei



zwingend gefordert, auf weitere, nicht immer zutreffende Aspekte wird hingewiesen. Die Standard-Anforderung „CON.6.A13 Vernichtung defekter digitaler Datenträger“ beschreibt, was zu tun ist, wenn Löschen nicht möglich ist, und weist auf notwendige Vereinbarungen mit potenziellen Dienstleistern hin. Die einzige und neue Anforderung bei erhöhtem Schutzbedarf, „CON.6.A14 Vernichten von Datenträgern auf erhöhter Sicherheitsstufe“, schließlich merkt an, dass das Vernichten entsprechend der Schutzstufe gemäß der Norm ISO/IEC 21964-1 zur Datenträgervernichtung erfolgen sollte.

Der Baustein „CON.8 Software-Entwicklung“ hat zwei neue Standard-Anfor-

derungen erhalten. Bei der „CON.8.A21 Bedrohungsmodellierung“ wird das ISMS aufgefordert, eine Analyse der möglichen späteren Bedrohungen auf Basis des Sicherheitsprofils, des Anforderungskatalogs und der geplanten Einsatzumgebung beziehungsweise des Einsatzszenarios durchzuführen und diese zu bewerten. Die Anforderung „CON.8.A22 Sicherer Software-Entwurf“ greift dann die Ergebnisse von CON.8.A21 auf und erstellt einen entsprechenden Softwareentwurf, auf dessen Basis eine sichere Softwarearchitektur entwickelt werden kann.

Der Baustein „CON.9 Informationsaustausch“ erhält die erste neue Anforderung für den erhöhten Schutzbedarf:

„CON.9.A9 Vertraulichkeitsvereinbarungen“. Sie besagt, dass vor einem Informationsaustausch mit Externen eine entsprechende Vereinbarung abzuschließen ist, und gibt Hinweise zum Inhalt.

Halten des Sicherheitsniveaus

Im Baustein „OPS.1.1.2 Ordnungsgemäße IT-Administration“ kam die Anforderung „OPS.1.1.2.A20 Verwaltung und Inbetriebnahme von Geräten“ hinzu. Sie ist nicht neu in den Katalogen, da sie aus dem Baustein „ORP.1 Organisation“ als ehemalige Anforderung „ORP.1.A7 Geräteverwaltung“ verschoben wurde.

Im Zuge der Konsolidierung von Anforderungen erhielt der Baustein „OPS.1.1.3 Patch- und Änderungsmanagement“ zwei neue Basis-Anforderungen: „OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software“ und „OPS.1.1.3.A16 Regelmäßige Suche nach Informationen zu Patches und Schwachstellen“. OPS.1.1.3.A15 fordert die Bewertung und Implementierung von Sicherheitskorrekturen in wiederkehrenden Abständen und OPS.1.1.3.A16 das regelmäßige Suchen nach Informationen über Patches und Updates und gibt Hinweise zum Umgang.

