IT-Grundschutz ++

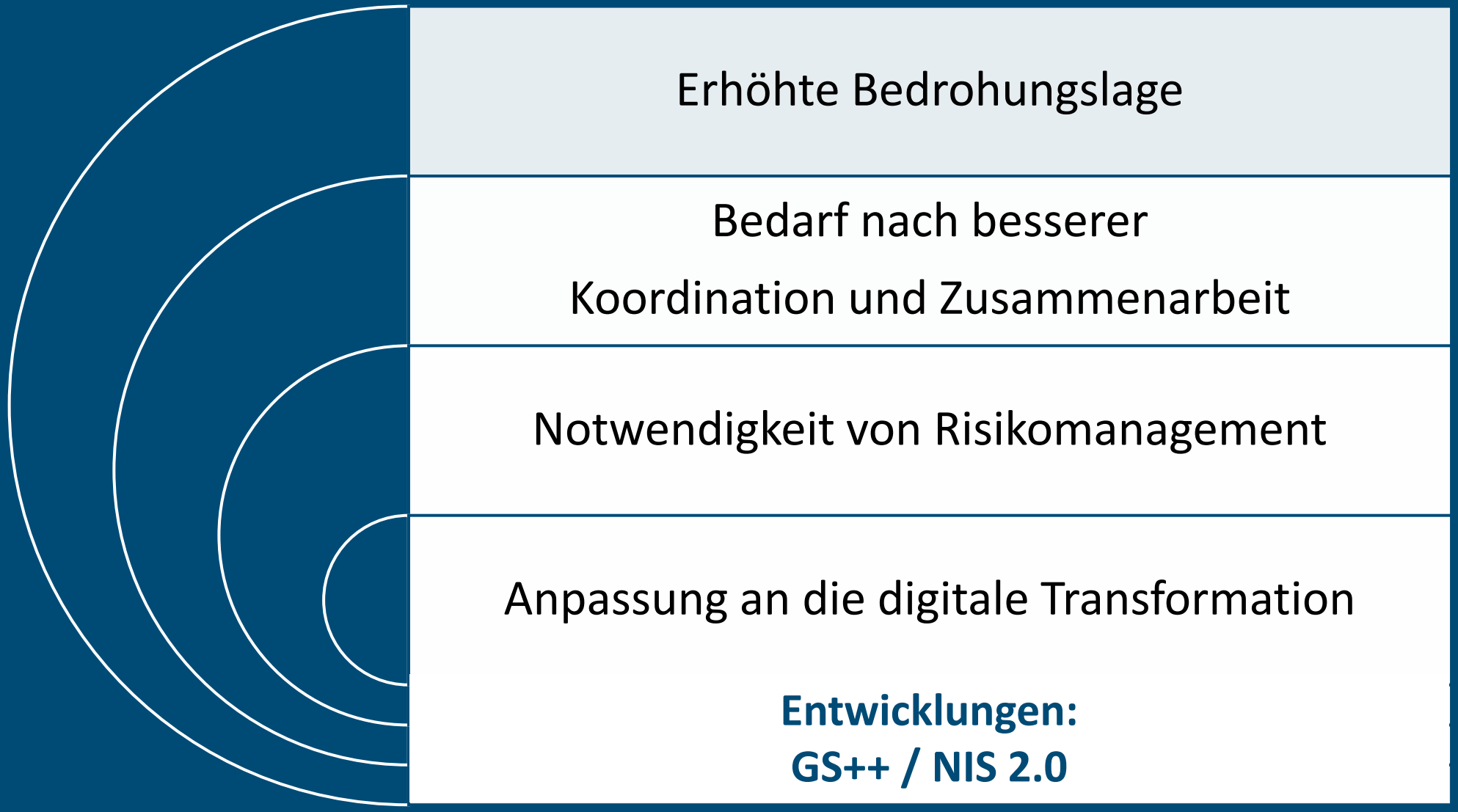
OMNISECURE 2025

Bundesamt
für Sicherheit in der
Informationstechnik

Bild: © AdobeStock/Nirut

Ausgangslage

DEU und EU



IT-Grundschutz++

Cybersicherheit ist mess- & automatisierbar:

