Bundesamt
für Sicherheit in der
Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

30 Jahre IT-Grundschutz: Gestern, heute, morgen

Nürnberg, 23.10.2024, 13:00 Uhr

Agenda

13:00 Uhr: Begrüßung und Keynote (Sandro Amendola)
13:15 Uhr: IT-Grundschutz gestern und heute (Holger Schildt)
13:35 Uhr: Weg in die Basis-Absicherung (WiBA) (Stefanie Euler)
13:55 Uhr: Cybersicherheitsvorgaben für die Bundesverwaltung (Julia Hein)
14:15 Uhr: Vision zur Weiterentwicklung des IT-Grundschutzes (Dr. Dennis Kügler)
14:30 Uhr: 15 Minuten Pause
14:45 Uhr: Struktur der zukünftige Anforderungen (Florian Göhler)
15:05 Uhr: Struktur des IT-Grundschutz-Kompendium (Christoph Weißenborn)
15:25 Uhr: Und was ist mit Dokumentation? (Daniel Gilles)
15:45 Uhr: Kennziffern zur Effizienzmessung (Stefan Schuck)
16:05 Uhr: Pause
16:15 Uhr: Fragen und Diskussion mit allen Vortragenden
17:00 Uhr: Ende

Bundesamt
für Sicherheit in der
Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

Begrüßung

Sandro Amendola, BSI

Vision

IT-Grundschutz++

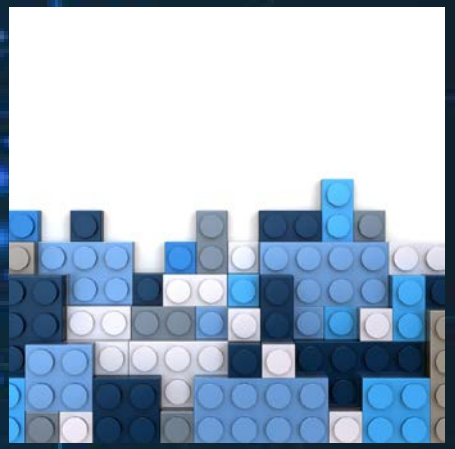
Cybersicherheit ist mess - & automatisierbar:

Sicherheitsanforderungen werden als priorisierte, maschinenlesbare Regeln in kontinuierlichen PDCA-Zyklen erstellt

IT-Grundschutz wird in einem umfangreichen Projekt zu IT-Grundschutz++:

IT-Grundschutz++ - eine BSI-Lösung, die wirklich hilft

Mehr Anwender-freundlichkeit



Digitale Syntax zur Maschinenlesbarkeit

Integrierte Fortschrittsmessung

Erhebliche Reduktion der Aufwände

Bild: ©AdobeStock, Nirut

Mehrwert

Schneller im Ziel durch
Filtern, Automatisieren und Vereinheitlichen

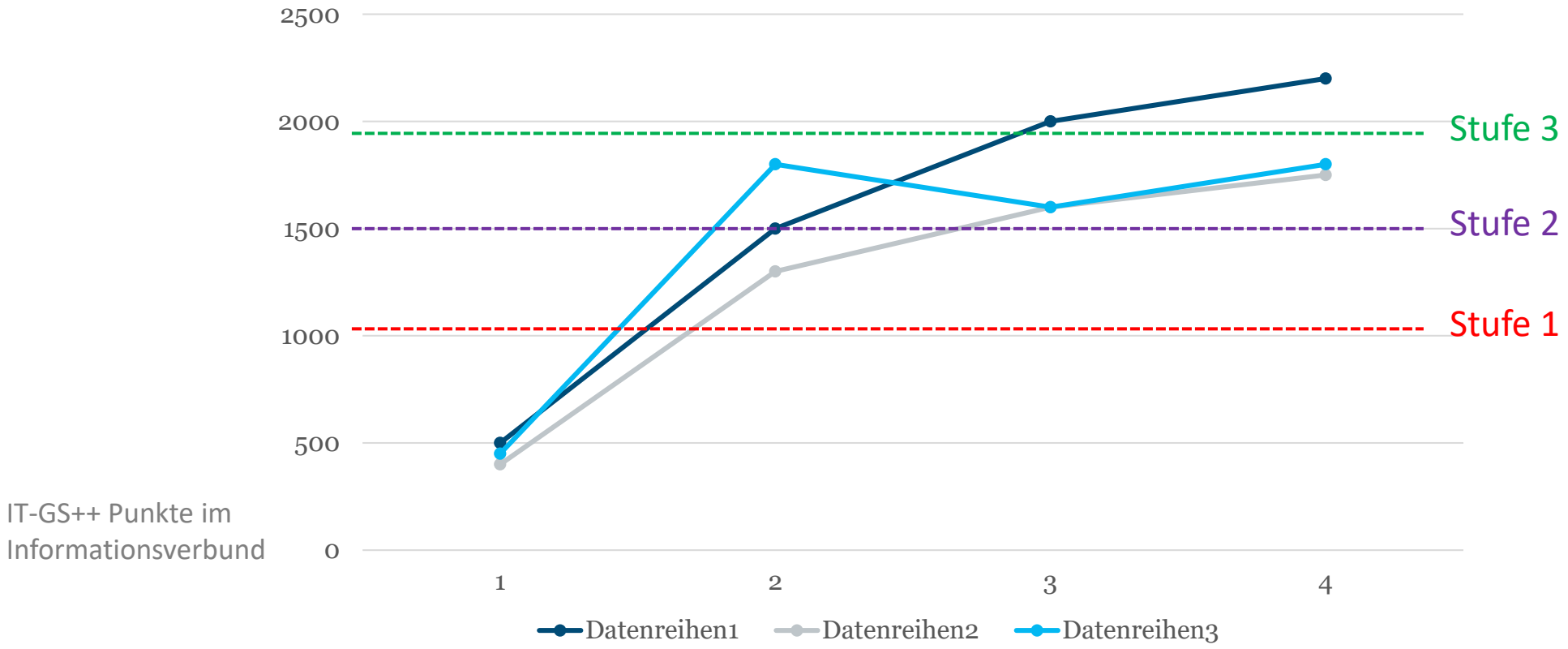
Fortschritt dynamisch messen
mit Kennzahlindikatoren

Bewährte Inhalte,
klarer formuliert und erklärt

Anpassung an
technische und rechtliche Neuerungen

Agile Veröffentlichung,
zeitnah und nachvollziehbar

Beispiel IT-Grundschutz++ Dashboard für das ISMS einer Institution



Nutzen Sie die Gelegenheit!

Bundesamt
für Sicherheit in der
Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

IT-Grundschutz gestern und heute

Holger Schildt, BSI

IT-Grundschutz

Basis zum Aufbau eines ISMS

für Behörden und Unternehmen jeglicher Art und Größe

Best-Practices unter Berücksichtigung des Stands der Technik

Rahmenwerk für Informationssicherheit

De-facto-Standard in Deutschland

30 Jahre IT-Grundschutz

Ein Schutz für alle ++

1994
Veröffentlichung IT-Grundschutzhandbuch

1998
Veröffentlichung GSTOOL

2002
Erteilung erstes Auditoren-Zertifikat

Erteilung erstes IT-Grundschutz-Zertifikat

2003
Veröffentlichung Leitfaden IT-Sicherheit – IT-Grundschutz kompakt

Erster IT-Grundschutz-Tag

Veröffentlichung Webkurs IT-Grundschutz

IT-Grundschutz als Basis für Informationssicherheit in Estland

2005
Veröffentlichung BSI-Standards 100-1, 100-2 und 100-3 sowie IT-Grundschutz-Kataloge

Veröffentlichung Webkurs GSTOOL

Kompatibilität ISO 27001 / Erstes ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

2008
Veröffentlichung BSI-Standard 100-4

2009
Veröffentlichung Webkurs Notfall-management

2015
Beginn Modernisierung des IT-Grundschutzes

2017
Veröffentlichung BSI-Standards 200-1, 200-2 und 200-3

2018
Veröffentlichung IT-Grundschutz-Kompendium

Erstes IT-Grundschutz-Profil

Veröffentlichung Online-Kurs zum modernisierten IT-Grundschutz

Erstes ISO 27001-Zertifikat auf der Basis des modernisierten IT-Grundschutzes

2019
Testat nach der Basis-Absicherung

IT-Grundschutz-Berater

IT-Grundschutz-Praktiker

2020
Veranstaltung des ersten Online-IT-Grundschutz-Tags

2021
Veröffentlichung eines Community Draft zum BSI-Standard 200-4

2022
Veröffentlichung der Edition 2022 des IT-Grundschutz-Kompendiums

2023
„Weg in die Basis-Absicherung" (WiBA) als Einstieg in den IT-Grundschutz wurde etabliert

Beginn der Überarbeitung des IT-Grundschutzes unter dem Arbeitstitel „IT-Grundschutz++"

Veröffentlichung BSI-Standard 200-4

2024
Einführung des Schulungsprogramms zum BCM-Praktiker

Anwenderworkshops und Veröffentlichung erster Dokumente unter dem Arbeitstitel „IT-Grundschutz++"

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Gestern | Heute | Morgen

1994: Veröffentlichung des IT-Grundschutzhandbuches

- Davor: IT-Sicherheitshandbuch (1992)
- 1992-1994 Handlungsbedarf:
  - Erstellung von IT-Sicherheitskonzepten vereinfachen, ohne die Qualität einzuschränken
  - Aufwand für IT-Sicherheitskonzepte auf hochschutzbedürftige IT-Systeme konzentrieren
  - für mittelschutzbedürftige IT-Systeme: IT-Grundschutz als standardisiertes Verfahren
- 1994
  - Die erste Ausgabe des IT-Grundschutzhandbuchs im Eigendruck
- 1995
  - Druckausgabe durch Bundesanzeiger

2002: Zertifizierung nach IT-Grundschutz

- Nachweis zur Umsetzung des IT-Grundschutzes
- Zertifizierung durch das BSI
- Zusammenarbeit mit beim BSI lizenzierter Auditoren
- 2005: ISO Zertifikat auf der Basis von IT-Grundschutz

2005: BSI-Standards 100-1/2/3 und IT-Grundschutz-Kataloge

Neustrukturierung und internationale Ausrichtung

- IT-Grundschutzhandbuch wurde durch zwei Werke abgelöst
  - Trennung Vorgehensweise (**BSI-Standards**) und **IT-Grundschutz-Kataloge**
- Wesentliche Neuerungen
  - Stärkere Fokussierung auf Managementsysteme
    (Sicherstellung ISO 27001-Kompatibilität)
  - Paradigmenwechsel: von der IT-Sicherheit hin zur Informationssicherheit
  - Einführung Schichtenmodell
- Ziel: **Sicherheitsniveau** erreichen, das für den **normalen Schutzbedarf** angemessen und ausreichend ist und als **Basis für Hochschutz** dienen kann
  - **Fokus: ISMS / Informationssicherheit**

2017: BSI-Standards 200-1/2/3 und IT-Grundschutz-Kompendium

Grundlegende Überarbeitung der Methode und IT-Grundschutz-Kataloge

- **Wesentliche Neuerungen**
  - Einführung unterschiedlicher Vorgehensweisen
  - Grundlegende Überarbeitung des Schichtenmodells und Umstellung der IT-Grundschutz-Kataloge auf das IT-Grundschutz-Kompendium
  - Anforderungen anstatt Maßnahmen in den Bausteinen (maximal 10 Seiten)
  - Stärkere Prozessorientierung (Einführung Prozessschicht und Systemschicht)
  - Vollständige Umstellung der Risikoanalyse auf G0er und Umstellung auf Matrix-Ansatz für die Bewertung von Risiken
  - Stärkere Berücksichtigung von anwenderspezifischen Anforderungen (IT-Grundschutz-Profile)
  - Erweiterung der Methode um Cloud Computing und Virtualisierung
  - Integration von industrieller IT und von Detektionsprozessen

Fokus: ISMS / Informationssicherheit

2018: Veröffentlichung erstes IT-Grundschutz-Profil

Werkzeug für anwenderspezifische Empfehlungen

Individuelle Anpassungen des IT-Grundschutzes an die jeweiligen Bedürfnisse möglich

Berücksichtigt Möglichkeiten und Risiken der Institution

Profile beziehen sich auf typische IT-Szenarien

Profile werden in der Regel durch Dritte (Verbände, Branchen, ...) und nicht durch das BSI erstellt

Nicht als BSI-Vorgabe zu verstehen!


IT-GRUNDSCHUTZ-PROFIL

BASIS-ABSICHERUNG KOMMUNALVERWALTUNG

08.05.2018

Deutscher Städtetag

DEUTSCHER LANDKREISTAG

DStGB

ARBEITSGRUPPE „MODERNISIERUNG IT-GRUNDSCHUTZ" mit Unterstützung durch
Deutscher Städtetag
Deutscher Landkreistag
Deutscher Städte- und Gemeindebund

2023: BSI-Standard 200-4

- BSI-Standard 200-4 Business Continuity Management
- Modernisierung des BSI-Standards 100-4 Notfallmanagement nach umfangreicher Beteiligung der Anwenderinnen und Anwender
- ermöglicht insbesondere unerfahrenen BCM-Anwenderinnen und -Anwendern einen leichten Einstieg
- Separater normativer Anforderungskatalog

2023: letzte Edition IT-Grundschutz-Kompendium

Umfang: insgesamt 111 Bausteine

Weiterhin laufende Veröffentlichung von Final Drafts

- SYS.2.1 Allgemeiner Client
- CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)
- CON.11.2 Geheimschutz VS-VERTRAULICH oder höher

Eventuell auftretende Fehler werden in Errata korrigiert

Grundlage für eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz bleibt Edition 2023

BSI Zertifizierungsstelle – Zahlen & Fakten (Stand 09/2024)

Zertifizierungsstelle existiert seit
2002

630 ISO 27001 Zertifikate auf der Basis von IT-Grundschutz ausgestellt

~75 Auditoren

159 aktuell gültige Zertifikate

49% an Unternehmen ausgestellt

51% an Regierungseinrichtungen ausgestellt

IT-Grundschutz-Berater sowie BCM- und IT-Grundschutz-Praktiker

- Über 160 IT-Grundschutz-Berater
- Das Schulungskonzept des BSI stellt ein einheitliches hohes Niveau an fachlicher Expertise sicher.
- Es besteht eine große Auswahl an Dienstleistern, doch wer hat die von mir benötigte Expertise?
- BCM-Praktiker angelaufen
- Für einen Informationssicherheitsprozess fehlt es in vielen Institutionen an der entsprechenden Expertise.
- Aus der kontinuierlich hohen Bedrohungslage und der schnell voranschreitenden Digitalisierung erwächst mehr und mehr der Bedarf an Informationssicherheit.
- Über 60 Schulungsanbieter

Ausbildung von über 6000 IT-Grundschutz-Praktikern seit 2019

IT-Grundschutz heute

Sonstiges aus der Welt des IT-Grundschutzes

Erstellung von weiteren Bausteinen als Draft

Unterstützung bei der Erstellung von IT-Grundschutz-Profilen

derzeit über 25 auf der Webseite des BSI veröffentlicht

Durchführung von IT-Grundschutz-Tagen

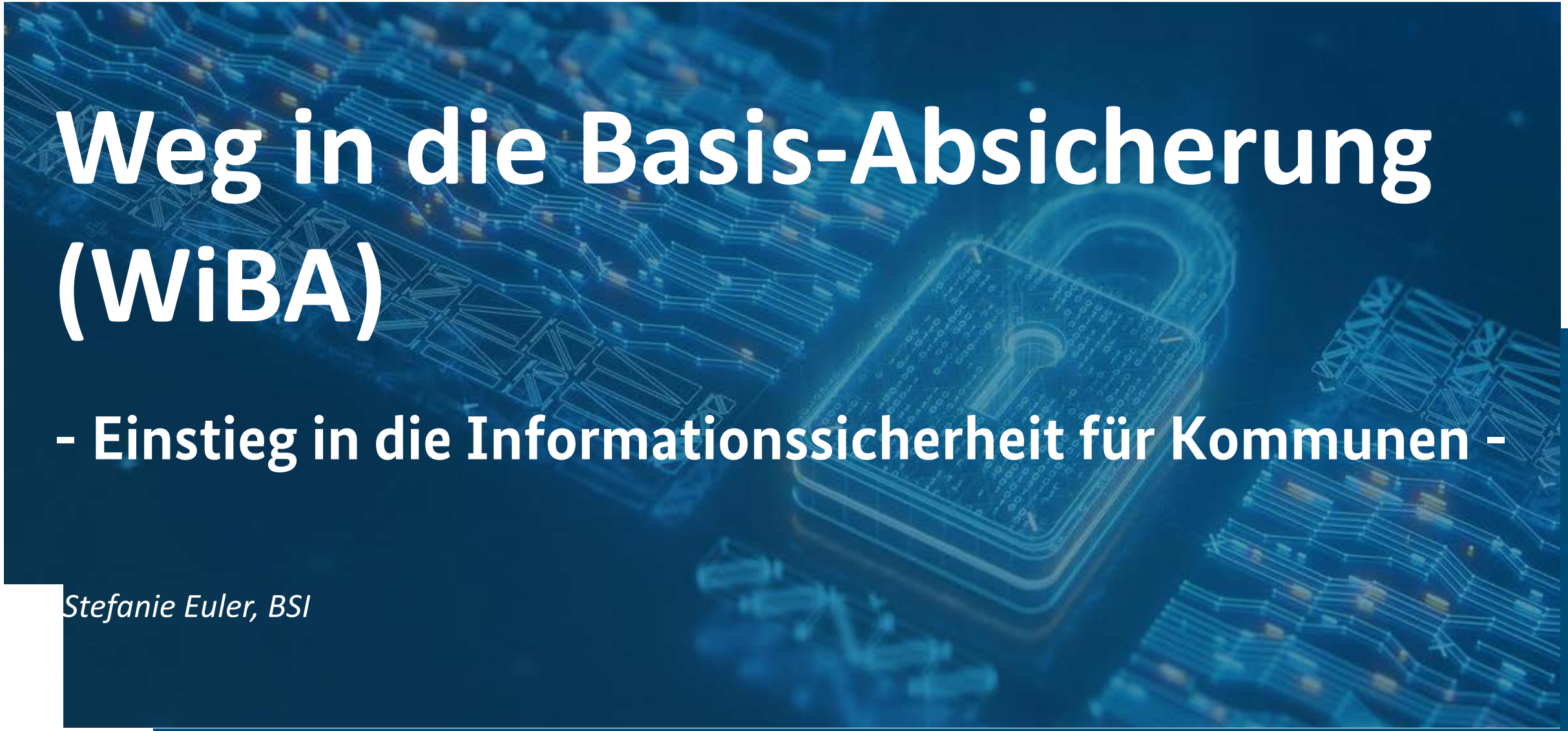
Save-the-Date: 4. Februar 2025 in Magdeburg

