Deep-Dive ins neue Kompendium

Know-how to go

HiSolutions AG

Benjamin Neweling

Agenda

1. Grenzen des Status Quo
2. Architektur & OSCAL
3. Deep Dive: Die neue Datenlogik
4. Compliance as Code

Benjamin Neweling
Senior Consultant

- Beratung und Begleitung von Unternehmen und öffentlichen Institutionen bei der Einführung und Verbesserung von Informationssicherheitsmanagementsystemen
- Erarbeitung von Sicherheitskonzepten auf Basis von IT-Grundschutz
- Interne Audits und Prüfungen
- Sicherheitsschulungen und -trainings
- Mitarbeit in den Pilotierungsphasen des Grundschutz++

Die Realität heute: Unstrukturierter Text statt prüfbarer Daten

OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung [Fachverantwortliche] (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Protokollierung erstellt werden. In dieser Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie die Protokollierung zu planen, aufzubauen und sicher zu betreiben ist. In der spezifischen Sicherheitsrichtlinie MUSS geregelt werden, wie, wo und was zu protokollieren ist. Dabei SOLLTEN sich Art und Umfang der Protokollierung am Schutzbedarf der Informationen orientieren. Die spezifische Sicherheitsrichtlinie MUSS vom ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Sie MUSS allen für die Protokollierung zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die spezifische Sicherheitsrichtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN dokumentiert werden.

Strukturelle Grenzen des bisherigen Kompendiums

Redundanz

Gleiche Aussage an 4 Orten

- OPS.1.1.5 (MUSS)
- NET.1.2 (SOLLTE)
- SYS.1.9 (SOLLTE)
- INF.14 (SOLLTE)

Widersprüchliche Modalverben für das gleiche Ziel.

Ungleichgewicht

Ungleiche Detailtiefe

- **Server**: 1 Satz (Loggen Sie alles)
- **OPS**: 13 ausführliche Anforderungen.
- **Exchange**: Aktiviere irgendein Logging.

Zufallsprinzip ohne klare Linie oder Kohärenz.

Lücken

Moderne Szenarien fehlen

- Cloud-Native Logging? Fehlt.
- Living-off-the-Land? Unbekannt.
- Tainting/Tracing? Nicht vorgesehen.

Regelwerk hinkt der Bedrohung hinterher.

Auswirkungen der textgetriebenen Struktur

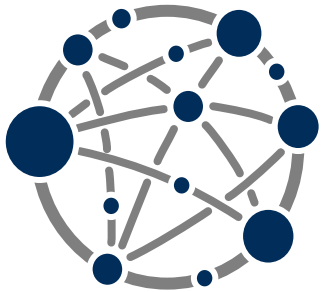
	Warum es für Automatisierung schwierig ist	Konsequenz in der Praxis
Produkt-/Feature-Nennung	▪ Forderungen sind an eine konkrete Plattform/einen Begriff gebunden. ▪ Alternative Umsetzungen sind nicht strukturiert abbildbar.	▪ Alterungseffekt der Anforderungen. ▪ Hoher Pflegeaufwand bei Technologie-Updates.
Unklare Prüfkriterien	▪ Begriffe wie „möglichst streng“ sind nicht messbar. ▪ Ergebnis „erfüllt/nicht erfüllt“ wird interpretationsabhängig.	▪ Auditprogramme werden organisationsspezifisch. ▪ Vergleichbarkeit der Umsetzungen sinkt.
Pflicht & Hinweis vermischt	▪ Normativer Kern und Erläuterung stehen im selben Absatz. ▪ Tools können den Pflichtteil nicht zuverlässig extrahieren.	▪ Manuelle Interpretation in Umsetzung & Audit. ▪ Unterschiedliche Umsetzungstiefen.
Intention nicht explizit	▪ „Wofür“ die Forderung gilt, steht nur indirekt im Text. ▪ Die Ableitung von Aufgabenpaketen/Nachweisen erfolgt manuell.	▪ Maßnahmenlisten werden uneinheitlich. ▪ Nachweise werden uneinheitlich dokumentiert.
Beziehungen/ Abhängigkeiten implizit	▪ Verweise sind textuell („siehe auch …“), nicht als Datenlink. ▪ Cluster/Implementierungspakete entstehen manuell.	▪ Lücken in Umsetzung („haben wir nicht gesehen“). ▪ Synergien werden nicht genutzt.