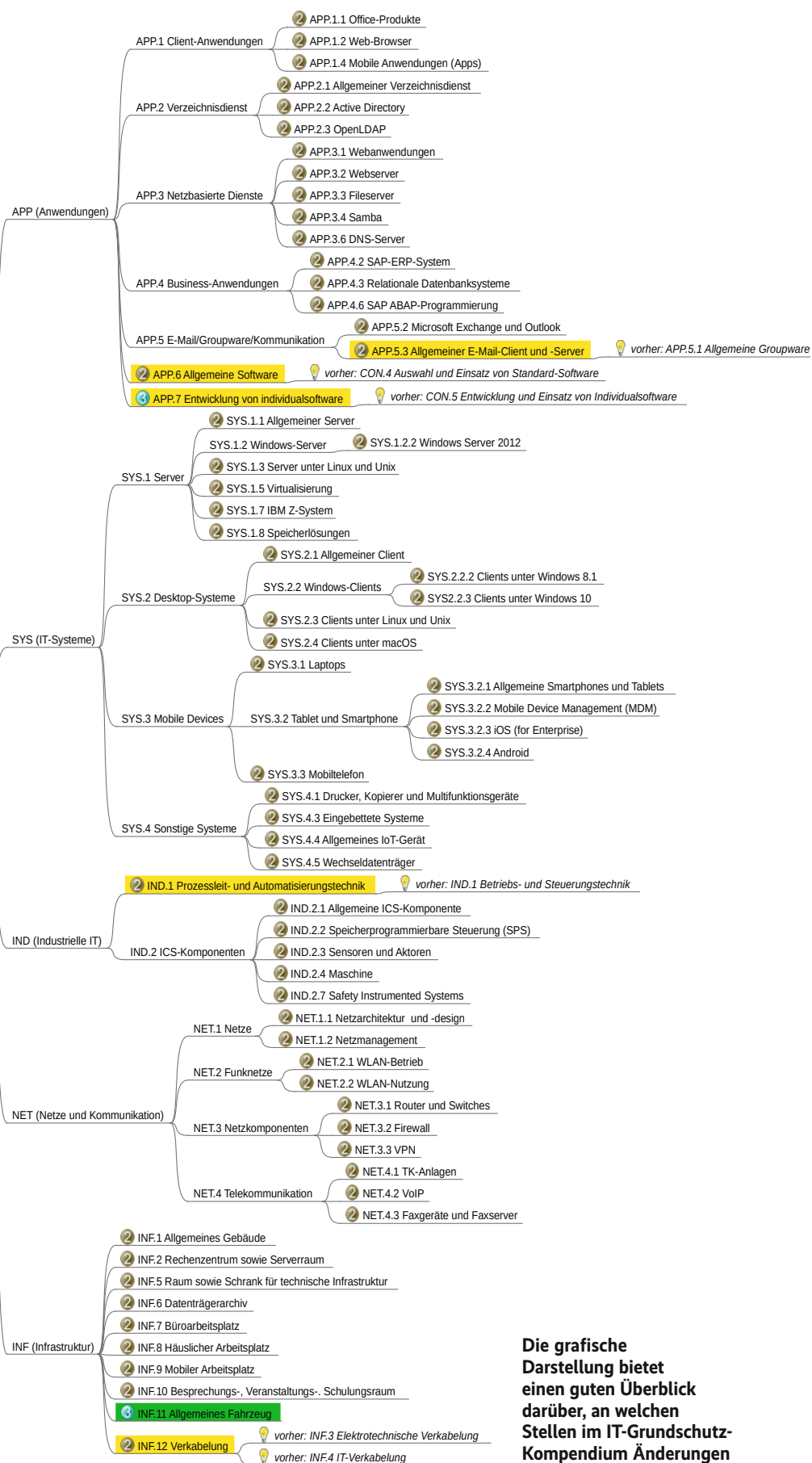
Im Baustein „OPS.1.1.6 Software-Tests und -Freigaben“ fordert die neue Standard-Anforderung „OPS.1.1.6.A15 Überprüfung der Installation und zugehörigen Dokumentation“ von einem ISMS, dies als Regelprozess einzuführen und umzusetzen. Die neue, zweite Anforderung bei erhöhtem Schutzbedarf verlangt mit „OPS.1.1.6.A16 Sicherheitsüberprüfung der Tester“, die Tester für solche Umgebungen sorgfältig auszuwählen und gegebenenfalls die Belange des Sicherheits-

überprüfungsgesetzes (SÜG) zu beachten.

Die neue Standard-Anforderung „OPS.1.2.5.A25 Entkopplung der Fernwartung“ im Baustein „OPS.1.2.5 Fernwartung“ fordert berechtigterweise die Nutzung von Sprung-Servern, wenn sich der Zugriff mittels Fernwartungsclient von außerhalb der Managementnetze nicht vermeiden lässt.

Sensibilisierung für Office-Gefahren

Der Baustein „APP.1.1 Office-Produkte“ möchte den Benutzer mit der neuen Basis-Anforderung „APP.1.1.A17 Sensibilisierung zu spezifischen Office-Eigenschaften“ für die zunehmende Gefahr von Sicherheitsvorfällen durch Kryptotrojaner sensibilisieren. Daher soll die jeweilige Organisation sie zu den Gefahren durch aktive Inhalte, dem Umgang mit externen Office-Dokumenten sowie den Möglichkeiten und Grenzen von Sicherheitsfunktionen informieren und aufklären.



Die grafische Darstellung bietet einen guten Überblick darüber, an welchen Stellen im IT-Grundschutz-Kompodium Änderungen stattgefunden haben.

Der Baustein „APP.1.2 Web-browser“ soll mit der neuen Basis-Anforderung „APP.1.2.A13 Nutzung von DNS-over-HTTPS“ erreichen, dass diese Funktion möglichst eingesetzt wird.

In „APP.1.4 Mobile Anwendungen (Apps)“ gibt es die neue Anforderung „APP.1.4.A16: Mobile Application Management“ bei erhöhtem Schutzbedarf. Sie plädiert dafür, dienstliche Apps spätestens bei erhöhtem Schutzbedarf zentral über ein Mobile Application Management zu konfigurieren.

Der Baustein „APP.7 Entwicklung von Individualsoftware“ löst den Baustein „CON.5 Entwicklung und Einsatz von Individualsoftware“ ab. Er wurde im Zusammenhang der Neukonzeptionierung des Bausteins „APP.6 Allgemeine Software“ in die APP-Schicht verschoben, dabei neu aufgebaut und erhielt eine Konkretisierung der Abgrenzung gegenüber dem Baustein „CON.8 Software-Entwicklung“. Entsprechend sind mehrere Basis-Anforderungen entstanden, die auf die speziellen Belange von Individualsoftware eingehen.

Sichere Planung ist alles

So fordert APP.7.A1 die Erweiterung der Planung des Softwareeinsatzes um Aspekte von Individualsoftware und APP.7.A2 schreibt Sicherheitsanforderungen an den Prozess der Softwareentwicklung vor. Dagegen fordert APP.7.A3 das Festlegen der Sicherheitsfunktionen zur Systemintegration und APP.7.A4 will im Rahmen der anforderungsgerechten Beauftragung die Sicherheitsbelange berücksichtigt wissen.

Die Standard-Anforderungen „APP.7.A7 Sichere Beschaffung von Individualsoftware“ und „APP.7.A8 Frühzeitige Beteiligung des Fachverantwortlichen bei entwicklungsbegleitenden Software-Tests“ weisen wiederum darauf hin, dass ein funktionierendes ISMS auch diese beiden Aspekte umfassen sollte.

Manchmal muss es zertifiziert sein

Bei erhöhtem Schutzbedarf enthält APP.7.A10 die Forderung, bei der Entwicklung sicherheitskritischer Anwendungen zertifizierte Softwareentwicklungsunternehmen zu beauftragen.

Änderung der Rollenbezeichnungen

Ausgabe 2020	Ausgabe 2021
Änderungsmanager Archivverwalter Ermittler Ermittlungsleiter Fax-Verantwortlicher TK-Anlagen-Verantwortlicher	Fachverantwortlicher
Beschaffer, Leiter Beschaffung	Beschaffungsstelle
Betriebsleiter Leiter Produktion und Fertigung	OT-Leiter
Innerer Dienst Leiter Organisation	Zentrale Verwaltung
Leitstellen-Operator Telearbeiter	Mitarbeiter
Hersteller	entfallen
ICS-Administrator	OT-Betrieb
Leiter Entwicklung	Entwickler
Leiter Haustechnik	Haustechnik
Leiter IT	IT-Betrieb
Leiter Netze	Planer
Leiter Personal	Personalabteilung
Pressestelle	Institutionsleitung
Verantwortlicher für die IS-Revision	Informationssicherheitsbeauftragter (ISB)