Weg in die Basis-Absicherung (WiBA)

Bundesamt für Sicherheit in der Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland Digital•Sicher•BSI•



Weg in die Basis-Absicherung (WiBA)

- Einstieg in die Informationssicherheit für Kommunen -

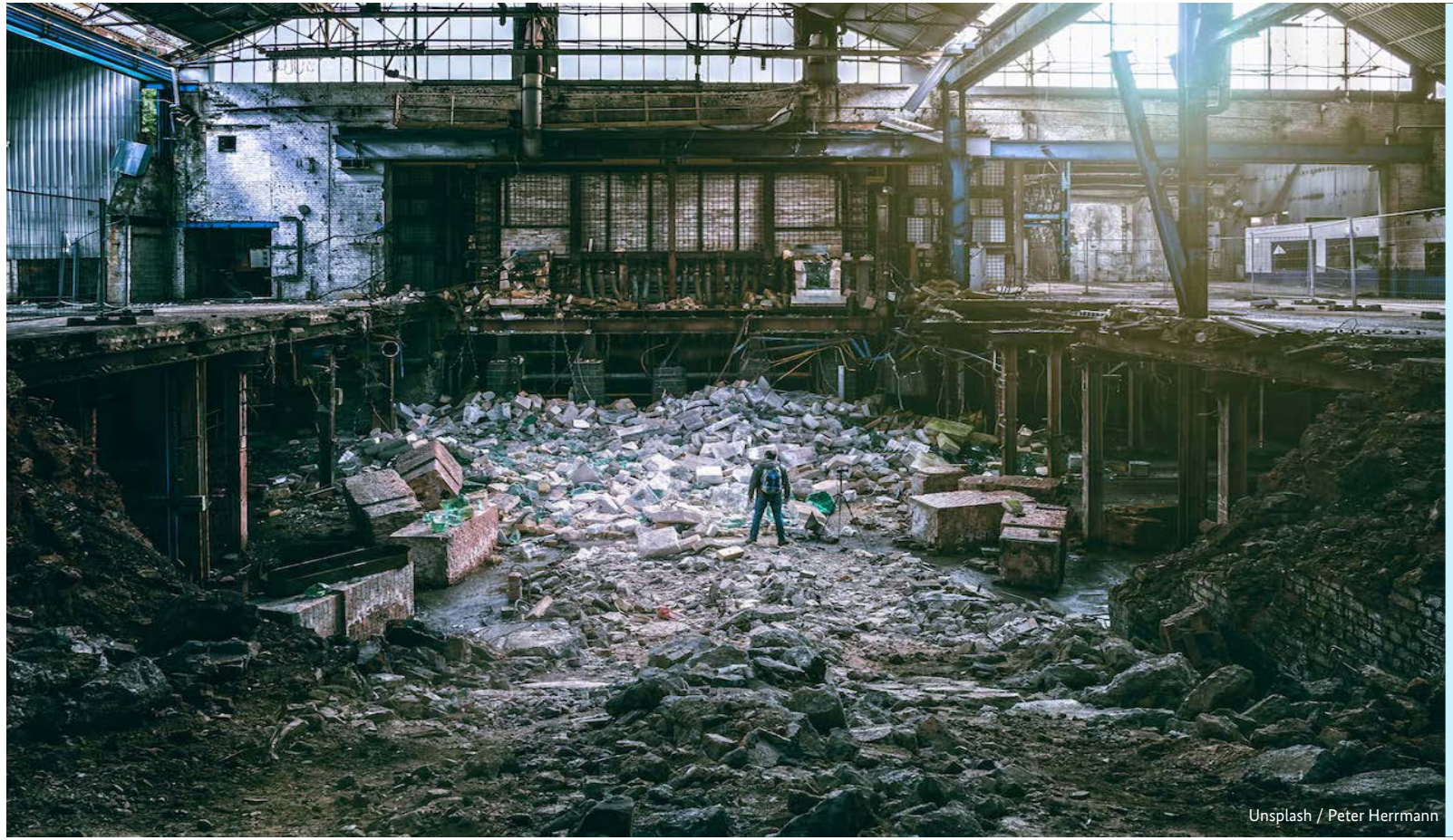
Stefanie Euler, BSI

Ganzheitliche Informationssicherheit ist …

- **Chef:Innensache!**
  - Die Verwaltungsspitze trägt die Gesamtverantwortung, mit starken Partnern an der Seite (z.B. ISB, IT-Leitung)

- **Ein fortlaufender Prozess!**
  - Sicherheit wird geschaffen und im Zyklus durch Kontrolle und Fortentwicklung aufrechterhalten
  - Einstieg: Weg in die Basis-Absicherung (WiBA)

#WoSollIchAnfangen - Ausgangslage


Unsplash / Peter Herrmann

Einstieg in den BSI IT-Grundschutz trotz Basis-Absicherung teilweise zu komplex:

vielen kleinen Institutionen fehlen ausreichend Ressourcen und Know-How

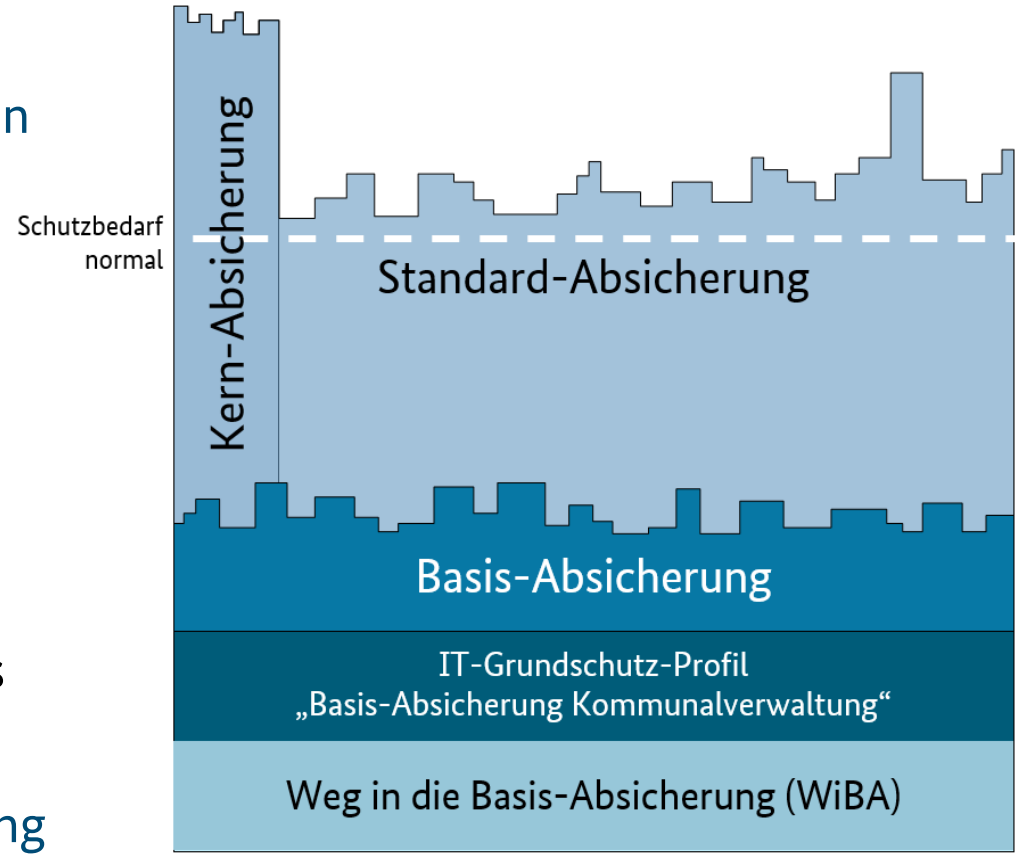
Im Fokus: **Kommunen**

Lösungsansatz

Ziel: Sachstände erheben und umzusetzende Anforderungen mittels Prüffragen und Checklisten mit wenig Aufwänden identifizieren.

Grundlage: IT-Grundschutz-Profil
„Basis-Absicherung Kommunalverwaltung“

- WiBA ist **KEIN** Standard für Informationssicherheit
- Keine Vorkenntnisse zur Methodik des IT-Grundschutzes notwendig.
- Es werden Hilfsmittel bereitgestellt, die bei der Umsetzung unterstützen.



WiBA-Vorgehensweise

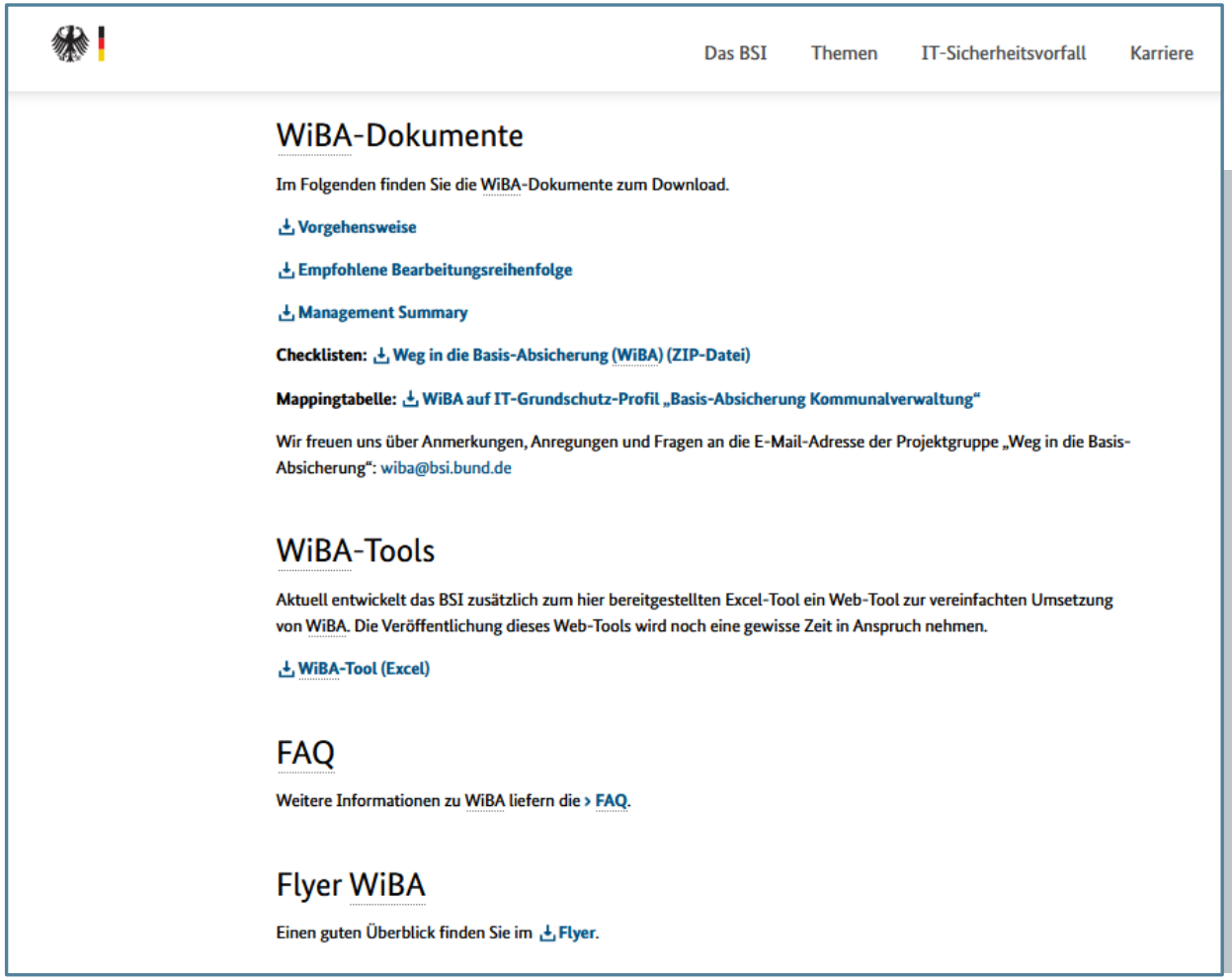
- Clusterung der **67** relevanten Bausteine in **19** themenspezifischen Checklisten
  - Festlegung eines möglichst praxisnahen Sicherheitsniveaus für den Einstieg (Reduktion auf wesentliche Anforderungen/Maßnahmen)
  - Bereitstellung von Hilfsmitteln / weitergehenden Informationen zur Unterstützung
  - Formulierung von konkreten Fragen
  - Verschmelzung von verschiedenen Bausteinanforderungen zu (thematisch sortierten) Prüffragen
  - Aufwandsschätzung (Kategorie 1 bis 4) zur Erleichterung der Priorisierung der Maßnahmen

Praxis-Test der Checklisten

- Einbindung der Arbeitsgruppe kommunale Basis-Absicherung (AG koBA) – federführend für das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“
- Einbindung von 6 Modellkommunen
  - Bewerbungs- und Auswahlverfahren über/mit Kommunalen Spitzenverbänden (DLT, DST, DStGB): über 130 Bewerbungen aus dem Bundesgebiet
  - zwei sehr kleine Kommunen, zwei mittelgroße Kommunen, eine große Stadt, ein Landkreis
  - jeweils mehrtägige Workshops
- Community Draft-Phase

Aus was besteht WiBA?

- Vorgehensweise
- Empfohlene Bearbeitungsreihenfolge
- Management Summary
- Checklisten
- Mappingtabelle
- Excel-“Tool“
- FAQ
- Flyer



Checklisten / Bearbeitungsreihenfolge

Prio 1

Backup
IT Administration
Organisation und Personal
Rollen / Berechtigungen / Authentisierung
Vorbereitung für Sicherheitsvorfälle

Prio 2

Bürosoftware
Client
Netze
Serversysteme
Serverraum und Datenträgerarchiv
Sicherheitsmechanismen
Webserver und Webanwendungen

Prio 3

Arbeit außerhalb der Institution
Arbeit innerhalb der Institution / Haustechnik
Mobile Endgeräte
Outsourcing und Cloud
Umgang mit Informationen

Prio 4

Drucker und Multifunktionsgeräte
Telefonie und Fax

Blick in die Checkliste „Backup“

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Stand: März 2024

Checkliste: Backup

Zugrundeliegende Bausteine (IT-Grundschutz-Kompendium 2023):

- CON.3 Datensicherungskonzept

Bearbeitungsinformationen

Hier bitte das/die betrachtete(n) Zielobjekt(e) einfügen.	
Anzahl Checkfragen: 7	**Davon umgesetzt:**
Checkliste bearbeitet am:	**Checkliste bearbeitet von (zuständige Stelle/Rolle):**

Backup

Ziel

Ein Backup (dt. Datensicherung) soll gewährleisten, dass durch einen redundanten Datenbestand der Betrieb der Informationstechnik kurzfristig wiederaufgenommen werden kann, wenn Teile des aktiv genutzten Datenbestandes verloren gehen. Daten sind die Grundlagen für sämtliche Geschäftsprozesse von Institutionen. Gehen diese verloren, z. B. durch defekte Hardware, Schadprogramme (Ransomware) oder versehentliches Löschen, können gravierende Schäden entstehen. Dies kann klassische IT-Systeme wie Server oder Clients betreffen. Aber auch Router, Switches oder IoT-Geräte können schützenswerte Informationen wie Konfigurationen speichern. Durch regelmäßige Datensicherung lassen sich Auswirkungen von Datenverlusten minimieren.

Daher soll in dieser Checkliste aufgezeigt werden, wie Institutionen relevante Daten identifizieren und sichere Backups erstellen und testen können.

Allgemeiner Hinweis

Ziel dieser Checkliste ist es, Kommunen bei einer ersten Bestandsaufnahme der Informationssicherheit zu unterstützen und den Einstieg in den IT-Grundschutz des BSI zu erleichtern.

Bei den hier aufgeführten Prüffragen handelt es sich um die wesentlichen Aspekte, die bei der Absicherung vorrangig betrachtet werden müssen. Dabei handelt es sich um einen Teilbereich des IT-Grundschutzes, der als Grundlage für den Aufbau einer Basis-Absicherung dienen kann. Die Prüffragen orientieren sich am IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ und ermöglichen mit wenig Aufwand einen ersten wichtigen Schritt in die Informationssicherheit. Dennoch handelt es sich nicht um ein vollumfängliches Managementsystem für Informationssicherheit (ISMS). Dies muss in einem Folgeschritt realisiert werden.

Um ein Mindestmaß an Dokumentation zu gewährleisten, sollte im Feld „Notizen“ der Sachstand zu den jeweiligen Prüffragen kurz dokumentiert sein.

Weiterführende Informationen

Grundsätzliche Informationen finden Sie im Backup-Leitfade der Sicherheitsberatung für Länder und Kommunen.

Deutschland Digital•Sicher•BSI•

Blick in die Checkliste „Backup“

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt		
			Ja	Nein	Nicht relevant
1	Ist festgelegt, welche Daten gesichert werden?	2			
	Bei der Festlegung sollten insbesondere folgende Fragestellungen berücksichtigt werden: • *Für welche IT-Systeme (u. a. auch mobile Endgeräte) und für welche Anwendungen (u. a. auch Fachverfahren) müssen Daten gesichert werden?* • *Welche Daten (Nutzdaten, Konfigurationsdateien, kryptografische Schlüssel, ...) müssen gesichert werden?* • *Werden nur lokal vorhandene Daten auf Client-IT-Systemen bei der Datensicherung berücksichtigt?* • *Welche Anforderungen und welche Gefährdungslage bestehen bezüglich Verfügbarkeit, Vertraulichkeit und Integrität der Daten?* • *Gibt es rechtliche Anforderungen, die zu beachten sind?*				
	Notizen				

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt		
			Ja	Nein	Nicht relevant
2	Ist festgelegt, in welchen zeitlichen Abständen die Daten gesichert werden?	2			
	Wie regelmäßig (wie oft und zu welchem Zeitpunkt) muss gesichert werden? Hierbei sollten grundsätzlich andere Prozesse berücksichtigt werden (z. B. Backup vor und nach großen Änderungen, Snapshot vor kleineren Konfigurationsänderungen).				
	Notizen				

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt		
			Ja	Nein	Nicht relevant
3	Ist festgelegt, auf welchem Speichermedium die Daten gespeichert werden?	2			
	Hierfür muss insbesondere die Art der Speichermedien den eigenen Anforderungen entsprechend festgelegt werden (z. B. Langlebigkeit, Wiederherstellbarkeit der Medien, Wie viel Platz benötigen die Sicherungen?). *Für Datensicherung sollten ausschließlich dedizierte Speichermedien verwendet werden.*				
	Notizen				

Der beste Zeitpunkt ist jetzt.

Die Bedrohungslage ist besorgniserregend.
Cyber-Angriffe sind keine höhere Gewalt!

Es gibt keine 100 % Sicherheit – aber Sie können aktiv handeln.

Methoden zur Absicherung stehen zur Verfügung.

Wir haben eine praxisnahe Einstiegsstufe in die Informationssicherheit entwickelt, um Sie bedarfsgerecht zu unterstützen!

Noch Fragen?

wiba@bsi.bund.de

Stefanie Euler
BSI Referat I 12 - Umsetzungsberatung für Länder und Kommunen

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

www.bsi.bund.de/dok/wiba

Bundesamt
für Sicherheit in der
Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

Cybersicherheitsvorgaben für die Bundesverwaltung

Julia Hein, BMI

Struktur

1. Aktuelle Vorgaben
2. Zukünftige Vorgaben
3. Modernisierungsauftrag IT-GS

1. Aktuelle Vorgaben

Aktuell ergeben sich die Vorgaben für die BV aus dem BSIG und dem UP Bund

BSIG

u.a.:

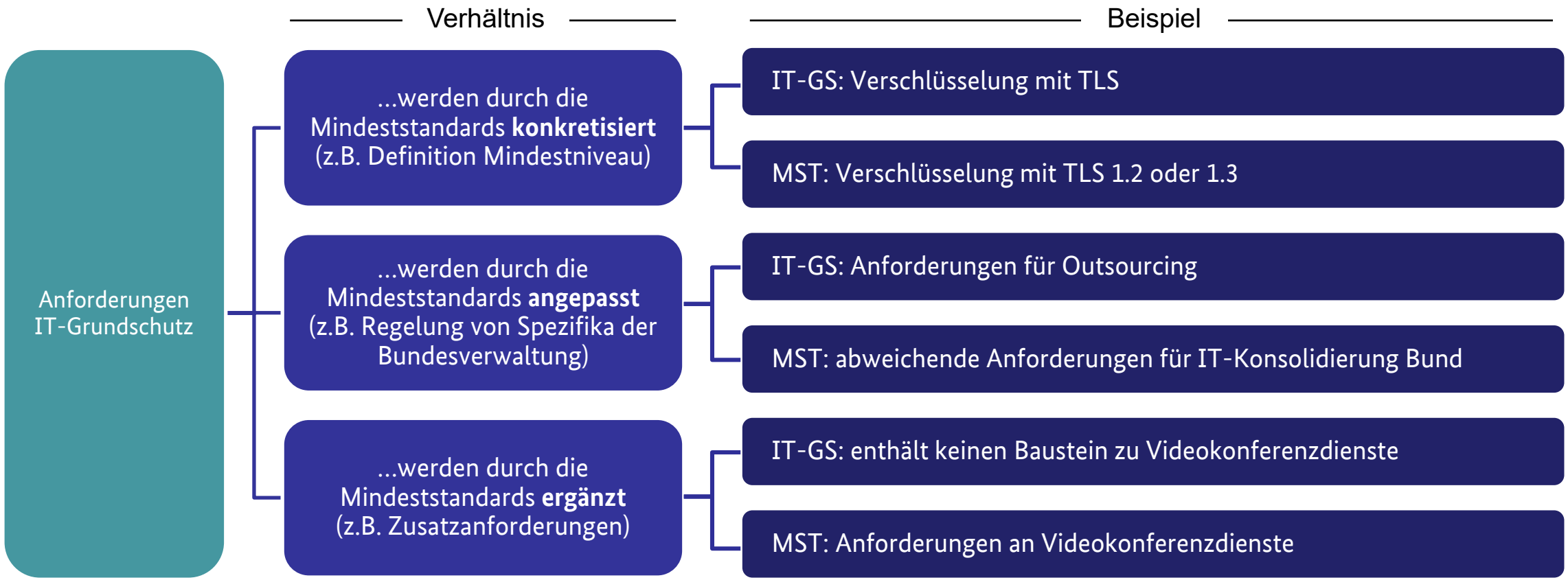
- Meldepflichten nach § 4
- Unterstützung des BSI bei Kontrollen nach § 4a
- **Umsetzung Mindeststandards nach § 8**
- Vertragliche Verpflichtung zur Informationssicherheit bei Beauftragung anderer Stellen nach § 8
- Beteiligung BSI bei wesentlichen Digitalisierungsvorhaben nach § 8

UP Bund

u.a.:

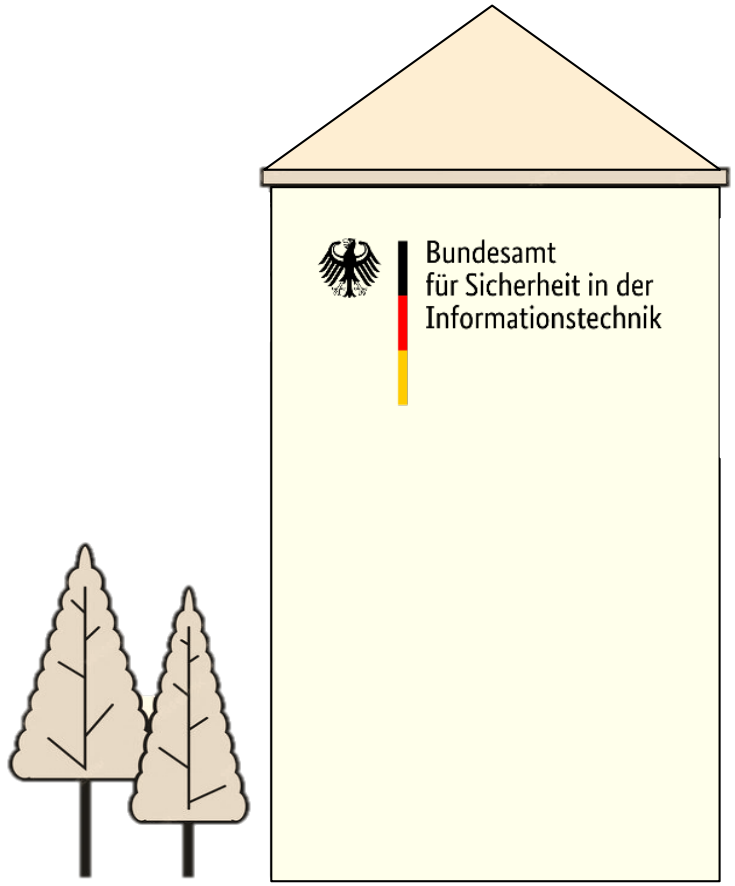
- **Verpflichtung zur Einhaltung des IT-Grundschutzes**
- Gesamtverantwortung der Einrichtungsleitung
- Rolle der Informationssicherheitsbeauftragten

Die Mindeststandards konkretisieren, ergänzen oder passen die Anforderungen des IT-GS an



2. Zukünftige Vorgaben

Das BSI erhält diverse neue Pflichten und Befugnisse



Auszug

Aufgaben nach §§ 3 und 44

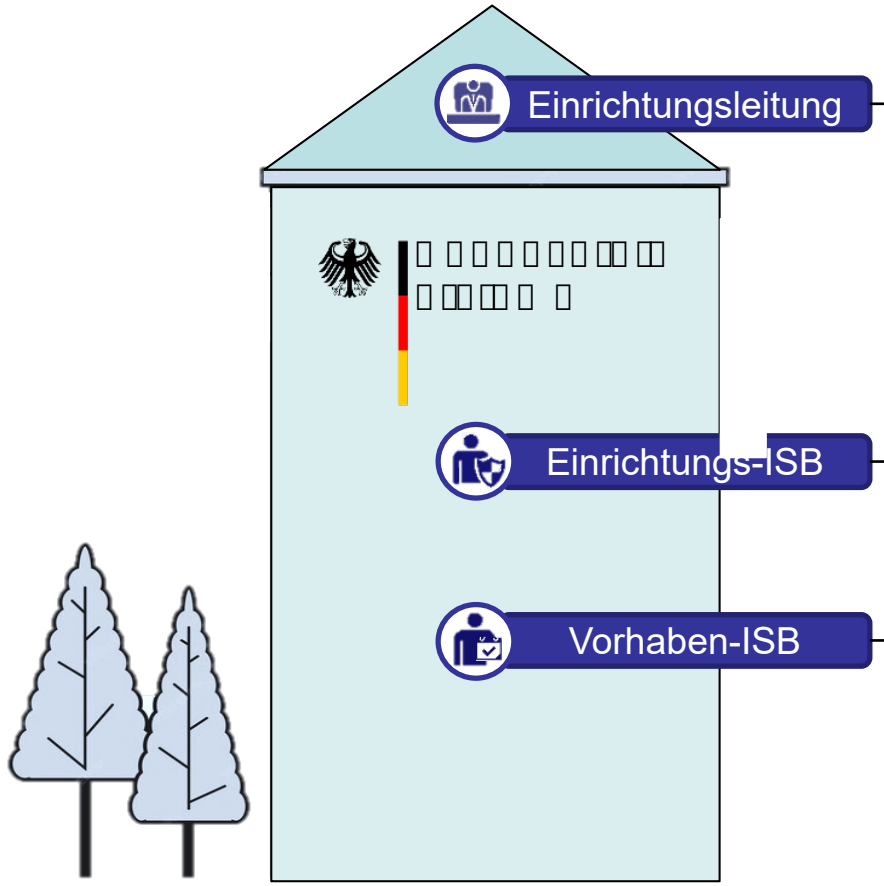
- **Festlegung der Mindeststands** (gesetzlich verpflichtend für alle Einrichtungen des Bundes) und des **IT-Grundschutz** (gesetzlich verpflichtend für Bundesministerien + BKAmt).
- Regelmäßige **Evaluierung und Fortschreibung** des IT-Grundschutz und der Mindeststandards entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis
- **Beratung** der Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung dieser Anforderungen, Bereitstellung **konkreter, praxisnaher Hilfsmittel** und **Unterstützung der Bereitstellung entsprechender Lösungen durch die IT-Dienstleister** des Bundes über den gesamten Lebenszyklus.

Auszug

Anordnungen nach §§ 7 und 10

- **Anweisung** von Einrichtungen des Bundes zur **Umsetzung der Vorschläge zur Verbesserung** nach Prüfungen innerhalb einer angemessenen Frist im Benehmen mit dem/der Ressort-ISB.
- Im Einzelfall **Anordnung erforderlicher Maßnahmen zur Abwendung/ Behebung eines gegenwärtigen Sicherheitsvorfalls** gegenüber Einrichtungen des Bundes; Aufforderung zur **Berichterstattung** innerhalb einer angemessenen Frist.

Die Einrichtungen der Bundesverwaltung erhalten ebenfalls diverse „neue“ Pflichten



Auszug

Einrichtungsleitung

- Trägt die **Gesamtverantwortung** für die Informationssicherheit der Einrichtung — § 43 (1)
- Nimmt regelmäßig an **Schulungen** teil — § 43 (2)
- Nimmt die **Registrierung** der Einrichtung beim BSI vor — § 43 (4)

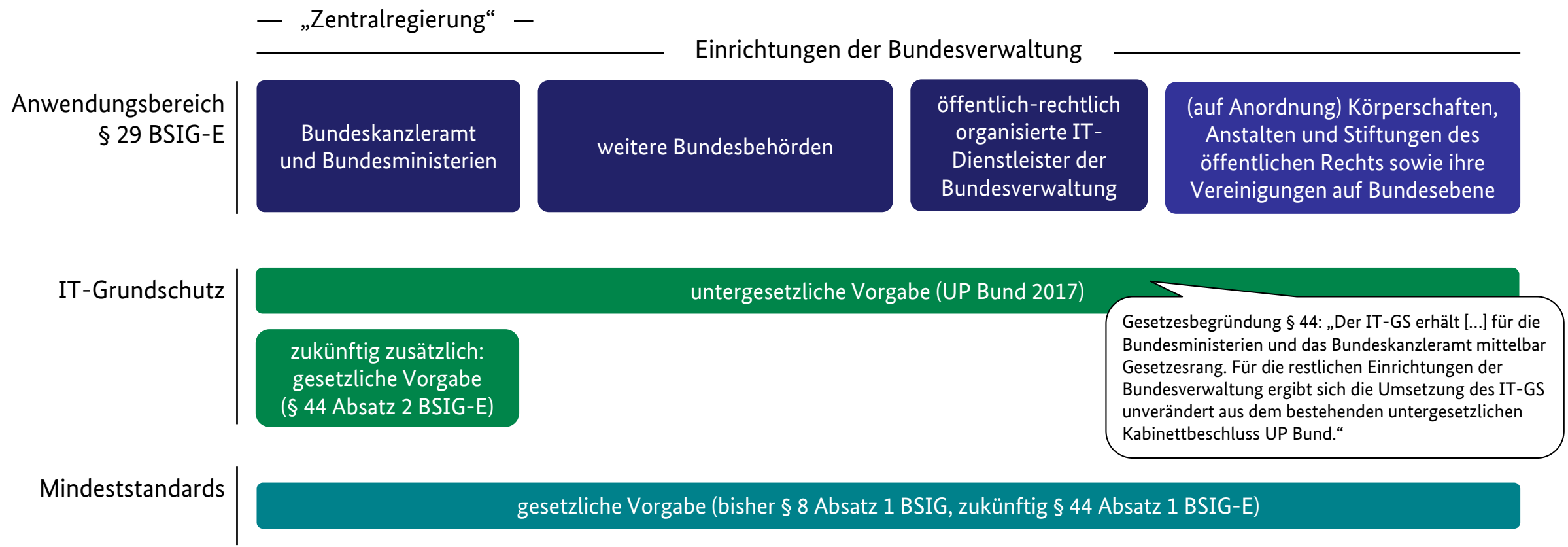
Einrichtungs-ISB

- **Berät und unterrichtet die Einrichtungsleitung** zum Stand der Informationssicherheit in der Einrichtung, zur Mittelausstattung und zu Sicherheitsvorfällen — § 45 (3)
- Steuert das **Informationssicherheitsmanagement** der Einrichtung und wirkt hierzu insb. auf die **Umsetzung von [IT-Grundschutz und] Mindeststandards** hin, kontrolliert diese und dokumentiert sie in einem **Sicherheitskonzept** — § 44 (1, 2), § 45 (3)
- **Weist** dem BSI die Umsetzung regelmäßig **nach** — § 43 (4)
- **Meldet Sicherheitsvorfälle** an das BSI — § 32, 43 (5)
- Unterstützt das BSI bei **Kontrollen seiner IT** und **berichtet auf Anweisung zur Umsetzung** der Verbesserungsvorschläge — § 7
- Verpflichtet **externe Dienstleister** zur Einhaltung der Vorgaben — § 43 (3)
- Befolgt Anweisungen des BSI zu Sicherheitsvorfällen — § 10

Vorhaben-ISB

- Stellt die **Informationssicherheit** bei wesentlichen **Digitalisierungsvorhaben** sicher (einschl. Kontrolle der Umsetzung von IT-Grundschutz und Mindeststandards in einem Sicherheitskonzept) — § 47 (1)
- Bezieht das BSI frühzeitig mit ein — § 47 (2)

Der IT-GS gilt untergesetzlich weiterhin für die gesamte Bundesverwaltung



3. Modernisierungsauftrag IT-GS

Die Herausforderungen zur Umsetzung des IT-GS wurde über eine Umfrage identifiziert

Projekt zur Neu-Positionierung des IT-GS in der Bundesverwaltung 2022:

Herausforderungen

u.a.:

- fehlendes Personal,
- Komplexität der Vorgabenstruktur (IT-GS, MST, VS)
- fehlende technische Unterstützung, wie bspw. ISMS-Tools
- aufwendige Dokumentationspflichten

Projektergebnisse

u.a.:

- Werkzeugkasten mit Arbeitshilfen
- Erstellung von IT-Grundschutz-Profilen
- ISB-Netzwerk

Das BSI muss den IT-GS bis 1.1.2026 modernisieren

§ 44 Absatz 2 Satz 4 NIS2UmsuCG

„Das Bundesamt wird den IT-Grundschutz bis zum **1. Januar 2026 modernisieren und fortentwickeln**.“

Gesetzesbegründung § 44 Absatz 2

„Um die Nachweisfrist von fünf Jahren ab Inkrafttreten (§ 43 Absatz 4 Satz 2) bei weiterhin knappen finanziellen und personellen Ressourcen umsetzen zu können, muss sichergestellt werden, dass der IT-Grundschutz so **effizient und unbürokratisch** wie möglich ausgestaltet ist. Das Bundesamt wird den IT-Grundschutz daher modernisieren, mit der Maßgabe, den **Umfang** und die bei der Umsetzung entstehenden **Dokumentationspflichten** auf das **notwendige Mindestmaß zu reduzieren**, eine **Priorisierung** der Anforderungen vorzunehmen und die **Anwendung von Automatisierungstools** weitestgehend zu **ermöglichen**.“

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Referat CI4
CI4@bmi.bund.de

Bundesministerium des Innern, für Bau und Heimat

Bundesamt
für Sicherheit in der
Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

Vision zur Weiterentwicklung des IT-Grundschutzes

Dr. Dennis Kügler, BSI

Papier verhindert keine Cyberangriffe

- Alles regeln?
- Alles dokumentieren?
- Wieviel Sicherheit schafft Papier?

- Weniger ist mehr!
  - Anforderungen reduzieren
  - Dokumentationsanforderungen minimieren
- Systematik erhöhen

Qualifiziertes Personal ist knapp

- Viel mehr Organisationen müssen cybersicher werden
  - Jede Organisation benötigt qualifiziertes Personal
  - Insgesamt: (zu) viele Personen!
  - Daher: Fachexpertise zentralisieren!

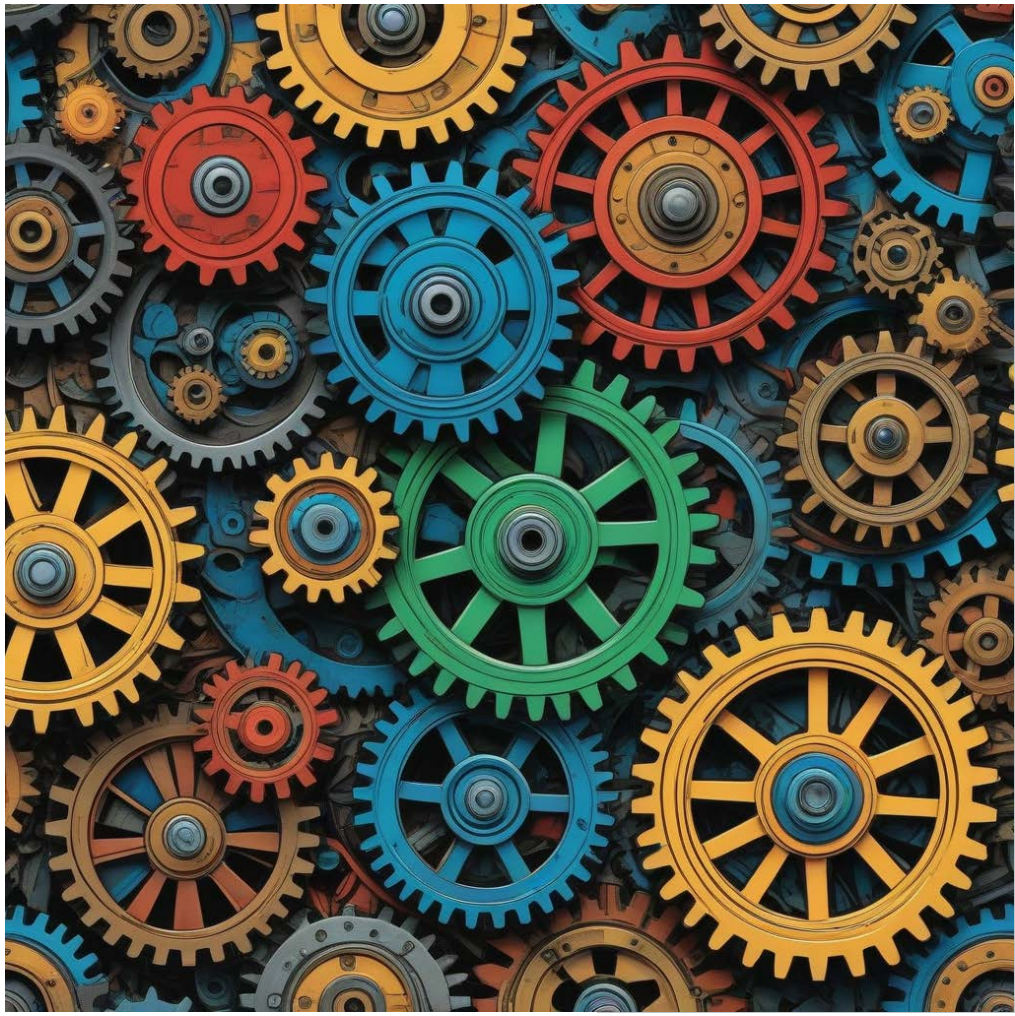
- **Der IT-Grundschutz des BSI soll unterstützen**
  - Kompendium als „Best Practice“ Regelwerk
  - Stand der Technik für die Umsetzung ermitteln
  - Automatisierung von Sicherheitsprozessen ermöglichen
  - Zertifizierung & Kennzeichnung geeigneter Produkte

Zunehmende Komplexität

- Anforderungen steigen mit Komplexität der IT-Infrastruktur
- Umsetzung/Aufrechterhaltung wird viel aufwändiger
- Nicht alles ist automatisierbar, z.B. bei Schwachstellen

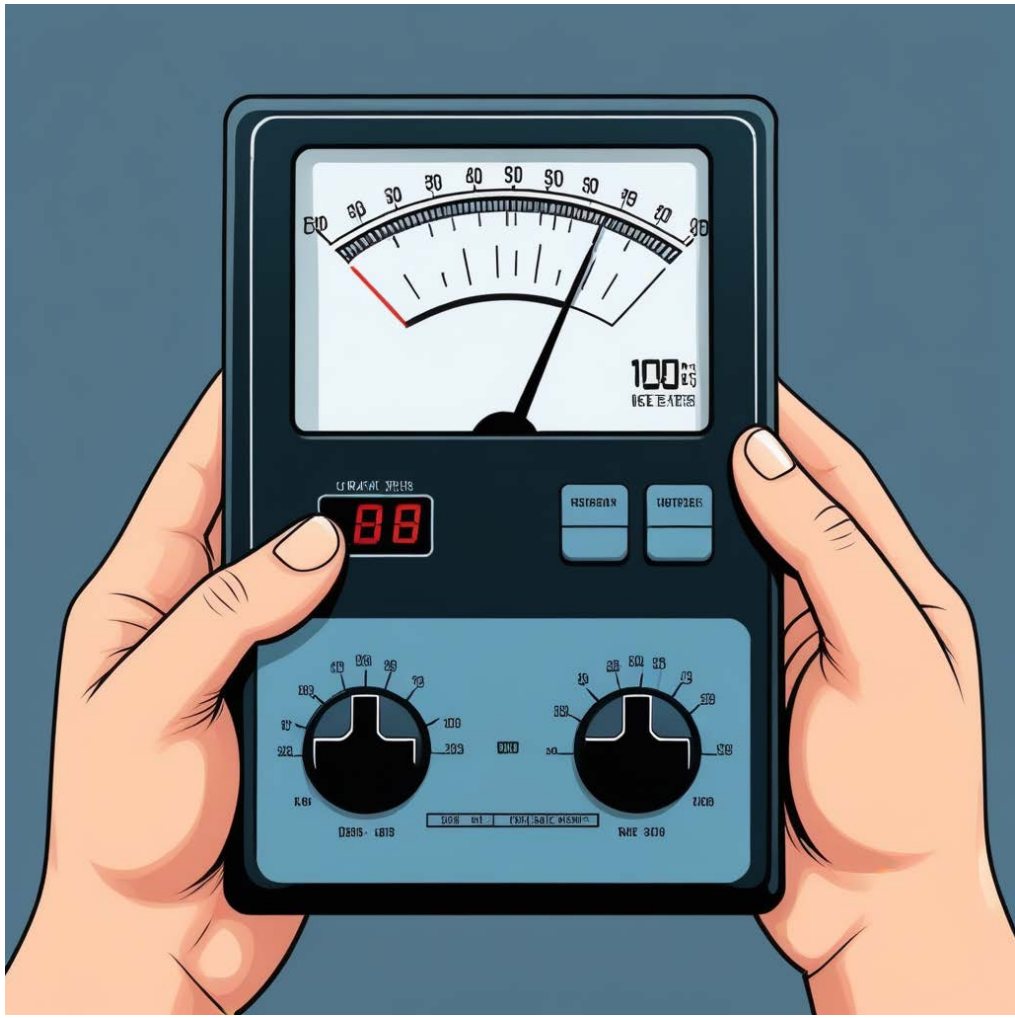
Kosten und Nutzen abwägen

- Welche Anforderungen sind (jetzt) wirklich wichtig?
- Nicht alles „MUSS“ umgesetzt werden.



Cybersicherheit messbar machen

- Priorität und Wertigkeit von Anforderungen festlegen
  - **Priorität**: Aufwand für Umsetzung
  - **Wertigkeit**: Risiko bei nicht-Umsetzung
- Bezogen auf Sicherheitsziele
  - Vertraulichkeit
  - Integrität/Authentizität
  - Verfügbarkeit



Wann ist sicher sicher genug?

- **Bisher:** Sicherheitsklassen
  - Basis, Standard, erhöhter Schutzbedarf
  - Alle Basisanforderungen MÜSSEN umgesetzt werden

- **Zukünftig:** Leistungszahlen für Cybersicherheit
  - Messwerte der umgesetzten Anforderungen

- Kontinuierlicher Verbesserungsprozess
  - Plan, Do, Check, Act
  - Leistungszahlen stetig erhöhen

One Size Fits All?

- IT-Grundschutz Regelwerk für Cybersicherheit
  - „Best Practice“
  - Meist **SOLLTE**-Anforderungen
- **Anpassung durch Anwendergruppen**
  - Verbindlichkeit von Anforderungen ändern
    - KANN <- **SOLLTE** -> MUSS
  - Anforderungen ergänzen / streichen
  - Festlegung von Mindest-Leistungszahlen
  - Festlegung einer bestimmten Umsetzungsweise
- Für den Anwender Bund: **Mindeststandards**

IT-Grundschutz ist zu kompliziert?

Checklisten als Ergänzung

- Verständliche Fragen statt strukturierter Anforderungen
- Reduziert auf das wirklich Wesentliche
- Automatisierte Erzeugung Profil -> Checklisten
- Konformitätserklärung als Selbstbewertung

Zielgruppen

- Große Organisationen: Einstieg in den IT-Grundschutz
- Kleine Organisationen: Alternative zu einem ISMS
- Andere Anwender

Agenda

13:00 Uhr: Begrüßung und Keynote (Sandro Amendola)
13:15 Uhr: IT-Grundschutz gestern und heute (Holger Schildt)
13:35 Uhr: Weg in die Basis-Absicherung (WiBA) (Stefanie Euler)
13:55 Uhr: Cybersicherheitsvorgaben für die Bundesverwaltung (Julia Hein)
14:15 Uhr: Vision zur Weiterentwicklung des IT-Grundschutzes (Dennis Kügler)
14:30 Uhr: 15 Minuten Pause
14:45 Uhr: Struktur der zukünftige Anforderungen (Florian Göhler)
15:05 Uhr: Struktur des IT-Grundschutz-Kompendium (Christoph Weißenborn)
15:25 Uhr: Und was ist mit Dokumentation? (Daniel Gilles)
15:45 Uhr: Kennziffern zur Effizienzmessung (Stefan Schuck)
16:05 Uhr: Pause
16:15 Uhr: Fragen und Diskussion mit allen Vortragenden
17:00 Uhr: Ende

Bundesamt
für Sicherheit in der
Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

Struktur der zukünftigen Anforderungen

Florian Göhler, BSI

IT-Grundschutz-Kompendium 2023

SYS.2.2: Windows-Clients

SYS.2.2.3: Clients unter Windows 10

1 Beschreibung

1.1 Einleitung

Mit Windows 10 hat Microsoft sein Client-Betriebssystem Windows an eine neue Unternehmensstrategie angepasst. Verändert hat sich insbesondere auch die Designphilosophie, weg vom bisherigen Prinzip des „lokalen Betriebssystems" hin zu einer Dienstleistung („Windows as a Service"). Das bedeutet, dass das Betriebssystem neben den bisherigen Funktionen auch darüber hinausgehende, insbesondere cloudbasierte, Anwendungen enthält und deswegen auf eine enge Anbindung an die Server-Infrastruktur des Herstellers angewiesen ist. Wichtige neue Aspekte im Vergleich zu den bisherigen Windows-Versionen sind vor allem der tief verankerte und teilweise nicht beeinflussbare Datenaustausch zwischen den Clients und der Herstellerinfrastruktur sowie die zunehmende Auslagerung von sicherheitskritischen Kernbestandteilen einer Windows-Infrastruktur (z. B. Authentisierung) in die Cloud. Diese Neuerungen sollten vor dem Einsatz von Windows 10 unbedingt berücksichtigt werden.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die durch und auf Windows 10-Clients verarbeitet werden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.2.2.2 *Clients unter Windows 10* ist für alle Client-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows 10 eingesetzt wird.

Dieser Baustein enthält spezifische Anforderungen, die zum sicheren Betrieb von Clients unter dem Betriebssystem Windows 10 zusätzlich zu den Anforderungen aus dem Baustein SYS.2.1 *Allgemeiner Client* zu beachten und zu erfüllen sind. Für Anwendungsprogramme, die auf den Windows-Clients verwendet werden, sind die Anforderungen der entsprechenden Bausteine zu erfüllen, beispielsweise APP.1.1 *Office-Produkte* oder APP.1.2 *Web-Browser*. Beim Einsatz in einer Windows-Domäne sind die

Prosa

Von „sicher" bis Maßnahme

IT-Grundschutz-Kompendium 2023

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.1 *Allgemeiner Server* ist auf alle Server-IT-Systeme mit beliebigem Betriebssystem anzuwenden.

In der Regel werden Server unter Betriebssystemen betrieben, bei denen jeweils spezifische Sicherheitsanforderungen zu berücksichtigen sind. Für verbreitete Server-Betriebssysteme sind im IT-Grundschutz-Kompendium eigene Bausteine vorhanden, die auf dem vorliegenden Baustein aufbauen. Der Baustein SYS.1.1 *Allgemeiner Server* bildet die Grundlage für die Bausteine der konkreten Server-Betriebssysteme. Sofern für ein betrachtetes IT-System ein konkreter Baustein existiert, ist dieser zusätzlich zum Baustein SYS.1.1 *Allgemeiner Server* anzuwenden. Falls für eingesetzte Server-Betriebssysteme kein spezifischer Baustein existiert, müssen die Anforderungen des vorliegenden Bausteins geeignet für das Zielobjekt konkretisiert und es muss eine ergänzende Risikobetrachtung durchgeführt werden.

Die jeweils spezifischen Dienste, die vom Server angeboten werden, sind nicht Bestandteil dieses Bausteins. Für diese Serverdienste müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Die Bereitstellung von Benutzendensitzungen durch Terminalserver ist ebenfalls als Dienst zu betrachten. Für Terminalserver ist entsprechend der Baustein SYS.1.9 *Terminalserver* zu modellieren.

Grundsätzlich sind die Anforderungen an das Rollen- und Berechtigungskonzept aus dem Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* zu berücksichtigen. Ebenfalls zu berücksichtigen sind Anforderungen aus dem Baustein DER.4 *Notfallmanagement*.

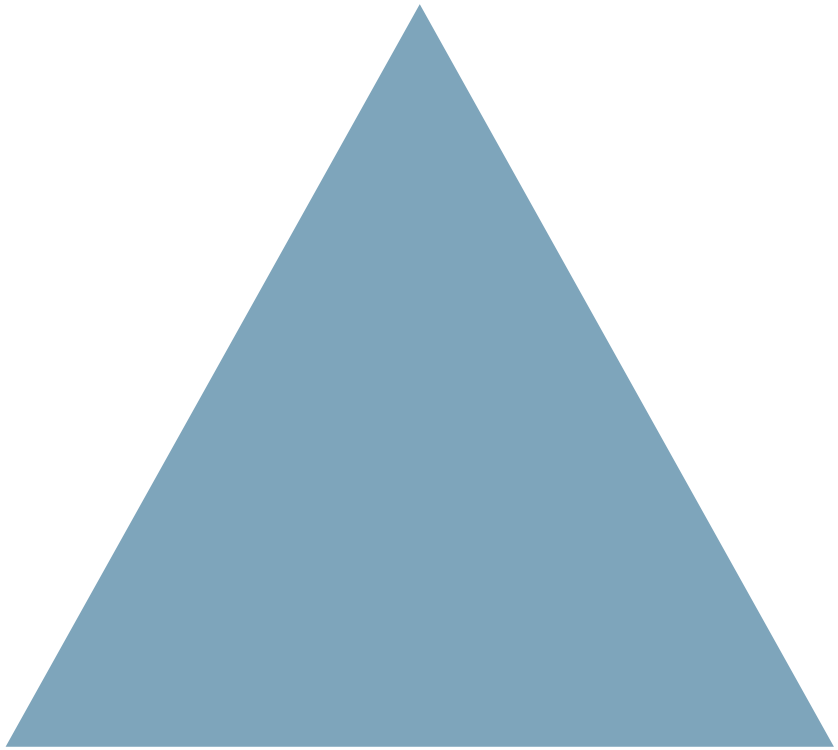
Prosa

Von „sicher“ bis Maßnahme

Manuelle Abhängigkeiten

Viele Redundanzen

Abstraktionsebenen



Businessanforderungen

„Die IT muss sicher sein“

Lösungsneutrale Anforderungen

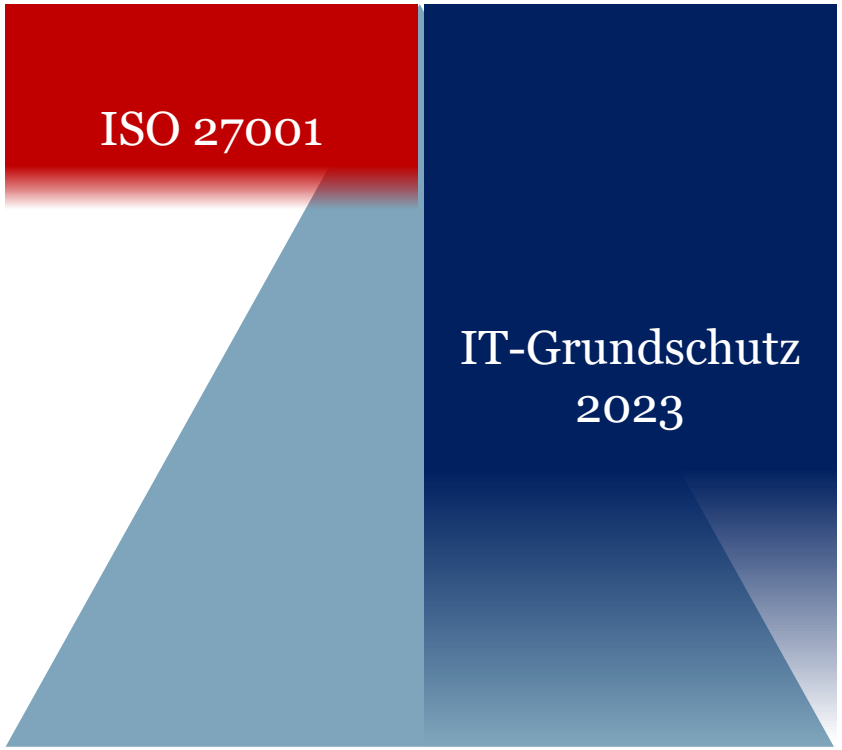
„Die Anwendung muss eine Transportverschlüsselung verwenden“

Technische Anforderungen

„Die Verschlüsselung muss AES256 im CBC-Modus verwenden“

„So abstrakt wie möglich, so genau wie nötig“

Abstraktionsebenen



Businessanforderungen

„Die IT muss sicher sein“

Lösungsneutrale Anforderungen

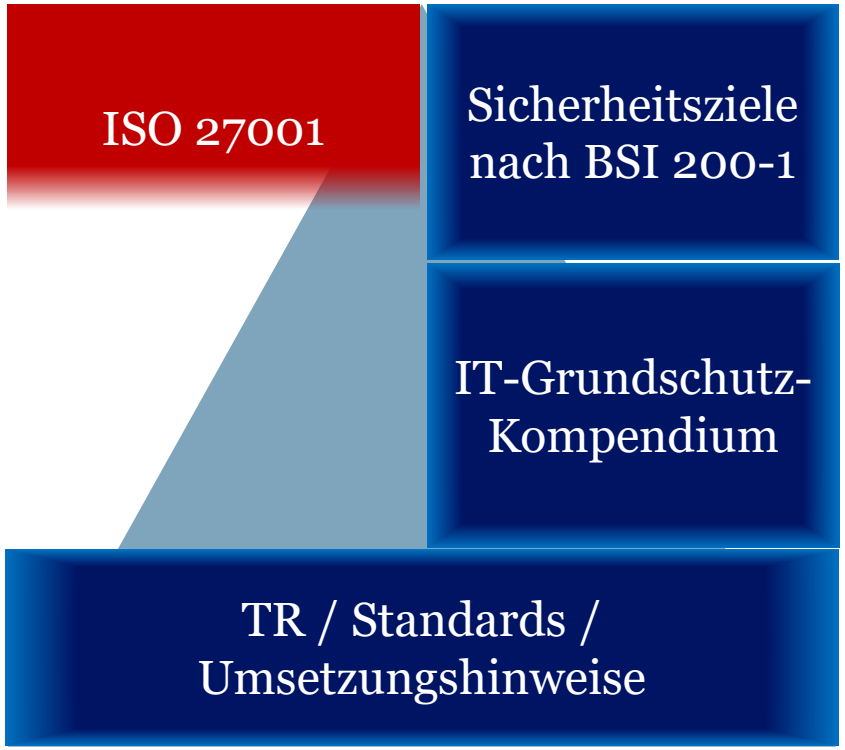
„Die Anwendung muss eine Transportverschlüsselung verwenden“

Technische Anforderungen

„Die Verschlüsselung muss AES256 im CBC-Modus verwenden“

„So abstrakt wie möglich, so genau wie nötig“

Abstraktionsebenen



Businessanforderungen

„Die IT muss sicher sein“

Lösungsneutrale Anforderungen

„Die Anwendung muss eine Transportverschlüsselung verwenden“

Technische Anforderungen

„Die Verschlüsselung muss AES256 im CBC-Modus verwenden“

„So abstrakt wie möglich, so genau wie nötig“

Struktur für Anforderungen durch Satzschablonen

{Subjekt} {Prädikat} <Objekt>

Struktur für Anforderungen durch Satzschablonen

{Praktik} [für {Zielobjekt}] {MODALVERB} <Ergebnis> {Handlungswort}

Praktiken: {Konfiguration, Sensibilisierung, Detektion, Monitoring…}

Zielobjekte: {Windows-Server, VK-Server, Mitarbeitende…}

Modalverb: {SOLLTE, KANN}

Ergebnis: <Zielzustand>

Handlungswort: {anweisen, verbieten, installieren, deaktivieren, …}

Struktur für Anforderungen durch Satzschablonen

{Praktik} [für {Zielobjekt}] {MODALVERB} <Ergebnis> {Handlungswort}

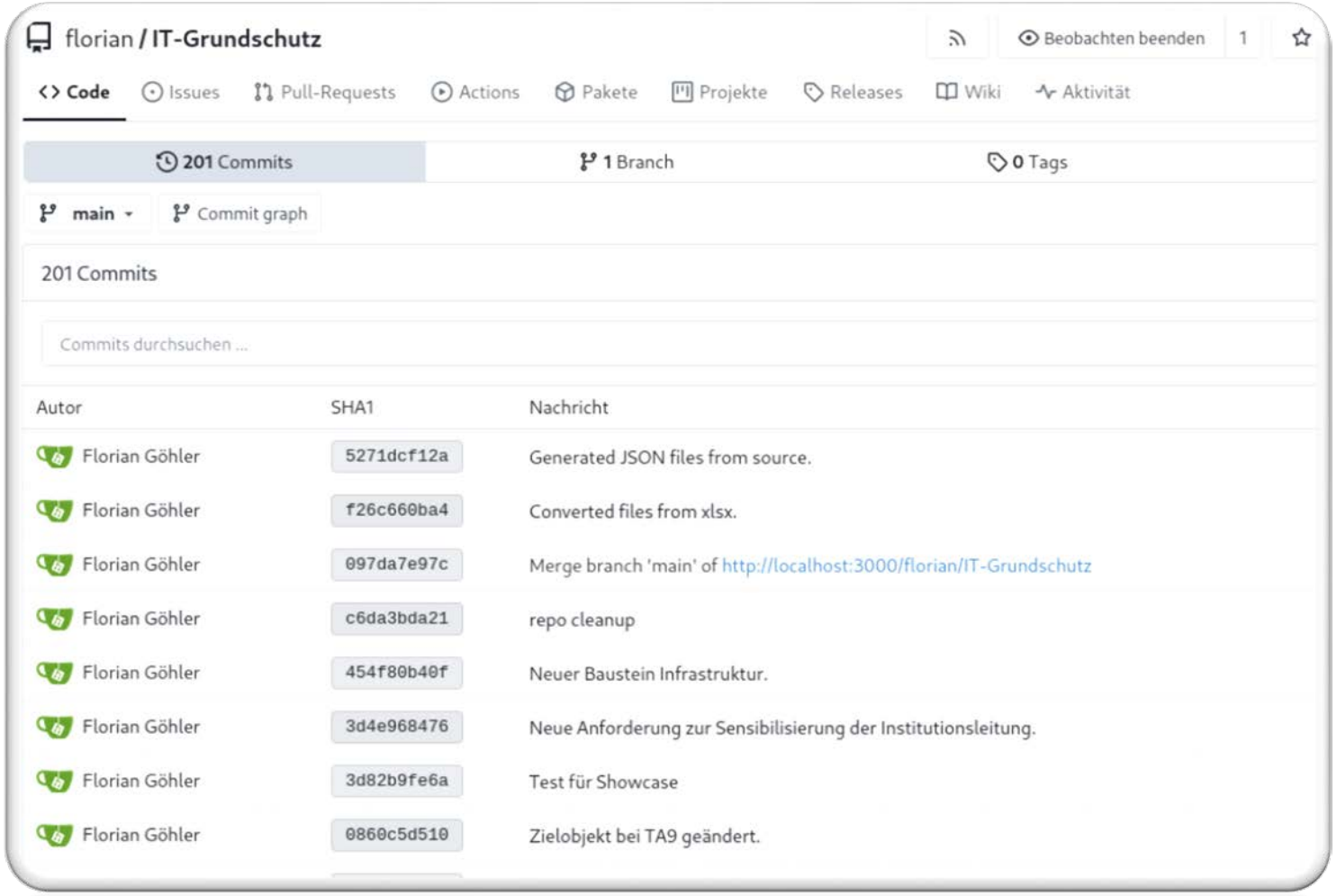
Beispiele:

- Die Praktik „Konfiguration“ für IT-Systeme SOLLTE die Änderung von Default-Passwörtern vor der ersten Verwendung festlegen.
- Die Praktik „IT-Betrieb“ SOLLTE die Installation von Software-Aktualisierungen (Updates oder Patches) auf das vom Hersteller bereitgestellte Patchlevel überprüfen.
- Die Praktik „Sensibilisierung“ für Benutzende SOLLTE die Weitergabe von personengebundenen Authentisierungsmitteln verbieten.

Struktur durch Metadaten

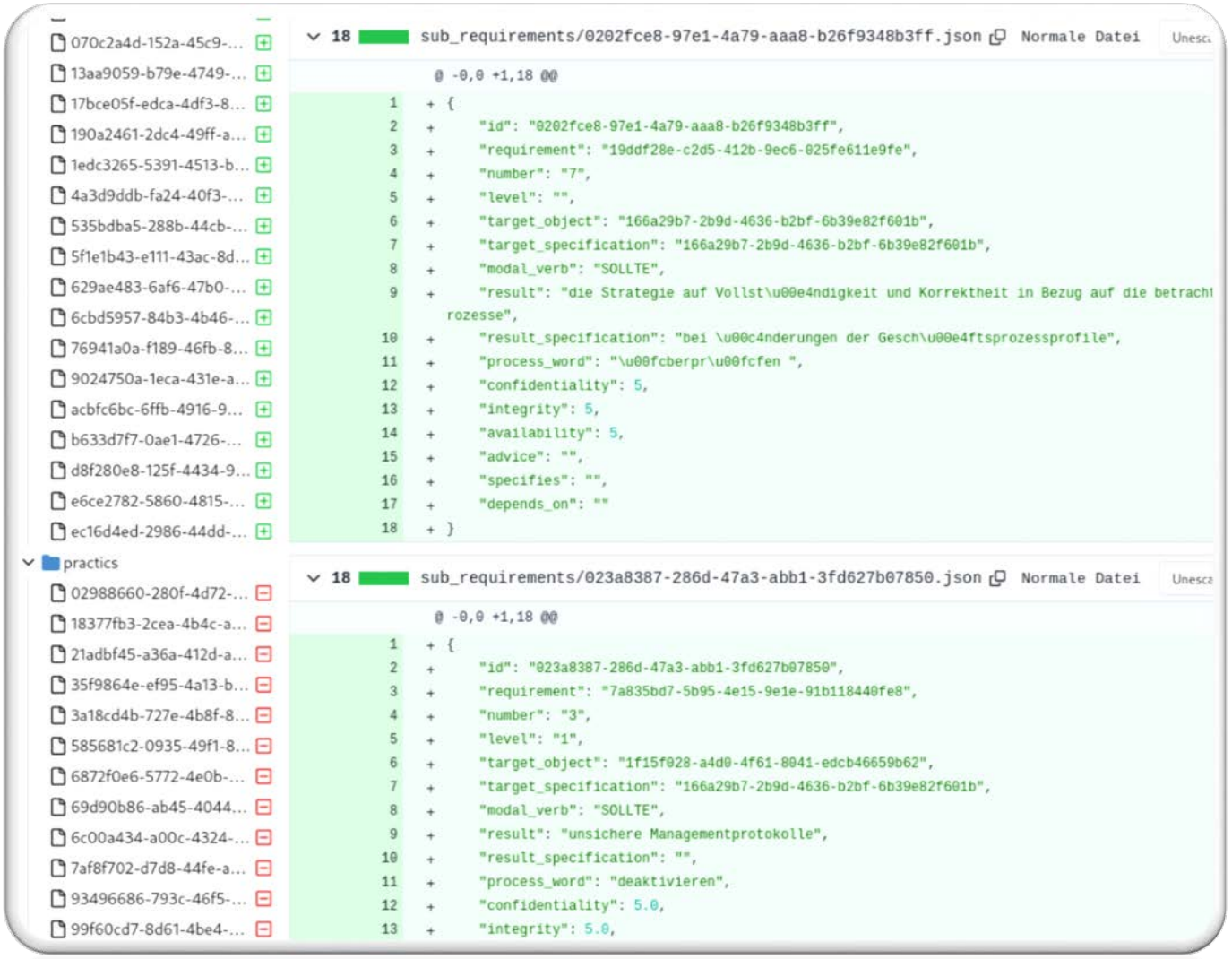
Stufe	Praktik	Zielobjekt	MODALVERB	Ergebnis	Präzisierung Ergebnis	Handlungswort	C	I	A	Hinweis
1	Konfiguration	IT-Systeme	SOLLTE	die Änderung von Default-Passwörtern	vor der ersten Verwendung	festlegen	6	2	0	vgl. ETSI EN 303 645
1	Konfiguration	VK-Server	SOLLTE	Mikrofon und Kamerabild von Clients bei Betreten eines VK-Raumes	per Default	deaktivieren	4	0	0	
1	Sensibilisierung	Benutzende	SOLLTE	die Weitergabe von personengebundenen Authentisierungsmitteln		verbieten	4	2	0	Passworte, Hardware-Token, z. B: für die VPN-Einwahl.

Community


florian / IT-Grundschutz
Beobachten beenden 1
Code
Issues
Pull-Requests
Actions
Pakete
Projekte
Releases
Wiki
Aktivität
201 Commits
1 Branch
0 Tags
main
Commit graph
201 Commits
Commits durchsuchen ...
Autor
SHA1
Nachricht
Florian Göhler 5271dcf12a Generated JSON files from source.
Florian Göhler f26c660ba4 Converted files from xlsx.
Florian Göhler 097da7e97c Merge branch 'main' of http://localhost:3000/florian/IT-Grundschutz
Florian Göhler c6da3bda21 repo cleanup
Florian Göhler 454f80b40f Neuer Baustein Infrastruktur.
Florian Göhler 3d4e968476 Neue Anforderung zur Sensibilisierung der Institutionsleitung.
Florian Göhler 3d82b9fe6a Test für Showcase
Florian Göhler 0860c5d510 Zielobjekt bei TA9 geändert.

von Johann zu JSON

Transparenz



Requirements Engineering - Mehr als nur eine Satzschablone

Fokus Informationssicherheit

Qualitätskriterien für Anforderungen

Vererbung durch Hierarchie von Zielobjekten

Definitionen für
Praktiken, Zielobjekte, Handlungsworte

Agile Veröffentlichung

Bundesamt für Sicherheit in der Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland Digital•Sicher•BSI•

Struktur des IT-Grundschutz-Kompendiums

Christoph Weißenborn, BSI

Agenda

1. Redundanz
2. Praktiken
3. Ansichten
4. Anforderungen

Redundant arbeiten soll die Technik, nicht der Mensch

SYS.3.1.A12 Verlustmeldung für Laptops [Benutzer] (S)

Benutzer SOLLTEN umgehend melden, wenn ein Laptop verloren gegangen ist oder gestohlen wurde. Dafür SOLLTE es in der Institution klare Meldewege geben. Wenn verlorene Laptops wieder auftauchen, SOLLTE untersucht werden, ob sie eventuell manipuliert wurden. Die darauf eingesetzte Software inklusive des Betriebssystems SOLLTE komplett neu installiert werden.

SYS.3.1.A13 Verschlüsselung von Laptops (S)

In Laptops verbaute Datenträger wie Festplatten oder SSDs SOLLTEN verschlüsselt werden.

SYS.3.1.A14 Geeignete Aufbewahrung von Laptops [Benutzer] (S)

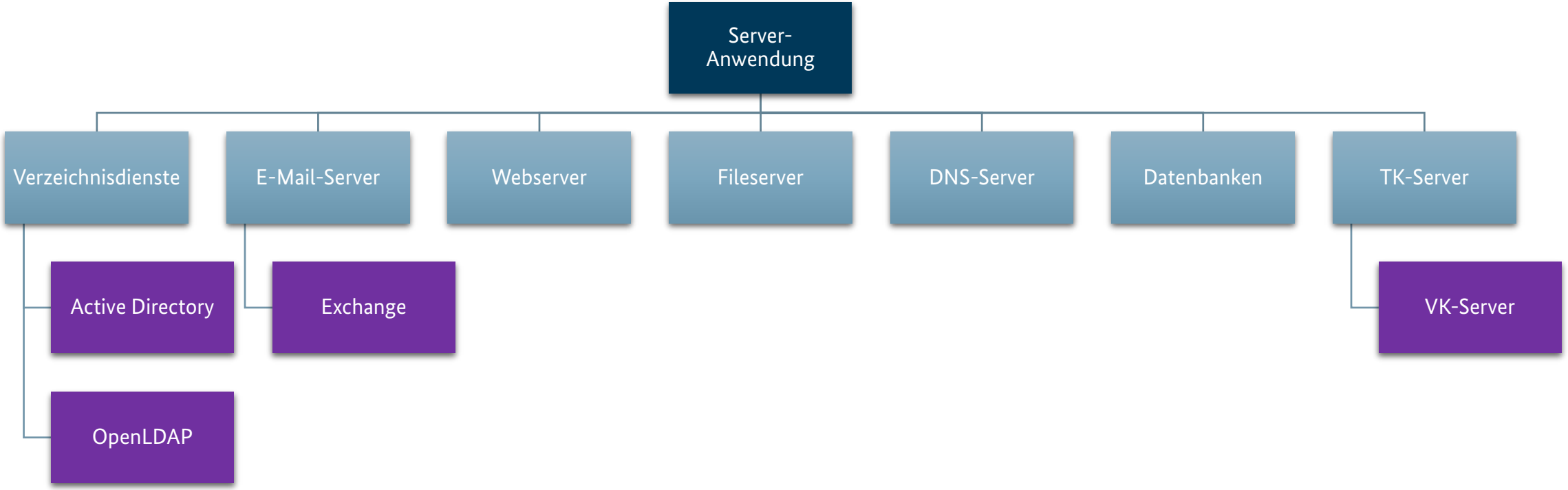
Alle Benutzer SOLLTEN darauf hingewiesen werden, wie Laptops außerhalb der Institution sicher aufzubewahren sind. Abhängig vom Schutzbedarf der darauf gespeicherten Daten SOLLTEN Laptops auch in den Räumen der Institution außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt werden.

SYS.3.1.A15 Geeignete Auswahl von Laptops [Beschaffungsstelle] (S)

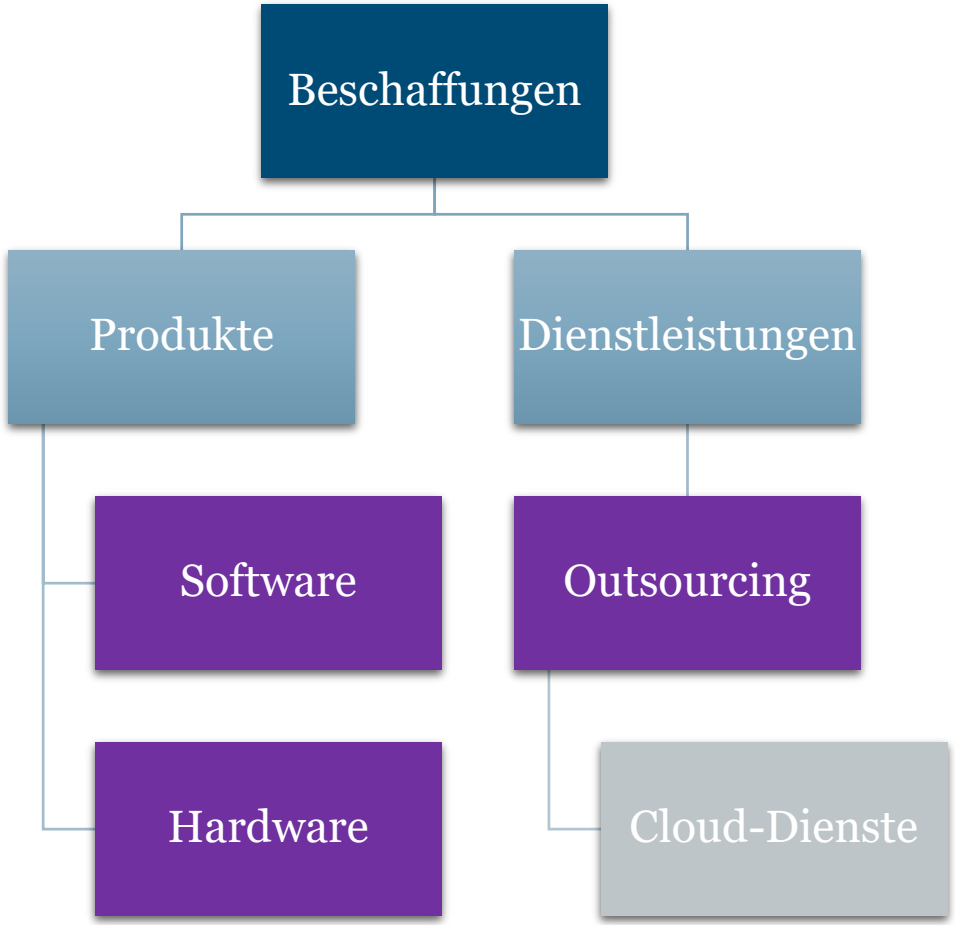
Bevor Laptops beschafft werden, SOLLTEN die Zuständigen eine Anforderungsanalyse durchführen. Anhand der Ergebnisse SOLLTEN alle infrage kommenden Geräte bewertet werden. Die Beschaffungsentscheidung SOLLTE mit dem IT-Betrieb abgestimmt sein.

Neue Ansicht: Praktiken

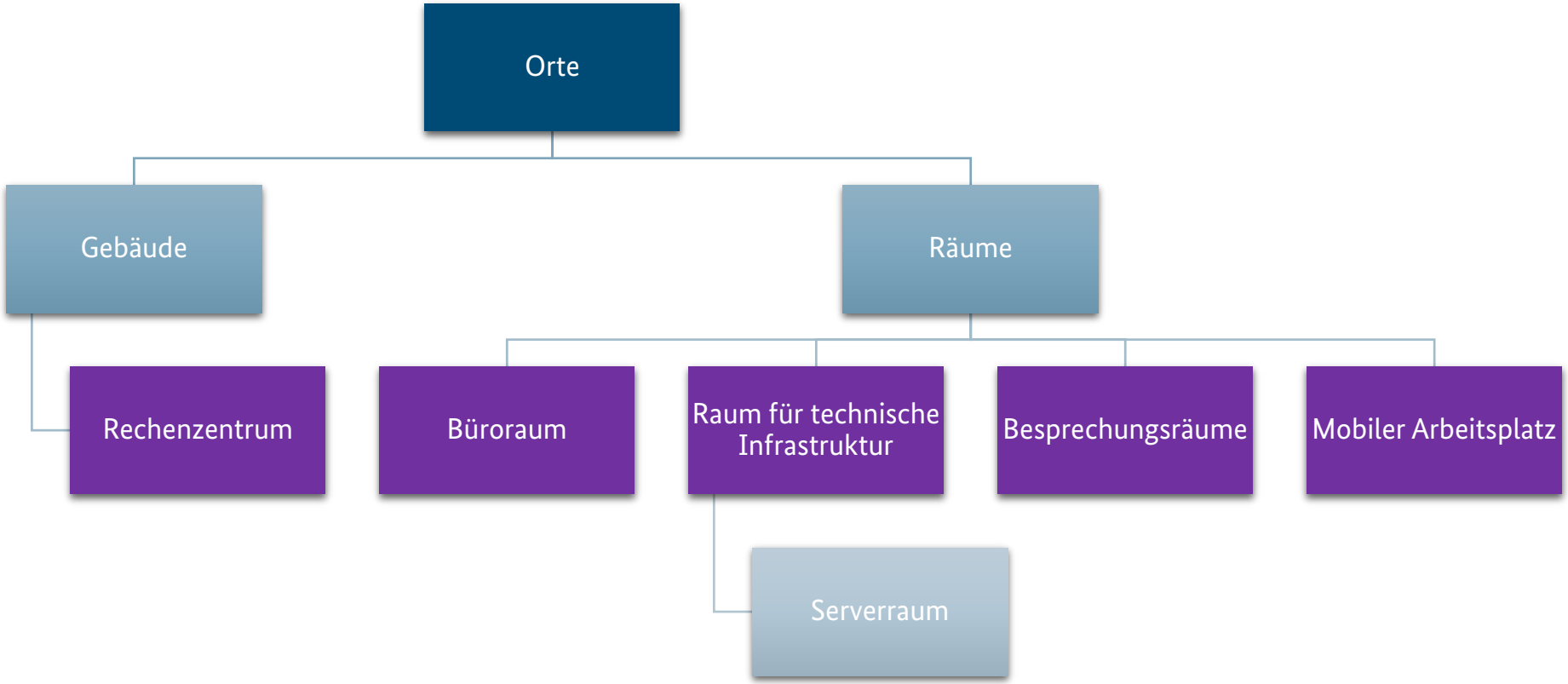
Neue Ansicht: Zielobjekte



Neue Ansicht: Beschaffung



Neue Ansicht: Orte



Neue Ansicht: Handlungsworte

- ✓ anweisen
- ○ beteiligen
- ○ sensibilisieren
- ✓ verbieten
- ○ informieren
- ○ überprüfen

vorangehen. Führungskräfte MÜSSEN die Sicherheitsvorgaben umsetzen. Hierüber hinaus MÜSSEN sie ihre Mitarbeitenden auf deren Einhaltung hinweisen.

Definition „VERBIETEN“

Den Benutzenden wird das in der Anforderung bestimmte Verhalten untersagt. Hierzu wird in Textform ausgehändigt, welches Verhalten zu welchen Bedingungen untersagt ist und dass bei Verstößen mit arbeitsrechtlichen Maßnahmen zu rechnen ist. Stellt die Institution das verbotene Verhalten fest, so ergreift sie Maßnahmen, um es zu beenden.

Neue Inhalte: Konkretisierung

ORP.3.A9 Spezielle Schulung von exponierten Personen und Institutionen (H)

Besonders exponierte Personen SOLLTEN vertiefende Schulungen in Hinblick auf mögliche Gefährdungen sowie geeignete Verhaltensweisen und Vorsichtsmaßnahmen erhalten.

Praktik	Zielobjekt	MODALVERB	Ergebnis	Handlungswort	Hinweis
Die Sensibilisierungspraktik	für Führungskräfte	SOLLTE	gegen gezielte Angriffe auf Führungskräfte (Whaling)	sensibilisieren	Inklusive spezialisierter Social Engineering Techniken wie Spear Phishing (z.B. anhand von Angaben in sozialen Netzwerken), CEO-Fraud, Deepfakes.
Die Sensibilisierungspraktik	für Führungskräfte	SOLLTE	zu ihrer Vorbildfunktion bei der Informationssicherheit	sensibilisieren	Die Vorbildfunktion von Führungskräften ist entscheidend, um eine robuste Sicherheitskultur zu etablieren und die Einhaltung der geschulten Inhalte im Arbeitsalltag zu gewährleisten.
Die Sensibilisierungspraktik	für Benutzende	KANN	gegen die in der Risikoanalyse festgestellten hohen Risiken	sensibilisieren	Werden in einer Risikoanalyse bei hohem Schutzbedarf spezielle hohe Risiken festgestellt, so sind Benutzende auf diese Risiken hinzuweisen.

Mensch, Prozess, Technik

Schneller im Ziel durch
Filtern, Automatisieren und Vereinheitlichen

Flexibel Anforderungen auswählen
und Fortschritt aufzeigen

Bewährte Inhalte,
klarer formuliert und erklärt

Konkrete Hilfe zu
Beschaffung, Schulung,...

Änderungen nachvollziehbar und in
kleineren Schritten

Bundesamt
für Sicherheit in der
Informationstechnik

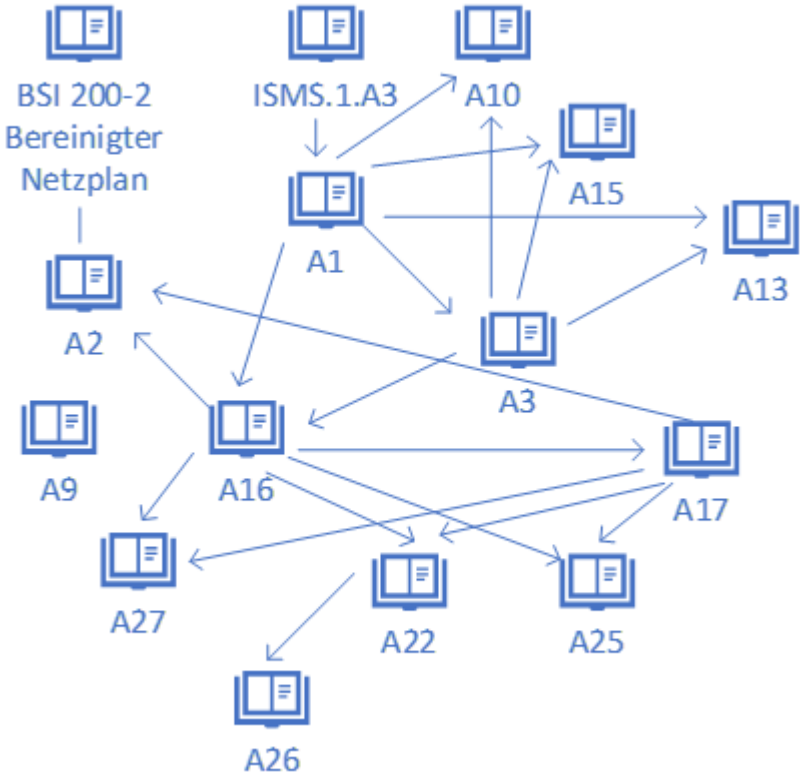
itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

Und was ist mit Dokumentation?