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

Wesentliche Veränderungen

Kompendium

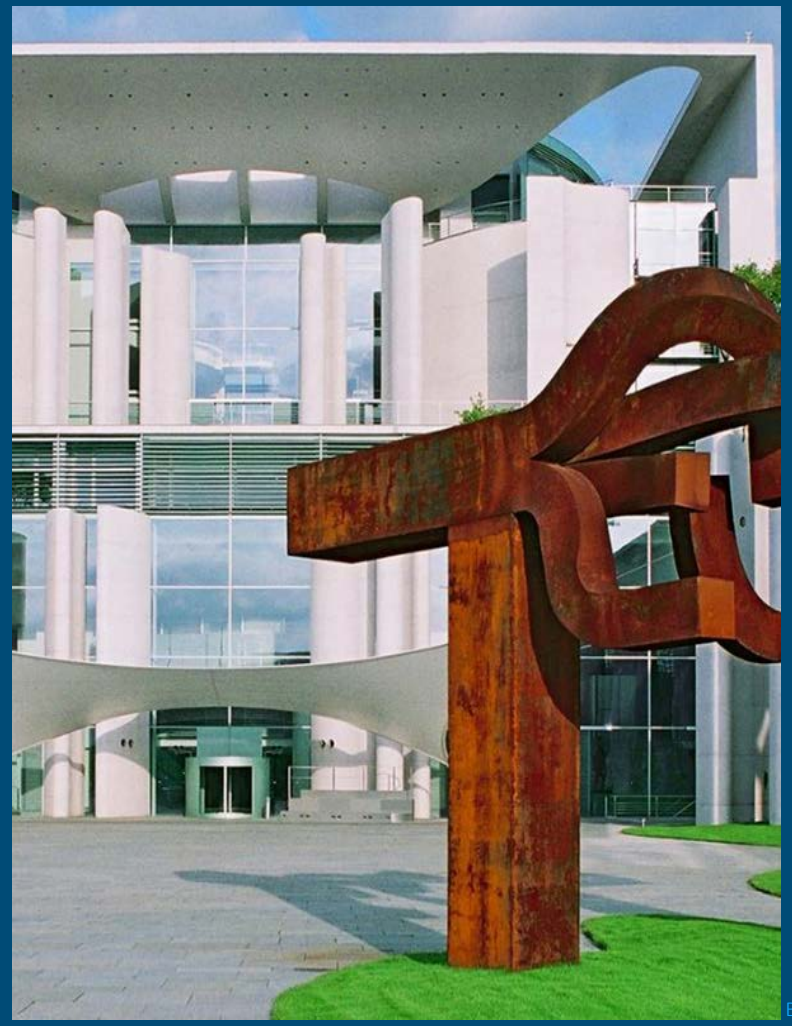


Bild: ©BSI

IT-Grundschutz **vs.** **IT-Grundschutz++**

historisch gewachsenes Gesamtwerk

111 Bausteine

redundante Informationen

Dokumentenversionierung

digitale Datensammlung

Kontinuierliche Ergänzung durch die Kommunity

Zielobjekte

JSON

Leistungsmessung

Index

Unterschiedliche Stufen des Sicherheitsniveaus

Praktiken

Filtern und Verstehen durch Metadaten

Genau das sehen, was Sie jetzt brauchen

Praktiken

- Prozesse des ISMS
- Strategie, Taktik, Operativ

Handlungsworte

- Tätigkeiten mit Definition
- Mensch oder Maschine

Zielobjekte

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

Hinweise

- Ziele und Definitionen
- Umsetzungshinweise

Stufe

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

Tags

- Querschnittsthemen im Fokus

NIS-2-Richtlinie – Worum geht es?

- rechtliche Maßnahmen zur **Steigerung des Gesamtniveaus der Cybersicherheit** in der EU
- **Einheitliches Sicherheitsniveau** in den Mitgliedstaaten der EU **schaffen und verbessern**
- **Umsetzung** der NIS-2-RL in nationales Recht durch **Änderung des BSI-Gesetzes** im NIS2UmsuCG.
- BSI wird für ca. **29.000** neue "besonders wichtige" (bwE) und "wichtige" Einrichtungen (wE) zur **Aufsichtsbehörde**; die bisherigen regulierten KRITIS werden eine Teilmenge der bwE
- Einführung von **abgestuften Registrierungs-, Meldepflichten** für bwE und wE
- Unternehmen müssen **angemessene, wirksame und geeignete Risikomanagementmaßnahmen** umsetzen

Intensität Regulierung

Wer ist Betroffen?

Betroffenheit – Relevante Kennzahlen

PLUS ggf. Dienstleiter und Lieferanten

Mitarbeitende

Jahresumsatz

Jahresbilanzsumme

≥ 50	oder	> 10 Mio. €	und	> 10 Mio. €	»	**wichtige** Einrichtungen
≥ 250	oder	> 50 Mio. €	und	> 43 Mio. €	»	**besonders wichtige** Einrichtungen

https://www.bsi.bund.de/dok/nis-2-betroffenheitspruefung

Was muss getan werden?

z.B. Risikomanagementmaßnahmen umsetzen

a) Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik

b) Bewältigung von Sicherheitsvorfällen

c) Aufrechterhaltung des Betriebs (BSM)

d) Sicherheit der Lieferkette

e) Sicherer Betrieb
u.a. Management und Offenlegung von Schwachstellen

f) Bewertung der Wirksamkeit von Risikomanagementmaßnahme

g) Sensibilisierung z.B. Schulungen von Geschäftsführer und Personal

h) Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,

i) Materielle Sicherheit z.B. Sicherheit des Personals, Konzepte für die Zugriffskontrolle

j) Sichere Kommunikation z.B. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung

„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbieter."
Quelle: NIS2 UmSG § 30 (2)

Blickwinkel der Lieferkettensicherheit

Beschaffung	• Informationssicherheit von Produkten und Dienstleistungen • Vertragsgestaltung mit Lieferanten • Prüfung und Dokumentation von Anforderungen an die Auswahl von Produkten bzw. Herstellern und Dienstleistern
Dienstleister-steuerung	• Prüfung und Überwachung von Sicherheits-, Prozess- und Vertragsanforderungen • Einhaltung definierter Standards bei Dienstleistungen, • Outsourcing und Cloud-Diensten
Assetmanagement	• Dienstleister und Lieferantenverzeichnis
Entwicklung	• sicheren Software- und Hardwareentwicklung • Dokumentation und Überwachung sicherheitskritischer Ereignisse

Filtern und Verstehen durch Metadaten

Genau das sehen, was Sie jetzt brauchen

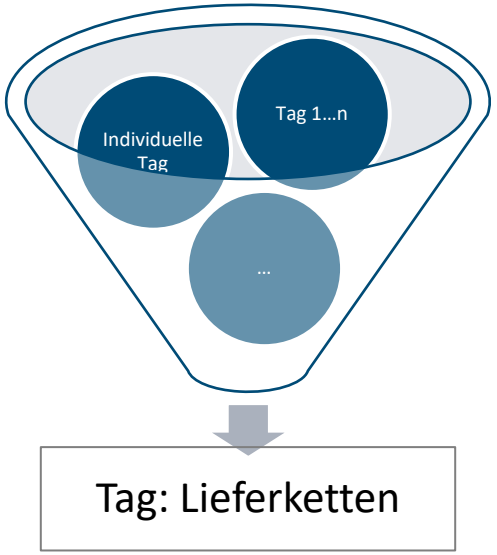
Praktik	Zielobjekt	MODALVERB	Ergebnis	Handlungswort	C	I	A	Hinweis	Tags
Konfiguration	IT-Systeme	SOLLTE	nicht benötigte Funktionen	deaktivieren	5	5	5	Deinstallieren oder Deaktivieren Sie Funktionen, die für Betrieb oder Sicherheit nicht benötigt werden, z.B. ungenutzte Cloud-Anbindungen, Module oder Einstellungen.	Hardening
Sensibilisierung	Benutzende	SOLLTE	die Weitergabe von personengebundenen Authentisierungsmitteln	verbieten	5	5	5	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	5	5	5	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)

Filterfunktionen: Kombination Tags und Handlungswörter

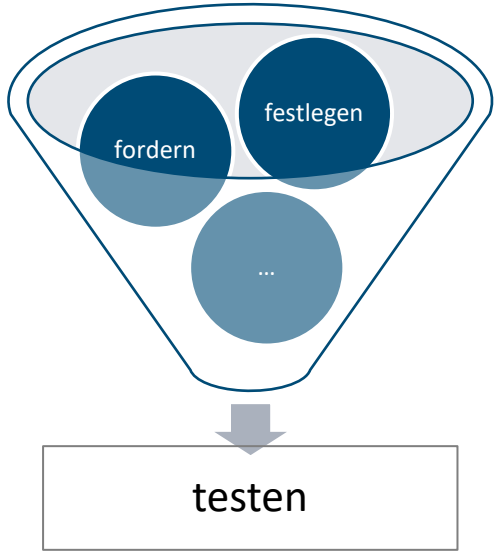
Wie kann die Komplexität reduziert werden?

Lieferkettensicherheit ist ein Querschnittsthema

Daher kann nach dem **Tag „Lieferketten“** über alle Praktiken gefiltert werden.



Ergebnis:
Beschaffung (60 Anforderungen)
Dienstleistung (27 Anforderungen)
Assetmanagement (5 Anforderungen)
Entwicklung (2 Anforderungen)