Im Baustein „SYS.1.1 Allgemeiner Server“ enthält die neue Standard-Anforderung „SYS.1.1.A35 Erstellung und Pflege eines Betriebshandbuchs“ die Empfehlung, alle erforderlichen Regelungen, Anforderungen und Einstellungen zum generellen Betrieb von Servern an einer Stelle zu dokumentieren. Außerdem mahnt die Anforderung an, dies pro Serverart zu tun, regelmäßig zu aktualisieren und die Aufzeichnungen vor Unberechtigten geschützt aufzubewahren. In den Anforderungen zu erhöhtem Schutzbedarf wurde „SYS.1.1.A36 Absicherung des Bootvorgangs“ hinzugefügt. Sie fordert, Bootloader und Betriebssystemkern durch Secure Boot zu schützen, da anderenfalls das Unterwandern von Sicherheitsmaßnahmen und Integrität möglich ist.

Für den Baustein „SYS.2.1 Allgemeiner Client“ wurde die Basis-Anforderung „SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen“ aus dem Baustein „SYS.2.3 Clients unter Linux und Unix“ übernommen. Hier steht für alle Clients der Organisation der Grundsatz im Vordergrund, nur zwingend notwendige Cloud- und Online-Funktionen des Betriebssystems zu erlauben.

Darüber hinaus wurden als Standard-Anforderungen die „SYS.2.1.A43 Lokale Sicherheitsrichtlinien für Clients“ und „SYS.2.1.A44 Verwaltung der Sicherheitsrichtlinien von Clients“ als generalisierte Versionen der entfallenen Anforderungen „SYS.2.2.3.A7 Lokale Sicherheitsrichtlinien für Windows 10“ und „SYS.2.2.3.A8 Zentrale Verwaltung der Sicherheitsrichtlinien von Clients“ übernommen. In vie-

len Fällen können und sollen lokale Einstellungen zentral gesetzt und durchgesetzt werden. So leisten die Einstellungen einen Beitrag zur Aufrechterhaltung des gewünschten Sicherheitsniveaus auf allen Clients. Die Anforderung bei erhöhtem Schutzbedarf „SYS.2.1.A45 Erweiterte Protokollierung“ erinnert daran, dass es unter diesen Umständen sinnvoll sein kann, Clientverhalten, das nicht mit der Sicherheit direkt in Verbindung steht, zu protokollieren und unverzüglich möglichst automatisiert auszuwerten.

Im Baustein „SYS.3.2.1 Allgemeine Smartphones und Tablets“ sind einige kleinere Standard-Anforderungen hinzugekommen. „SYS.3.2.1.A31 Regelung zu

Mobile-Payment“ und „SYS.3.2.1.A32 MDM-Nutzung“, in der empfohlen wird, Regelungen zum Mobile Device Management (MDM) zu treffen. „SYS.3.2.1.A33 Auswahl und Installation von Sicherheits-Apps“ weist auf den Einsatz zusätzlicher Sicherheits-Apps hin. Die neue Standard-Anforderung „SYS.3.2.1.A34 Konfiguration des verwendeten DNS-Servers“ schlägt vor, bei eingesetzten DNS-Servern eigene Einstellungen vorzunehmen, um hier ebenfalls möglichem Missbrauch vorzubeugen.

Die Anforderung bei erhöhtem Schutzbedarf „SYS.3.2.1.A35 Verwendung einer Firewall“, die aus dem Baustein „SYS.3.2.4 Android“ hierher verschoben wurde, soll zusätzliche Sicherheit bringen.

Stiefkind industrielle IT

Lange Zeit wurde die industrielle IT aus Sicherheitssicht vernachlässigt, erst in den letzten Jahren berücksichtigt man sie nach und nach. Im Baustein „IND.1 Prozessleit- und Automatisierungstechnik“ kamen mehrere Anforderungen hinzu. Die beiden Basis-Anforderungen „IND.1.A18 Protokollierung“ und „IND.1.A19 Erstellung von Datensicherungen“ fordern unabhängig, diese Themen umzusetzen.