Daniel Gilles, BSI

NET.1.1. Netzarchitektur und –design: Dokumentationsaufwände



Beispiel, Ist-Situation Dokumentationsaufwände NET.1.1

Der Baustein NET.1.1 „Netzarchitektur und -design" beinhaltet im IT-Grundschutz-Kompendium der Edition 2022 mindestens 13 Anforderungen, die Dokumentationsanforderungen explizit motivieren. Dies erschließt sich zum Teil direkt aus dem Titel der Anforderung, zum Teil aber auch erst aus deren Inhalt und den enthaltenen *Indikatoren* (so fordert A9 die *Festlegung* der als vertrauenswürdig geltenden Netze, A10 ein *Konzept* zur DMZ-Segmentierung, A15 die *Festlegung* von Personen, Prüfkriterien und Vorgaben).

1. NET.1.1.A1 Sicherheitsrichtlinie für das Netz [IT-Betrieb] (B)
   a. Setzt voraus: ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit [Institutionsleitung] (B)
2. NET.1.1.A2 Dokumentation des Netzes [IT-Betrieb] (B)
   a. Steht in Beziehung zu: Bereinigter Netzplan aus BSI 200-2
3. NET.1.1.A3 Anforderungsspezifikation für das Netz (B)
4. NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (B)
5. NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet (B)
6. NET.1.1.A13 Netzplanung (B)
7. NET.1.1.A15 Regelmäßiger Soll-Ist-Vergleich (B)
8. NET.1.1.A16 Spezifikation der Netzarchitektur (S)
9. NET.1.1.A17 Spezifikation des Netzdesigns (S)
10. NET.1.1.A22 Spezifikation des Segmentierungskonzepts (S)
11. NET.1.1.A25 Fein- und Umsetzungsplanung von Netzarchitektur und -design (S)
12. NET.1.1.A26 Spezifikation von Betriebsprozessen für das Netz (S)
13. NET.1.1.A27 Einbindung der Netzarchitektur in die Notfallplanung [IT-Betrieb] (S)

Und jetzt zwei Schritte zurück für mehr Übersicht:

Die IT-Grundschutz(++) Dokumentenpyramide

Strategisch

- Aussagen zu Zielen, Umfeld, Leitgedanken & Rahmenwerken der Institution und ihres Informationsverbundes
- **Sicherheitsleitlinie** oder Cloud-Strategie, Notfall-Strategie, Dienstleister-Strategie

Taktisch

- Konkrete Vorgaberichtlinien (Anforderungen)für in sich abgeschlossenen Bereiche in der Institution
  - xyz MUSS, SOLLTE, DARF NICHT gemacht werden…
- Im IT-Grundschutz stellen bereits die Bausteine des Kompendiums diese Vorgaberichtlinien dar

Operativ – Gestaltung (Thema)

- individuell-spezifische Gestaltung ausgewählter Themen, die nicht abschließend durch die taktischen Vorgaberichtlinien geregelt werden können
- Bsp.: Kryptokonzept, Notfallkonzept, Datensicherungskonzept, …

Operativ – Vermittlung (Adressaten)

- individuell-spezifische Vermittlung an ausgewählte Adressaten
- Bsp.: Arbeitsanweisungen, Prozessabläufe, Checklisten, Schulungsinhalte, …

Operativ – Ergebnis

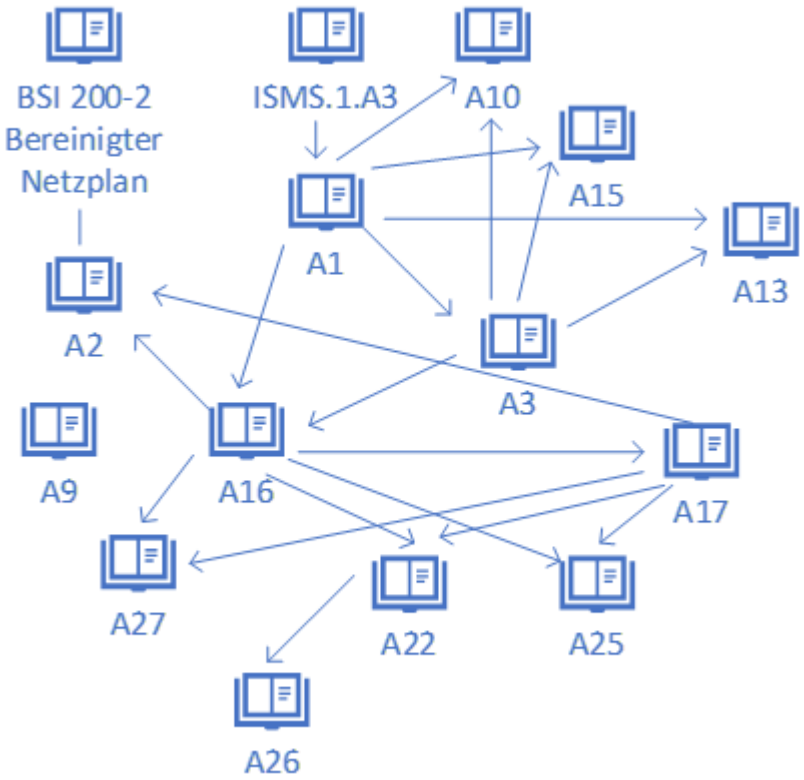
- Explizit geforderte Dokumentation ausgewählter Ereignisse oder Aktivitäten
- Bsp.: Liste Zutrittsbefugter, Netzplan, FW-Konfiguration, Ergebnisse der Protokollierung, Protokoll Revision (KVP), …

Hinweise
DA = Dokumentationsaufwand
IV = Informationsverbund
KVP = Kontinuierlicher Verbesserungsprozess

(1) Ein DA kann Inhalte enthalten, die sich mehr als einem Typ zuordnen lassen. Dies gilt insbesondere für operative DA, die sowohl Inhalte zu Gestaltung als auch zu Vermittlung und ggf. Ergebnissen enthalten können.

(2) Nur aus formalen Gründen werden keine DAs gefordert. Ein „Operativ-Ergebnis“ DA setzt z.B. nicht zwingend einen „Operativ-Vermittlung“ oder „Operativ-Gestaltung“ DA voraus.

NET.1.1. Netzarchitektur und –design: Dokumentationsaufwände



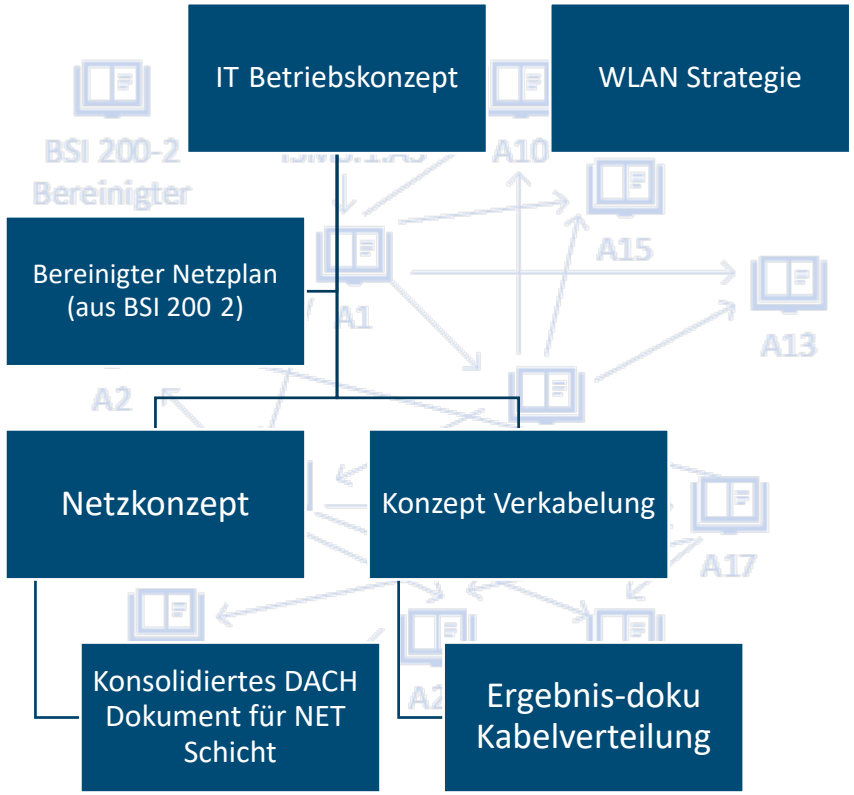
Beispiel, Ist-Situation Dokumentationsaufwände NET.1.1

Der Baustein NET.1.1 „Netzarchitektur und -design" beinhaltet im IT-Grundschutz-Kompendium der Edition 2022 mindestens 13 Anforderungen, die Dokumentationsanforderungen explizit motivieren. Dies erschließt sich zum Teil direkt aus dem Titel der Anforderung, zum Teil aber auch erst aus deren Inhalt und den enthaltenen *Indikatoren* (so fordert A9 die *Festlegung* der als vertrauenswürdig geltenden Netze, A10 ein *Konzept* zur DMZ-Segmentierung, A15 die *Festlegung* von Personen, Prüfkriterien und Vorgaben).

1. NET.1.1.A1 Sicherheitsrichtlinie für das Netz [IT-Betrieb] (B)
   a. Setzt voraus: ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit [Institutionsleitung] (B)
2. NET.1.1.A2 Dokumentation des Netzes [IT-Betrieb] (B)
   a. Steht in Beziehung zu: Bereinigter Netzplan aus BSI 200-2
3. NET.1.1.A3 Anforderungsspezifikation für das Netz (B)
4. NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (B)
5. NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet (B)
6. NET.1.1.A13 Netzplanung (B)
7. NET.1.1.A15 Regelmäßiger Soll-Ist-Vergleich (B)
8. NET.1.1.A16 Spezifikation der Netzarchitektur (S)
9. NET.1.1.A17 Spezifikation des Netzdesigns (S)
10. NET.1.1.A22 Spezifikation des Segmentierungskonzepts (S)
11. NET.1.1.A25 Fein- und Umsetzungsplanung von Netzarchitektur und -design (S)
12. NET.1.1.A26 Spezifikation von Betriebsprozessen für das Netz (S)
13. NET.1.1.A27 Einbindung der Netzarchitektur in die Notfallplanung [IT-Betrieb] (S)

Jetzt optimiert!

NET.1.1. Netzarchitektur und –design: Dokumentationsaufwände



<u>Statt 10+ nur 1 Operativ-Gestaltung DA zu NET.1.1</u>

Thematische Konsolidierung technischer DA-Anteile

- Segmentierung (A1, A5, A6, A10, A16, A19, A22, A23)
- Zonierung (A1, A4, A16)
- Kommunikationsbeziehungen (A1, A16)
- Protokolle (A1, A7, A16)
- Organisationsinterne und -übergreifende Vernetzung & Absicherung (Ver-schlüsselung) (A1, A7, A16, A17)
- Anbindung an nicht vertrauenswürdige Netze (A8, A9, A10, A11, A12, A16, A18)
- Administration (A17, A21)
- Netzkomponenten (A17)
- Anbindung von Endgeräten (A17, A20)

Thematische Konsolidierung organisatorischer DA-Anteile

- Erstellung, Bekanntgabe, Aktualisierung, Überprüfung des Anforderungsdokuments, sofern nicht bereits durch die Festlegungen zur Lenkung und dem Einsatz von Dokumenten abgedeckt (A1)
- Planung, Aufbau, Betrieb, Not-Betrieb, Aktualisierung, Außerbetriebnahme & Überprüfung von Netzanteilen (A13, A14, A15)

Ansatz zur Unterstützung im aktuellen IT-Grundschutz

- **Aufbauend** auf dem aktuellen IT-Grundschutz
  - Mit dem Ziel, den **aktuellen Umgang** mit Dokumentation zu optimieren
  - Als **Empfehlung** bzw. Best-Practice des BSI zu verstehen, sozusagen als *„empfohlenen Interpretation des IT-Grundschutzes“*
  - **nicht** normativ
- **Grundlage** für die weitere Fortentwicklung im Grundschutz++
- Einführung und Orientierung an der **Dokumentenpyramide**

Excel Übersicht über konsolidierte DA im IT-Grundschutz - Stand Kompendium 2023

Dokumentenname (konsolidiertes Dachdokument oder atomar relevantes Dokument)	Kurze Inhaltsangabe	übergreifende Themen (primär aus den Prozess- und Netzbausteinen)	Stufe (In Bezug auf übergreifende Themen)	bausteinspezifische Ergänzungen (aus den Systembausteinen)
Leitlinie zur Informationssicherheit	Siehe Spalte B	ISMS.1: A2, A3	Basis	-
Sicherheitskonzept (Organisation des Sicherheitsprozesses ISMS)	Beschreibung der über die Leitlinie hinausgehenden Rahmenbedingungen des ISMS, der Organisation, Aufbau und des Sicherheitsprozesses des ISMS.	ISMS.1: A6, A7, A10, A11, A13, A16 ORP.5: A1, A5 CON.2: A1 ORP.1: A1, A2, A4 ORP.2: A1, A2, A14, A15(Falls diese ihnalte bereits an anderer Stelle hinreichend beschrieben sind, z.B. in einem detaillierten GVP, bedarf es keiner Kopie ins Sicherheitskonzepts.)	Basis Standard erhöhter Schutzbedarf	APP.2.1: A1 IND. 2.7: A4
Management-Berichte	Berichte über den aktuellen Stand des ISMS an die Leitungsebene	ISMS.1: A12	Standard	

Optimierungsansätze im IT-Grundschutz++ weiter gedacht

- Transparente Forderung und Konsolidierung der DAs im **nativen IT-Grundschutz++** ohne Hilfsmittel
- Bessere **Strukturierung** der Bausteine
- Gebündelter **Einstieg** zu IT-Grundschutz Dokumentation
- **Hinweise** zu den Formaten der DA und Freiheiten in der Gestaltung der DA
- Möglichst **wenige** notwendige Quellen zu jedem DA
- **Jeder Baustein** informiert über seine notwendigen (konsolidierten!) DA
- **ITGS-Tool-freundliche** Umsetzung der Baustein-DA-Anteile
- Gremium **engagierter** ITGS-Anwendungs- und Vermittlungsvertreter
- Entbehrlichkeit von DA zu abgeschlossenen Lebenszyklusphasen

*

** DA = Dokumentationsaufwand*

Bundesamt
für Sicherheit in der
Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY

Deutschland
Digital•Sicher•BSI•

Kennziffern zur Effizienzmessung

Stefan Schuck, BSI

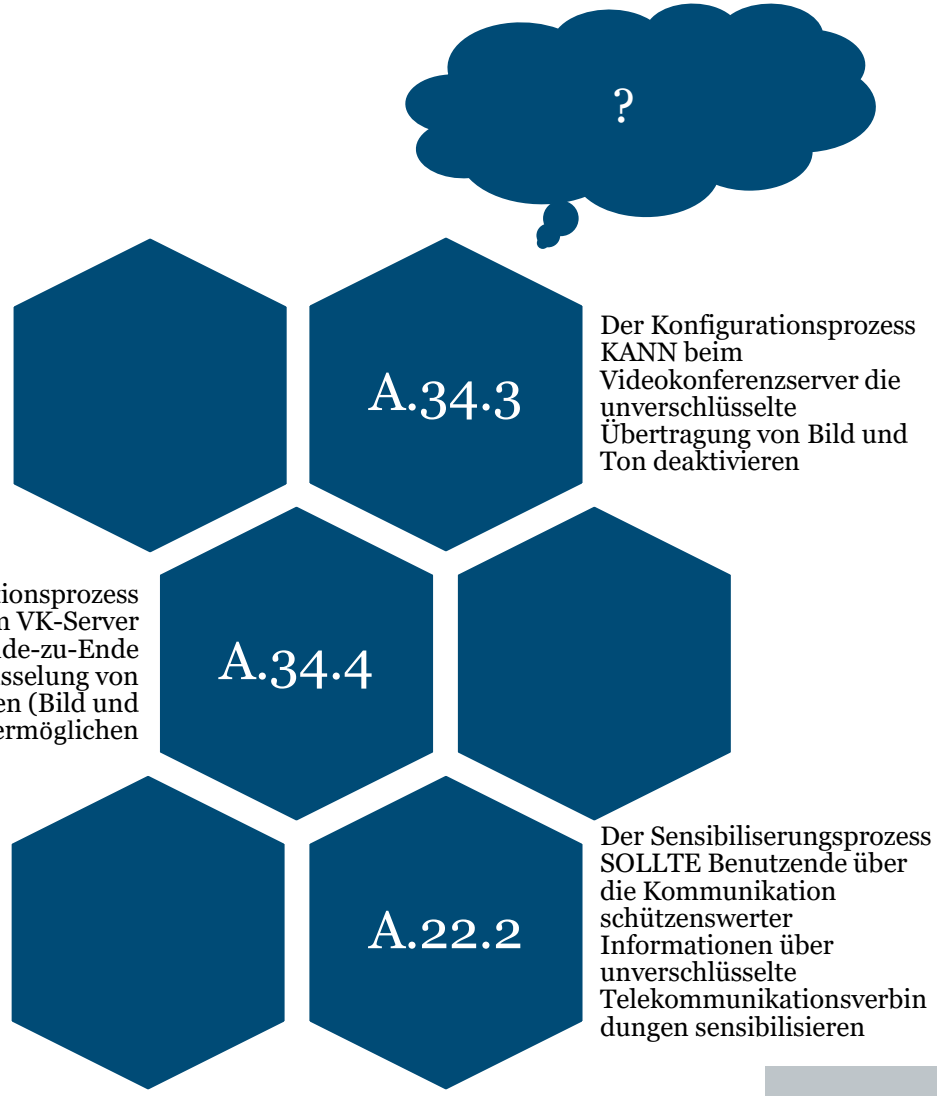
Wo bleibt das (Sicherheits-)Niveau?

IT-Grundschutz

Basis Anforderungen
- Mindestniveau

Standard Anforderungen
- Erweiterung des Niveaus

Anforderungen für einen erhöhten Schutzbedarf
- Risikobasierte Erweiterung



Die Stufen

1
- Für alle Umsetzbar
- Schnell umgesetzt
- Schützt gegen zahlreiche Vorfälle

2
- Für Kleinunternehmen (z.B. Handwerksbetriebe) umsetzbar
- Umsetzung ist in bis zu 60 Minuten vorstellbar
- Schützt gegen typische Sicherheitsvorfälle

3
- Für KMU umsetzbar
- Umsetzung braucht nicht mehr als einen Arbeitstag

4
- Für Bundesbehörden oder größere Unternehmen umsetzbar
- Anforderung entspricht Stand der Technik

5
- Anforderung übersteigt den normalen Schutzbedarf

Was bringt mir eine Anforderung

Kreuzreferenztabelle

SYS.1.1	Name	CIA	G 0.8	G 0.14	G 0.16	G 0.18	G 0.19	G 0.20
SYS.1.1.A1	Zugriffsschutz und Nutzung				X			
SYS.1.1.A2	Authentisierung an Servern			X			X	
SYS.1.1.A3	ENTFALLEN							
SYS.1.1.A4	ENTFALLEN							
SYS.1.1.A5	Schutz von Schnittstellen							
SYS.1.1.A6	Deaktivierung nicht benötigter Dienste			X		X	X	
SYS.1.1.A7	ENTFALLEN							
SYS.1.1.A8	ENTFALLEN							
SYS.1.1.A9	Einsatz von Virenschutz-Programmen auf Servern							
SYS.1.1.A10	Protokollierung							
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server							
SYS.1.1.A12	Planung des Server-Einsatzes							
SYS.1.1.A13	Beschaffung von Servern							
SYS.1.1.A14	ENTFALLEN							
SYS.1.1.A15	Unterbrechungsfreie und stabile Stromversorgung							
SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern							
SYS.1.1.A17	ENTFALLEN							
SYS.1.1.A18	ENTFALLEN							
SYS.1.1.A19	Einrichtung lokaler Paketfilter						X	
SYS.1.1.A20	ENTFALLEN							
SYS.1.1.A21	Betriebsdokumentation für Server					X		

Welche Gefährdungen werden behandelt

Effektivitätskennziffern

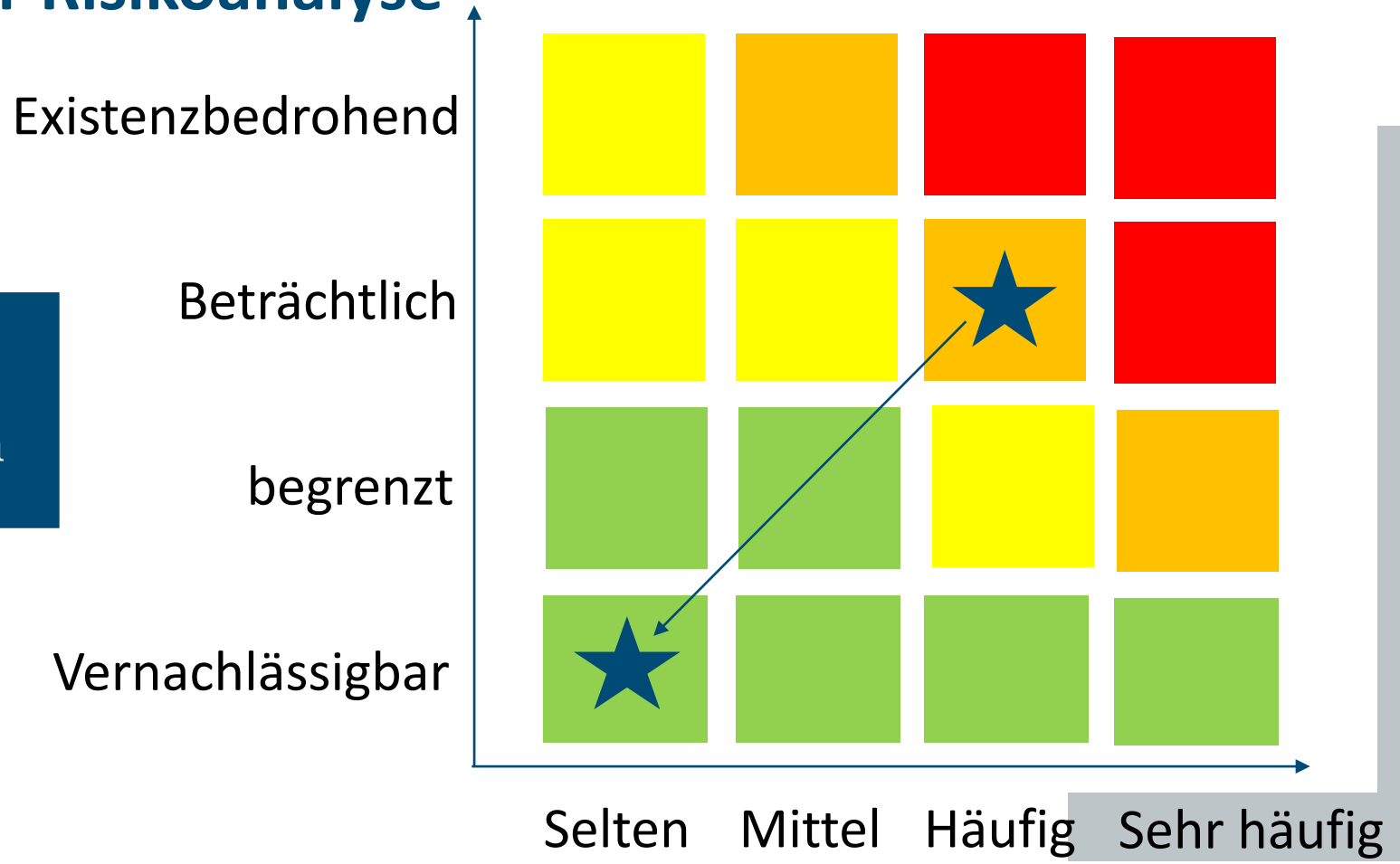
Welche Gefährdung/en werden behandelt

Wie Effektiv ist die Anforderung in der Behandlung EINER Gefährdung

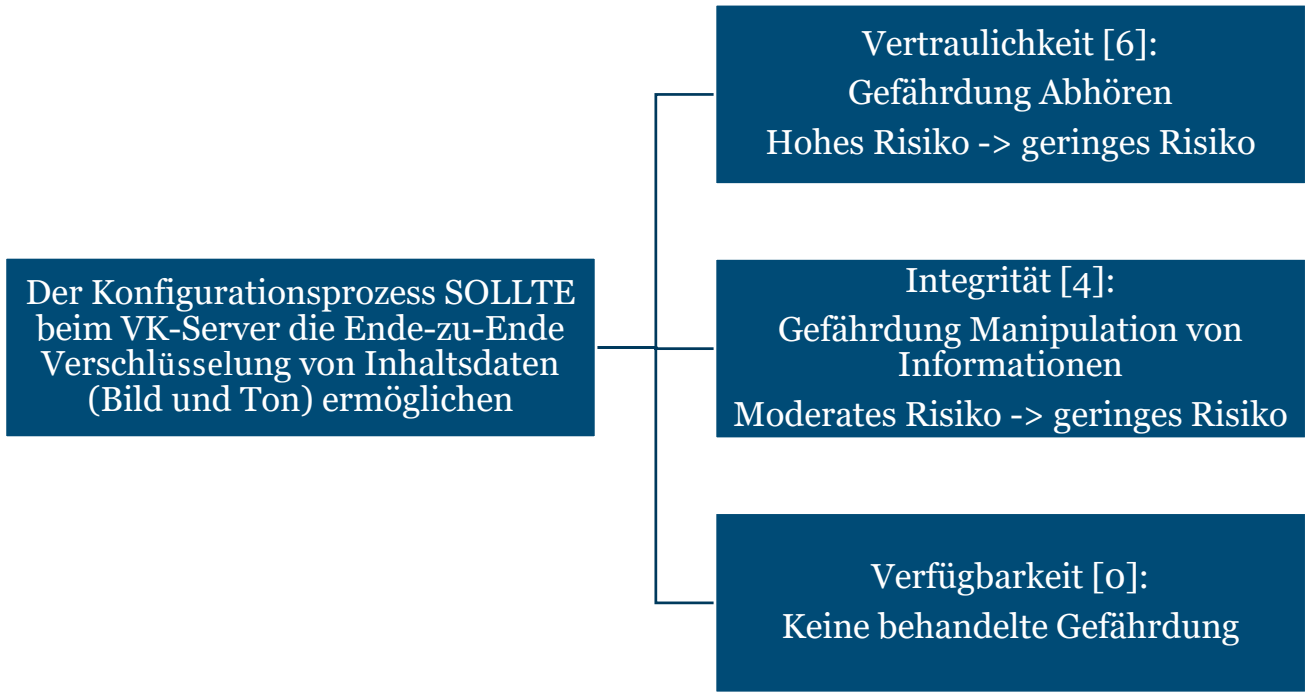
Kennziffern auf Basis der Risikoanalyse

Vertraulichkeit [6]:

Aus einem hohen Risiko der Gefährdung Abhören wird ein geringes Risiko



Das bringt mir diese Anforderung



Kennziffern:

- Ergeben sich aus der Risikoanalyse
- Sind unabhängig für Vertraulichkeit, Verfügbarkeit und Integrität berechnet

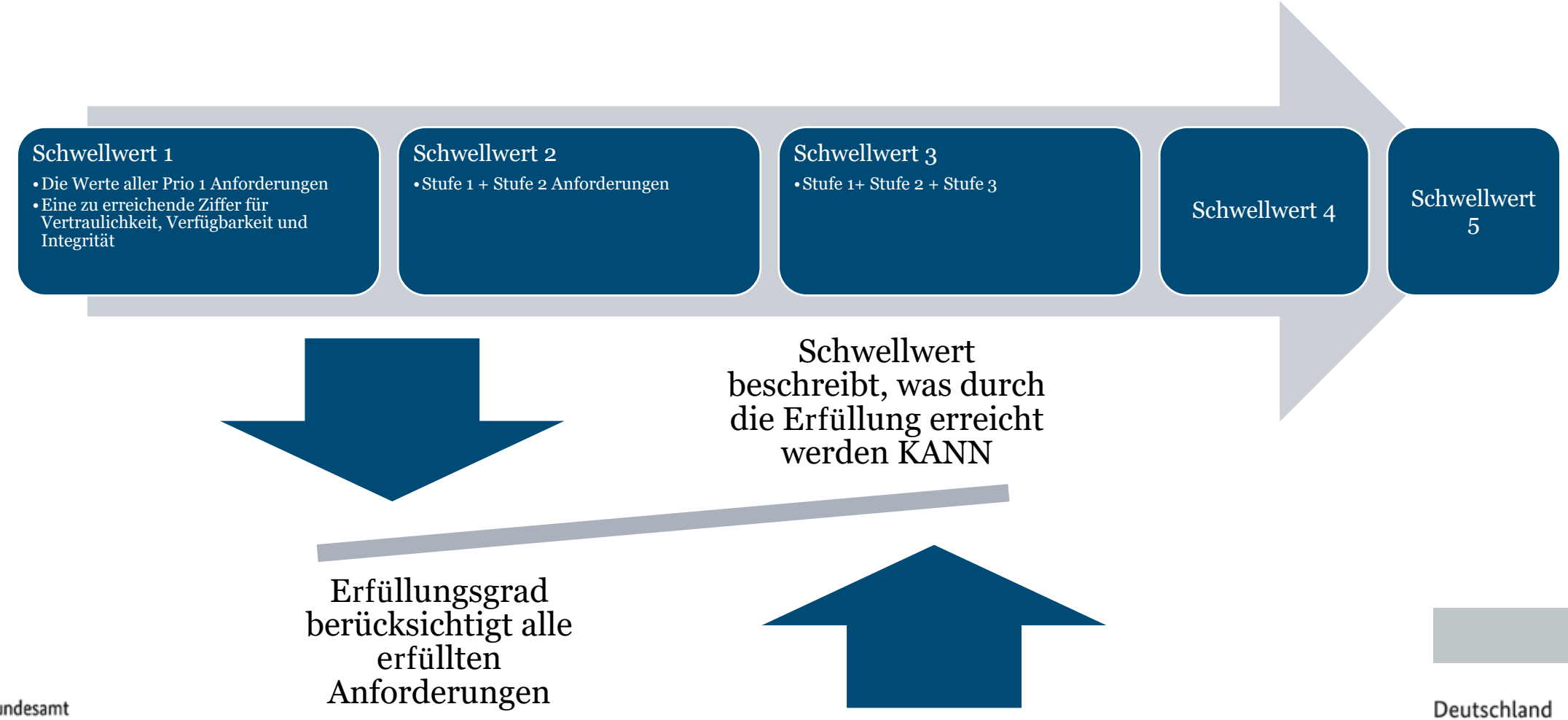
Schwellwerte für VK-Server

[Stufe 1] Sensibilisierung gegen die Bild- und Tonaufzeichnung ohne vorherige Ankündigung an alle Betroffenen	• Vertraulichkeit : 6 • Integrität: 0 • Vertraulichkeit 0
[Stufe 1] Der IT-Betrieb legt zeitnahe Installation von Sicherheitsupdates fest	• Vertraulichkeit [4] • Integrität [3] • Verfügbarkeit [4]
[Stufe 1]	• Vertraulichkeit [X] • Integrität [Y] • Verfügbarkeit [Z]

Schwellwert 1

- ☐ Vertraulichkeit [10+X]
- ☐ Integrität [3+Y]
- ☐ Verfügbarkeit[4+Z]

Was muss ich erfüllen?



Agenda

13:00 Uhr: Begrüßung und Keynote (Sandro Amendola)
13:15 Uhr: IT-Grundschutz gestern und heute (Holger Schildt)
13:35 Uhr: Weg in die Basis-Absicherung (WiBA) (Stefanie Euler)
13:55 Uhr: Cybersicherheitsvorgaben für die Bundesverwaltung (Julia Hein)
14:15 Uhr: Vision zur Weiterentwicklung des IT-Grundschutzes (Dennis Kügler)
14:30 Uhr: 15 Minuten Pause
14:45 Uhr: Struktur der zukünftige Anforderungen (Florian Göhler)
15:05 Uhr: Struktur des IT-Grundschutz-Kompendium (Christoph Weißenborn)
15:25 Uhr: Und was ist mit Dokumentation? (Daniel Gilles)
15:45 Uhr: Kennziffern zur Effizienzmessung (Stefan Schuck)
16:05 Uhr: Pause
16:15 Uhr: Fragen und Diskussion mit allen Vortragenden
17:00 Uhr: Ende

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland Digital•Sicher•BSI•

Sandro Amendola
Holger Schildt
Stefanie Euler
Julia Hein, BMI
Dr. Dennis Kügler
Florian Göhler
Christoph Weißenborn
Daniel Gilles
Stefan Schuck

It-grundschutz@bsi.bund.de
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik

itsa EXPO CONGRESS
HOME OF IT SECURITY