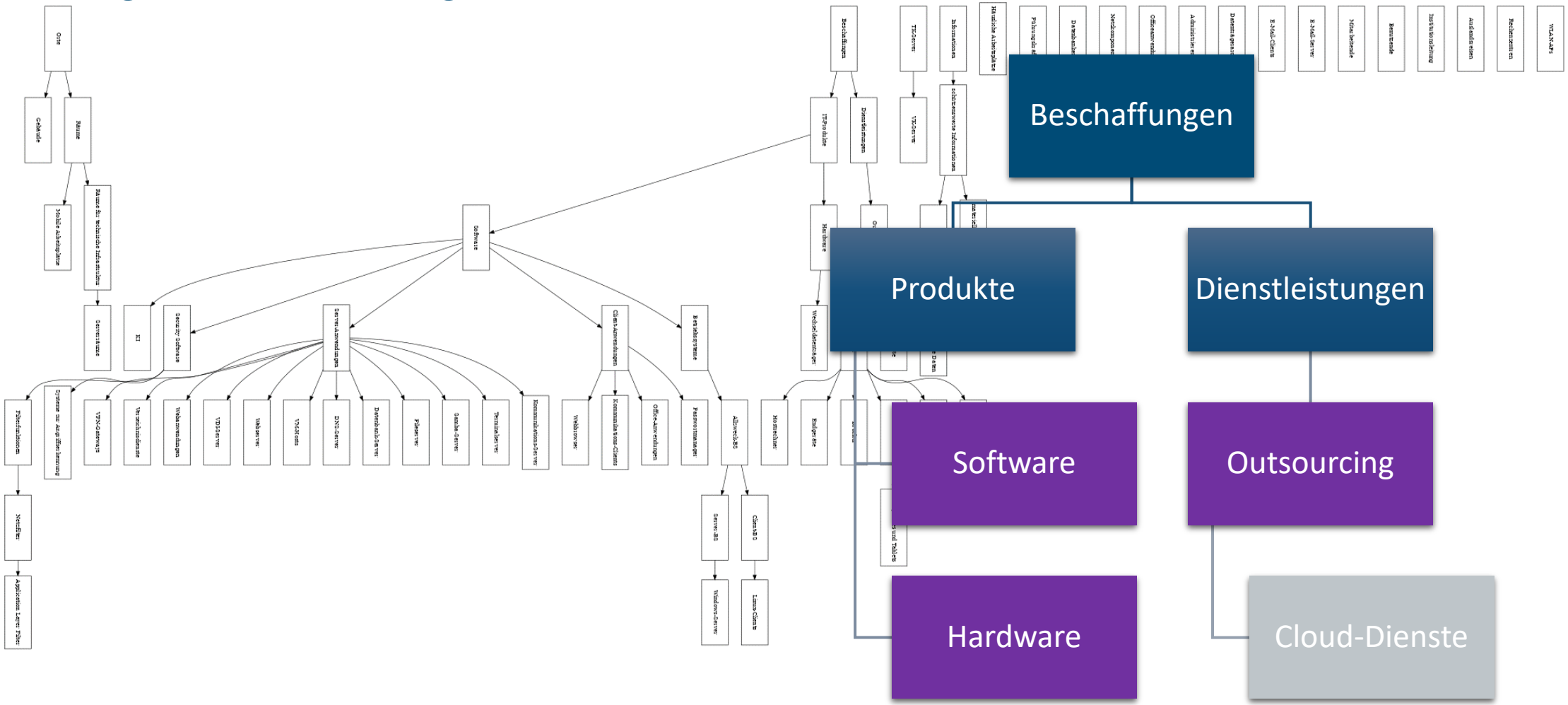


Ergebnis:
5 Anforderungen zum testen

Handlungswörter sind definierte Verben, die die Tätigkeit beschreiben.
Es gibt bisher 18 Prozesswörter nach denen gefiltert werden könnte.

Selektion der Zielobjekte

Vererbung von Anforderungen



Anwendungsmöglichkeiten

Was ist heute möglich und was soll morgen realisiert werden?

Heute

EXCEL

JSON

WiBA Web-Frontend

Kompendiumdokumente

Morgen

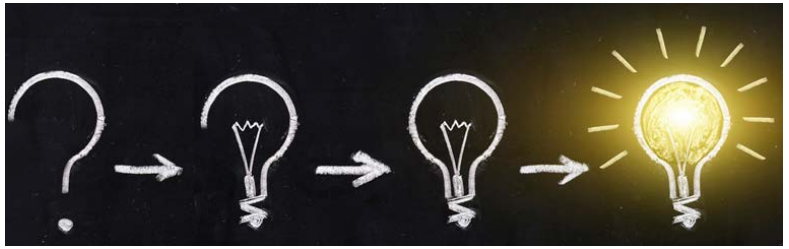
Web-Frontends für

- Kompendium
- Maßnahmen

➔ automatisierter **Stand der Technik**

Bundesamt
für Sicherheit in der
Informationstechnik

Zusammenarbeit



Wie Können Sie bei der Pilotierung mitarbeiten?

Teilnahme an einem digitalen GS++ Beteiligungsworkshop.

Vielen Dank für Ihre Aufmerksamkeit!

Sandra Karger
Referatsleiterin – Stand der Technik

Sandre.Karger@bsi.bund.de
Tel.: +49 (0) 228 9582 5027
Mobil: +49 160 91807974

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Heinemannstrasse 11-13
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: