IT-Grundschutz++

Vom Brockhaus zum Wiki in 30 Minuten

Bundesamt
für Sicherheit in der
Informationstechnik

05.05.2025 | 11. Kommunaler IT-Sicherheitskongress

Daniel Gilles | BSI-Standards und IT-Grundschutz | BSI

Agenda

1. Motivation und Ziele
2. Konsequent Prozessorientiert
3. …und wie?
4. Offenes Gespräch

Bild: © AdobeStock/Liudmyla

01. Motivation und Ziele

Vision IT-Grundschutz++

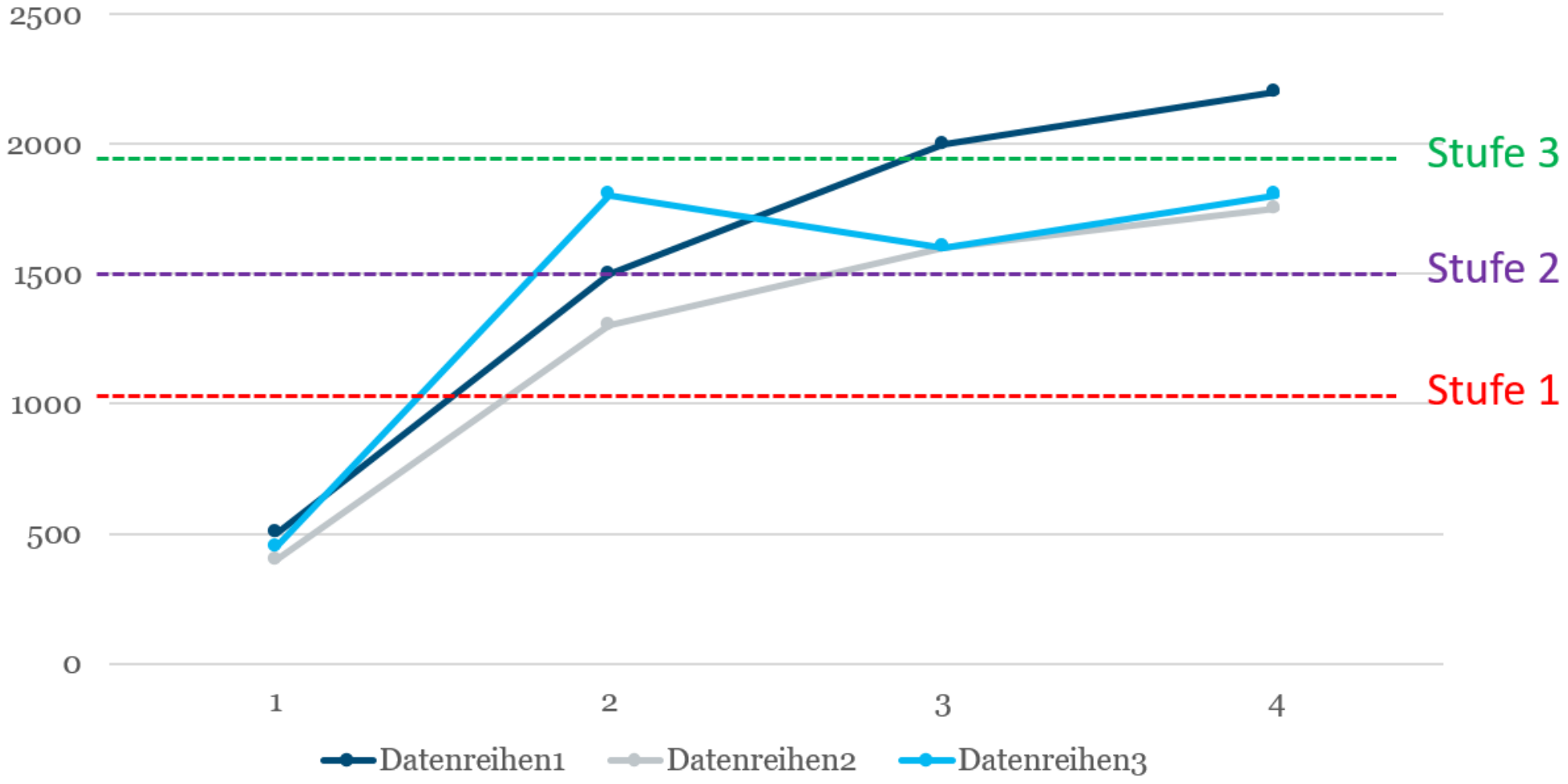
Wer Visionen hat, soll zum BSI gehen

Cybersicherheit ist mess- & automatisierbar:

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

Kennzahlen für Entscheider

Resilienz wird messbar, vergleichbar und verständlich durch Kennzahlindikatoren



Anwendung datengesteuerter Werkzeuge weitgehend ermöglichen

Automatisierung des ISMS

Erfassung

- Systeme
- Daten
- Lieferanten

Integration

- Continuous Integration, Delivery and Deployment
- Smart Standards
- Smart Contracts

Aufrechterhaltung

- Überwachung der Konformität
- Sperrung
- Alarmierung

Redundant arbeiten soll die Technik, nicht der Mensch

Ein Blick auf die Herausforderungen im aktuellen IT-GS

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 Anforderungen der entsprechenden Bausteine wie APP.2.2 *Active Directory* zu erfüllen.

2 Gefährdungslage

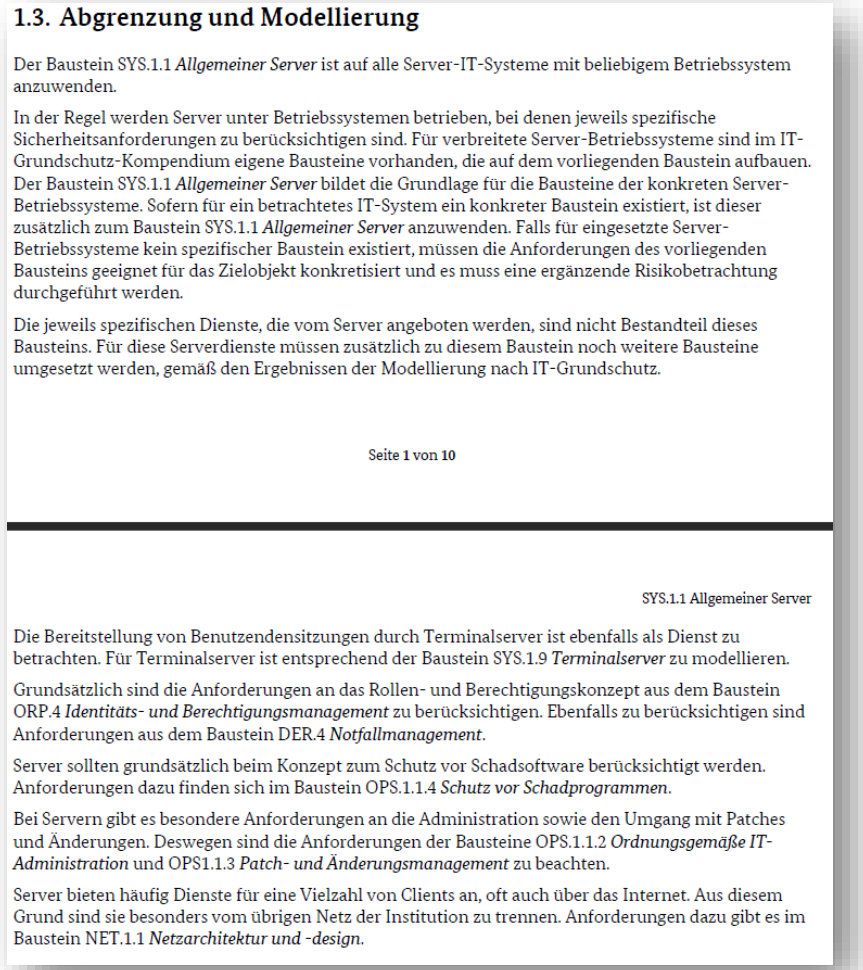
Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.2.3 *Clients*

Prosa

Von „sicher" bis Maßnahme

Redundant arbeiten soll die Technik, nicht der Mensch

Ein Blick auf die Herausforderungen im aktuellen IT-GS



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.

Seite 1 von 10

SYS.1.1 Allgemeiner Server

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*.

Server sollten grundsätzlich beim Konzept zum Schutz vor Schadsoftware berücksichtigt werden. Anforderungen dazu finden sich im Baustein OPS.1.1.4 *Schutz vor Schadprogrammen*.

Bei Servern gibt es besondere Anforderungen an die Administration sowie den Umgang mit Patches und Änderungen. Deswegen sind die Anforderungen der Bausteine OPS.1.1.2 *Ordnungsgemäße IT-Administration* und OPS1.1.3 *Patch- und Änderungsmanagement* zu beachten.

Server bieten häufig Dienste für eine Vielzahl von Clients an, oft auch über das Internet. Aus diesem Grund sind sie besonders vom übrigen Netz der Institution zu trennen. Anforderungen dazu gibt es im Baustein NET.1.1 *Netzarchitektur und -design*.

Prosa

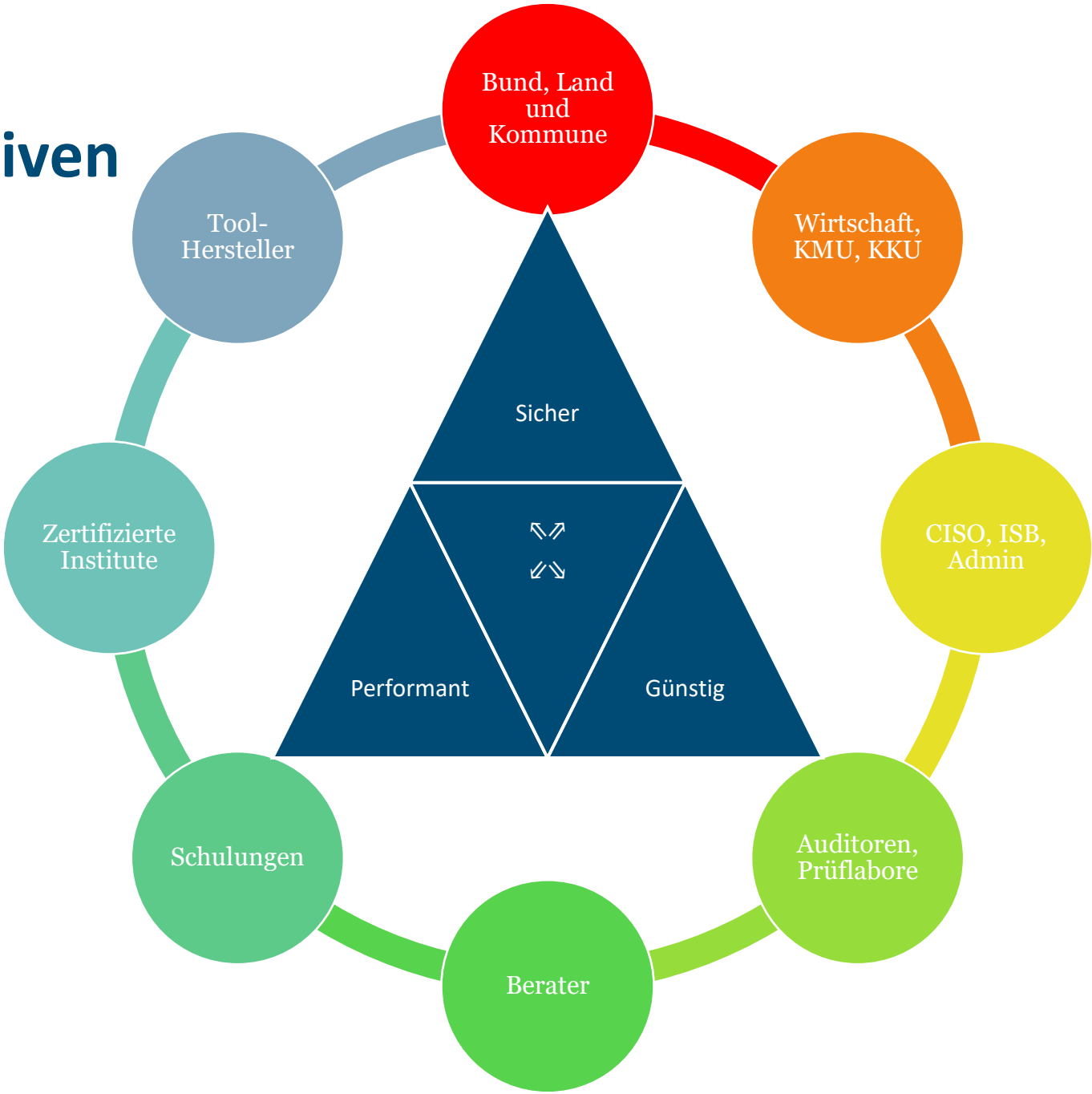
Von „sicher“ bis Maßnahme

Manuelle Abhängigkeiten

Viele Redundanzen

Stakeholder und Perspektiven

Viele Brillen, ein Bild



02. Konsequent Prozessorientiert

Praktiken – ein neuer Zugang zu Anforderungen

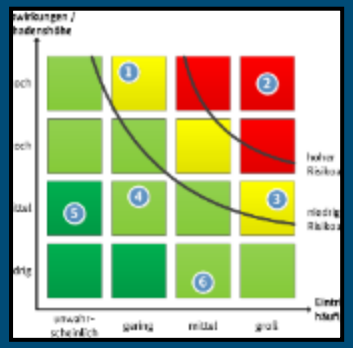
Integration von Prozessen und Technologien

Von Bausteinen zu Themen

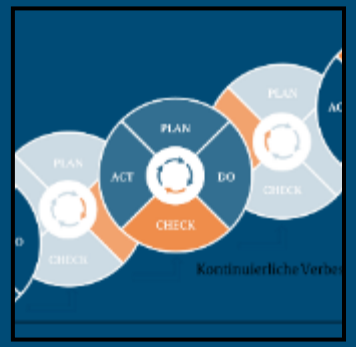
Zuständigkeiten

Change Management

Risikoanalyse



Checks und Audits



Anweisung und Schulung

Architektur

Protokollierung

Detektion und Pentest

Monitoring

Datensicherung

Vom Baustein zur Praktik

Praktiken als Prozesse des ISMS

Ebenen der Abstraktion

Flughöhen im Zusammenhang

Geschäfts- und Sicherheitsziele

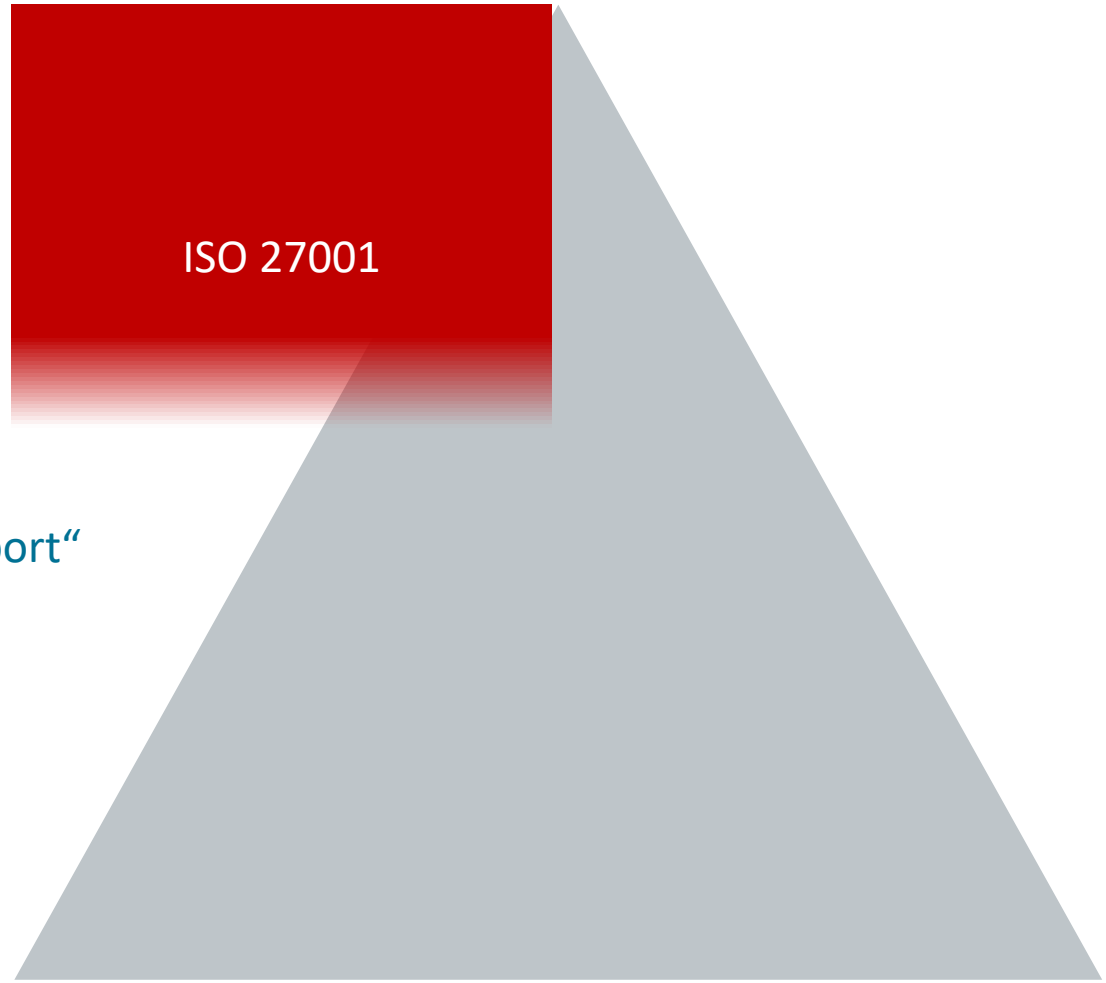
„Vertraulichkeit für unsere Daten“

Lösungsneutrale Prinzipien

„Anwendungen verschlüsseln Daten beim Transport“

Lösungsspezifikation

„Verschlüsselung mit AES256 im CBC-Modus “



Ebenen der Abstraktion

Flughöhen im Zusammenhang

Geschäfts- und Sicherheitsziele

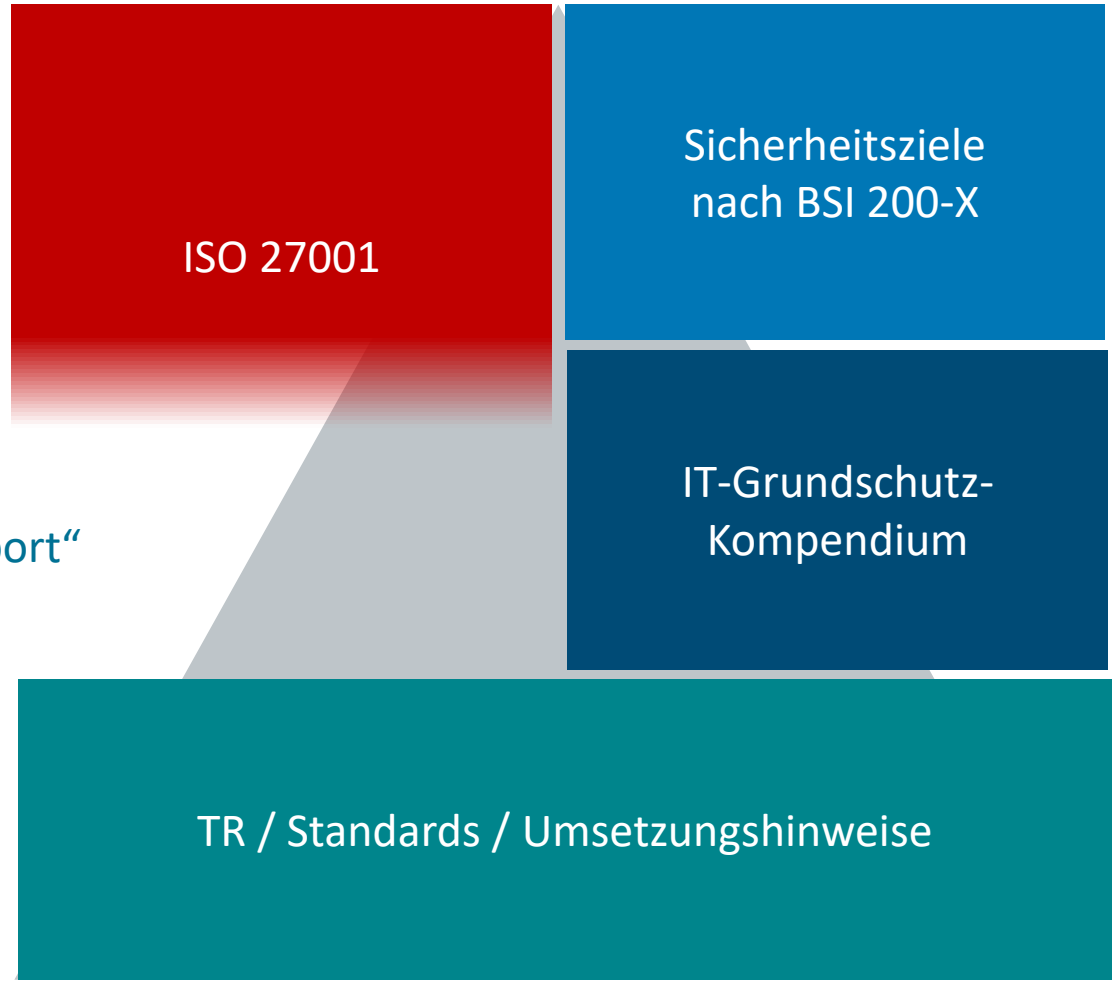
„Vertraulichkeit für unsere Daten“

Lösungsneutrale Prinzipien

„Anwendungen verschlüsseln Daten beim Transport“

Lösungsspezifikation

„Verschlüsselung mit AES256 im CBC-Modus “



03. …und wie?

Bild: © AdobeStock/Azazul

Struktur für Anforderungen durch Satzschablonen

Von Johann zu JSON

{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.

Filtern und Verstehen durch Metadaten

Genau das sehen, was Sie jetzt brauchen

Praktik	Zielobjekt	MODALVERB	Ergebnis	Handlungswort	Hinweis	Tags
Konfiguration	IT-Systeme	SOLLTE	nicht benötigte Funktionen	deaktivieren	Deinstallieren oder Deaktivieren Sie Funktionen, die für Betrieb oder Sicherheit nicht benötigt werden, z.B. ungenutzte Cloud-Anbindungen, Module oder Einstellungen.	Hardening
Sensibilisierung	Benutzende	SOLLTE	die Weitergabe von personengebundenen Authentisierungsmitteln	verbieten	Personengebundene Authentisierungsmittel sind z.B. Passworte, Private PKI-Schlüssel oder Mehr-Faktor-Authentifizierungstoken wie Smartcards.	
Detektion	VPN-Gateways	SOLLTE	VPN-Verbindungen auf unberechtigte Einwahlen	überprüfen	Kann manuell oder durch automatische Analyse von Logdateien erfolgen. Dabei kann z.B. nach ungewöhnlichen vielen fehlgeschlagenen Anmeldungen, veralteten Berechtigungen, Einwahlen von Adminaccounts, ungewöhnlichen Einwahlorten/IP-Adressbereichen/User Agents oder Uhrzeiten gesucht werden.	Zero Trust, Advanced Persistent Threats (APT)

Filtern und Verstehen durch Metadaten

Genau das sehen, was Sie jetzt brauchen

Praktiken

- Prozesse des ISMS
- Strategie, Taktik, Operativ

Handlungsworte

- Definierte Tätigkeiten
- Mensch oder Maschine

Zielobjekte

- Technik: Server, Linux, …
- Organisatorisch:
  Standorte, Adressaten, Verträge, …

Hinweise

- Ziele und Definitionen
- Umsetzungshinweise

Stufe 0-5

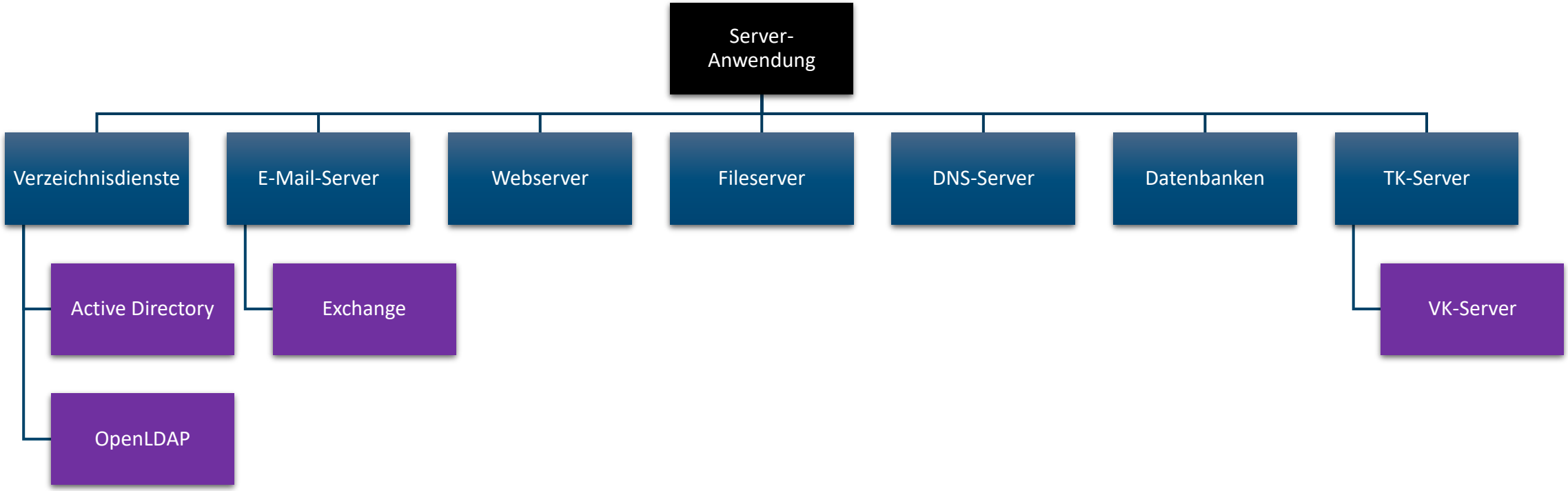
- Von Quick-Win bis Nice-to-have
- Von Jeder bis erhöhter Schutzbedarf

Tags

- Querschnittsthemen
- Trends im Fokus

Filter: Technische Zielobjekte

Anforderungen horizontal und vertikal abhaken



… und was ist mit Dokumentation?

Dokumentenpyramide IT-Grundschutz

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

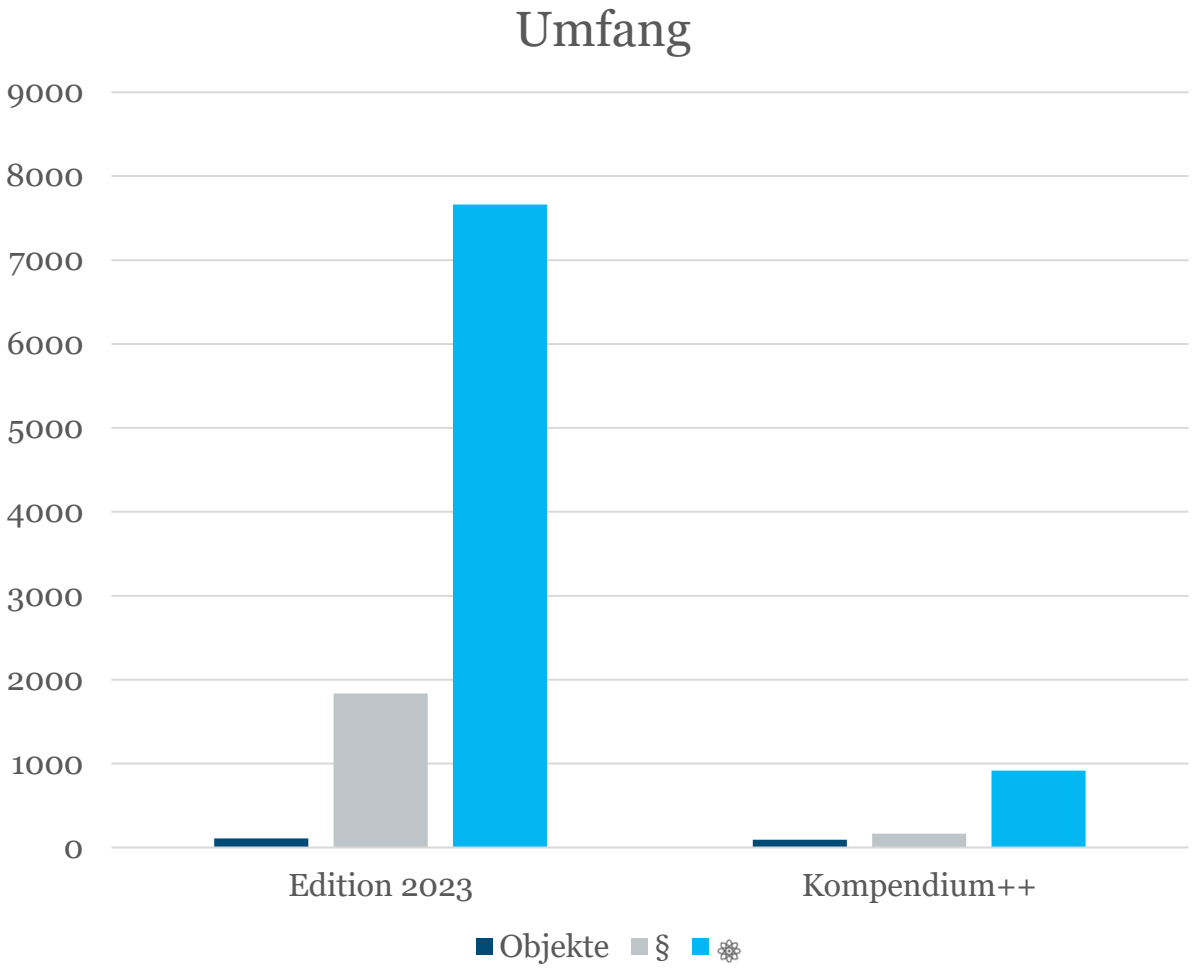
(1) Ein DA kann Inhalte enthalten, die sich mehr als einem Typ zuordnen lassen. Dies gilt insbesondere für operative DA, die sowohl Inhalte zu Gestaltung als auch zu Vermittlung und ggf. Ergebnissen enthalten können.

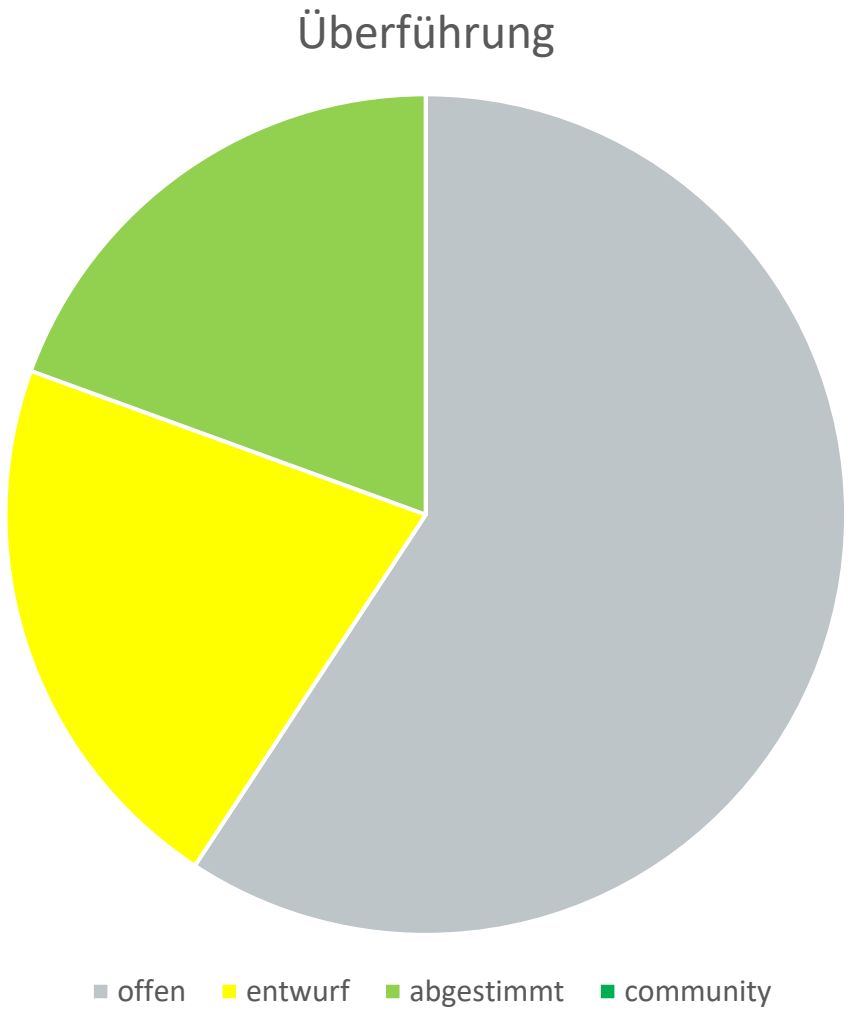
(2) Nur aus formalen Gründen werden keine DAs gefordert. Ein „Operativ-Ergebnis“ DA setzt z.B. nicht zwingend einen „Operativ-Vermittlung“ oder „Operativ-Gestaltung“ DA voraus.

04. Aktueller Sachstand

Sachstand

Wie viel ++ steckt schon im neuen Kompendium?



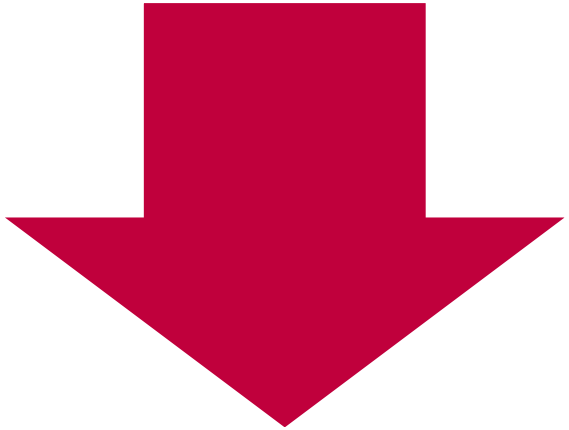


Fachinhalte im Fokus

Reduktion der Masse, nicht der Sicherheit

Fokussiert

- Konkretisierung: Was ist wann zu erreichen
- Hinweise: Zweck, Definitionen, Umsetzung
- Neuerungen: NIS2, Videokonferenz-Server



Reduziert

- Anforderungen ohne klares Sicherheitsziel
- Doppelungen

Bundesamt
für Sicherheit in der
Informationstechnik

Vielen Dank für Ihre Aufmerksamkeit!

IT-Grundschutz++ Team

it-grundschutz@bsi.bund.de
Tel.: +49 (0) 228 9582 0

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Follow us:

Bild: © AdobeStock/ The Little Hut

ab hier Ende

Bild: © AdobeStock/ The Little Hut