Es folgen vier Standard-Anforderungen. Die „IND.1.A20 Systemdokumentation“ mahnt die Dokumentation für die Industriekomponenten an, um die oft speziellen Besonderheiten im Betrieb und die Möglichkeiten zur Systemverwaltung festzuhalten. Bei der „IND.1.A21 Doku-

Abgleich GS-Kompendium 2021 mit 2020 – Übersicht der Teilanforderungen (Auszug)

Baustein	Anforderung	Teilanforderung 2020	Vergleich	Status	Bewertung
ISMS.1 Sicherheitsmanagement	ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	Es MUSS regelmäßig geprüft werden, ob die Organisationsstruktur für Informationssicherheit noch angemessen ist oder ob sie an neue Rahmenbedingungen angepasst werden muss.	Neu: Es MUSS regelmäßig geprüft werden, ob die Organisationsstruktur für Informationssicherheit noch angemessen ist oder ob sie an neue Rahmenbedingungen angepasst werden muss.	gleich	
ISMS.1 Sicherheitsmanagement	ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen	Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert werden. Die Sicherheitsmaßnahmen SOLLTEN regelmäßig aktualisiert werden.	Alt: Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert werden. Die Sicherheitsmaßnahmen SOLLTEN regelmäßig aktualisiert werden. Neu: Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert und regelmäßig aktualisiert werden.	Änderung	mittel
ISMS.1 Sicherheitsmanagement	ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess	Alle Mitarbeiter MÜSSEN in den Sicherheitsprozess integriert sein. Hierfür MÜSSEN sie über Hintergründe und die für sie relevanten Gefährdungen informiert sein. Sie MÜSSEN Sicherheitsmaßnahmen kennen und umsetzen, die ihren Arbeitsplatz betreffen.	Alt: Alle Mitarbeiter MÜSSEN in den Sicherheitsprozess integriert sein. Hierfür MÜSSEN sie über Hintergründe und die für sie relevanten Gefährdungen informiert sein. Sie MÜSSEN Sicherheitsmaßnahmen kennen und umsetzen, die ihren Arbeitsplatz betreffen. Neu: Alle Mitarbeiter MÜSSEN in den Sicherheitsprozess integriert sein. Hierfür MÜSSEN sie über Hintergründe und die für sie relevanten Gefährdungen informiert sein. Sie MÜSSEN Sicherheitsmaßnahmen kennen und umsetzen, die ihren Arbeitsplatz betreffen. Sie MÜSSEN in die Lage versetzt werden, Sicherheit aktiv mitzugestalten. Daher SOLLTEN die Mitarbeiter frühzeitig bei der Planung von Sicherheitsmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt werden.	Änderung	kritisch
ISMS.1 Sicherheitsmanagement	ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess	Bei der Einführung von Sicherheitsrichtlinien und Sicherheitswerkzeugen MÜSSEN die Mitarbeiter ausreichend informiert sein, wie diese anzuwenden sind.	Neu: Bei der Einführung von Sicherheitsrichtlinien und Sicherheitswerkzeugen MÜSSEN die Mitarbeiter ausreichend informiert sein, wie diese anzuwenden sind.	gleich	
ISMS.1 Sicherheitsmanagement	ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess	Die Mitarbeiter MÜSSEN darüber aufgeklärt werden, welche Konsequenzen eine Verletzung der Sicherheitsvorgaben haben kann.	Neu: Die Mitarbeiter MÜSSEN darüber aufgeklärt werden, welche Konsequenzen eine Verletzung der Sicherheitsvorgaben haben kann.	gleich	
ISMS.1 Sicherheitsmanagement	ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse	Informationssicherheit SOLLTE außerdem mit anderen Bereichen in der Institution, die sich mit Sicherheit und Risikomanagement beschäftigen, abgestimmt werden.	Neu: Informationssicherheit SOLLTE außerdem mit anderen Bereichen in der Institution, die sich mit Sicherheit und Risikomanagement beschäftigen, abgestimmt werden.	gleich	

mentation der Kommunikationsbeziehungen“ geht es um Kommunikationstransparenz und darum, dass ausschließlich die gewünschte Kommunikation stattfindet und neue Komponenten unverzüglich auffallen.

„IND.1A22 Zentrale Systemprotokollierung und -überwachung“ ergänzt die neue Basis-Anforderung IND.1.A18 um zentrale Protokollspeicher und eine Alarmierung bei sicherheitskritischen Ereignissen, während die „IND.1.A23 Aussonderung von ICS-Komponenten“ am Ende des Lebenszyklus der Komponenten auf das sichere Löschen und das Entfernen von Zugangsdaten verweist. Die Anforderung bei erhöhtem Schutzbedarf „IND.1.A24 Kommunikation im Störfall“ weist darauf hin, alternative und unabhängige Kommunikationsmöglichkeiten für den Fall der Fälle vorzusehen.

Referenz an mehreren Stellen

Wenig komplett Neues gibt es bei den Netzverbindungen und der Kommunikation sowie bei den baulich-technischen Gegebenheiten. Bei der Notfallvorsorge stellt sich dem Anwender immer die Frage, ob dieser

Aspekt besser in übergeordneten Prozessen realisiert werden sollte oder beim konkreten Fachthema. Der „Baustein NET.3.2 Firewall“ erinnert daher mit der neuen Standard-Anforderung „NET.3.2.A32 Notfallvorsorge für die Firewall“ analog zur Anforderung im Baustein „NET.3.1 Router und Switches“ zumindest an die Umsetzung dieses wichtigen Schrittes.

Der Baustein „INF.1 Allgemeines Gebäude“ wurde um die neue Standard-Anforderung „INF.1.A36 Regelmäßige Aktualisierungen der Dokumentation“ ergänzt. Sie soll daran erinnern, sich wenigstens alle drei Jahre auch dieses Themas anzunehmen und bei Änderungen die Mitarbeiter zu informieren. Mit der neuen Anforderung für den erhöhten Schutzbedarf zum Perimeterschutz von Gebäuden INF.1.A35 gibt das BSI hier Hinweise, welche Komponenten im Bedarfsfall hinsichtlich ihrer Umsetzbarkeit und ihres Nutzens in eine planerische Prüfung einbezogen werden sollten.

Mit der Ergänzung des Bausteins „INF.9 Mobiler Arbeitsplatz“ um die Standard-Anforderung „INF.9.A12 Nutzung eines Bildschirmschutzes“ spricht sich das BSI für die generelle Nutzung der Bildschirmsperre aus.

Fazit

Die Neuausgabe des IT-Grundschutz-Kompendiums 2021 bietet den Anwendern den Stand der Technik in der Umsetzung von Informationssicherheit als gut strukturiertes Werk. Neben zwei vollständig neuen Bausteinen sind viele weitere Sicherheitsaspekte in die aktuelle Ausgabe eingeflossen. Aufgrund der vielen Änderungen wird eine Toolunterstützung bei der Umsetzung immer wichtiger. Leider dauert es eine Weile, bis die Hersteller den neuen Katalog eingearbeitet haben. Bis dahin gilt bei Zertifizierung und Anwendung wie immer ein Jahr Übergangsfrist, dann ist die jetzige Edition verbindlich. (ur@ix.de)

Quellen

Das neue BSI-IT-Grundschutz-Kompendium, die Änderungsdokumente sowie weitere Hilfestellungen sind über ix.de/zaxj zu finden.

Ronny Frankenstein

ist Mitautor des IT-Grundschutz-Kompendiums, IT-Grundschutz-Evangelist und Director für Cyber Security bei der HiSolutions AG.