Die (R)Evolution: „Das Buch“ wird zum Datensatz

Die Vergangenheit (IT-Grundschutz)

- Unstrukturierter Text (PDF)
- Manuelle Übertragung
- Statische Versionierung
- Hoher Pflegeaufwand

Die Zukunft (Grundschutz++)



- Maschinenlesbares Format (**OSCAL**)
- Atomare Anforderungen
- Versionierung via **Git**
- Automatisierte Verarbeitung

OSCAL verwandelt statische Unterlagen in versionierte, maschinenlesbare Daten.

Die gemeinsame Sprache: OSCAL

(Open Security Controls Assessment Language)

Ein vom NIST entwickelter Standard (XML/JSON/YAML) für den Austausch von Sicherheitsanforderungen und -umsetzungen.

Interoperabilität

Werkzeuge verstehen sich blind – Datenaustausch ohne Medienbrüche.

Automatisierung

Audit-Tools können Konfigurationen automatisch gegen Regelwerke prüfen.

Rückverfolgbarkeit

Änderungen in Katalogen und Profilen sind historisch exakt nachvollziehbar.

Das Medium ändert sich radikal, um **maschinelle Verarbeitung** und **Automatisierung** möglich zu machen.

Das Regelwerk als versionierbare Daten (Git + JSON)

- Bereitstellung als OSCAL/JSON (maschinenlesbar)
- Versionierung im Repository: Änderungen nachvollziehbar (Diffs)
- Releases/Tags definieren einen konkreten „Stand“ des Regelwerks
- Grundlage für Import/Sync in Tools und saubere Updates

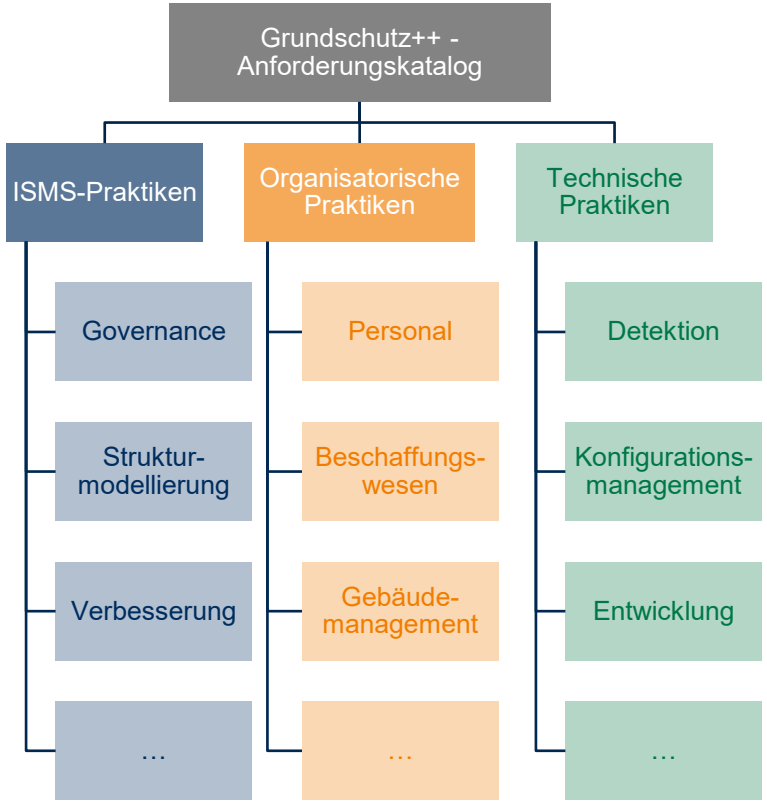
Updates werden planbarer: Anstatt „neues PDF lesen“ → „Änderungen gezielt prüfen“.

Der Katalog als Single Source of Truth

Der Grundschutz++-Anforderungskatalog definiert die **Rohdaten** der Anforderungen.

Anforderungen werden nicht mehr über „Container-IDs“ für mehrere Teilanforderungen, sondern atomisierte, permanente **UUIDs** (alt-identifier) identifiziert.

```
"id": "KONF.6.1.1",
"class": "BSI-Stand-der-Technik-Kernel",
"title": "Datenkapselung",
"props": [
  {
    "name": "alt-identifier",
    "value": "6bb18861-0616-4cde-afed-7929b71ba16c"
  },
```



Der Paradigmenwechsel: Konsolidierung statt Streuung

Die Vergangenheit (IT-Grundschutz)

Protokollierung – OPS.1.1.5

- 1 Hauptbaustein mit 11 Anforderungen bzw. 45 Teilanforderungen.
- Zusätzlich: Zielobjektspezifische Protokollierungsanforderungen in **mehr als 30 weiteren Bausteinen.**

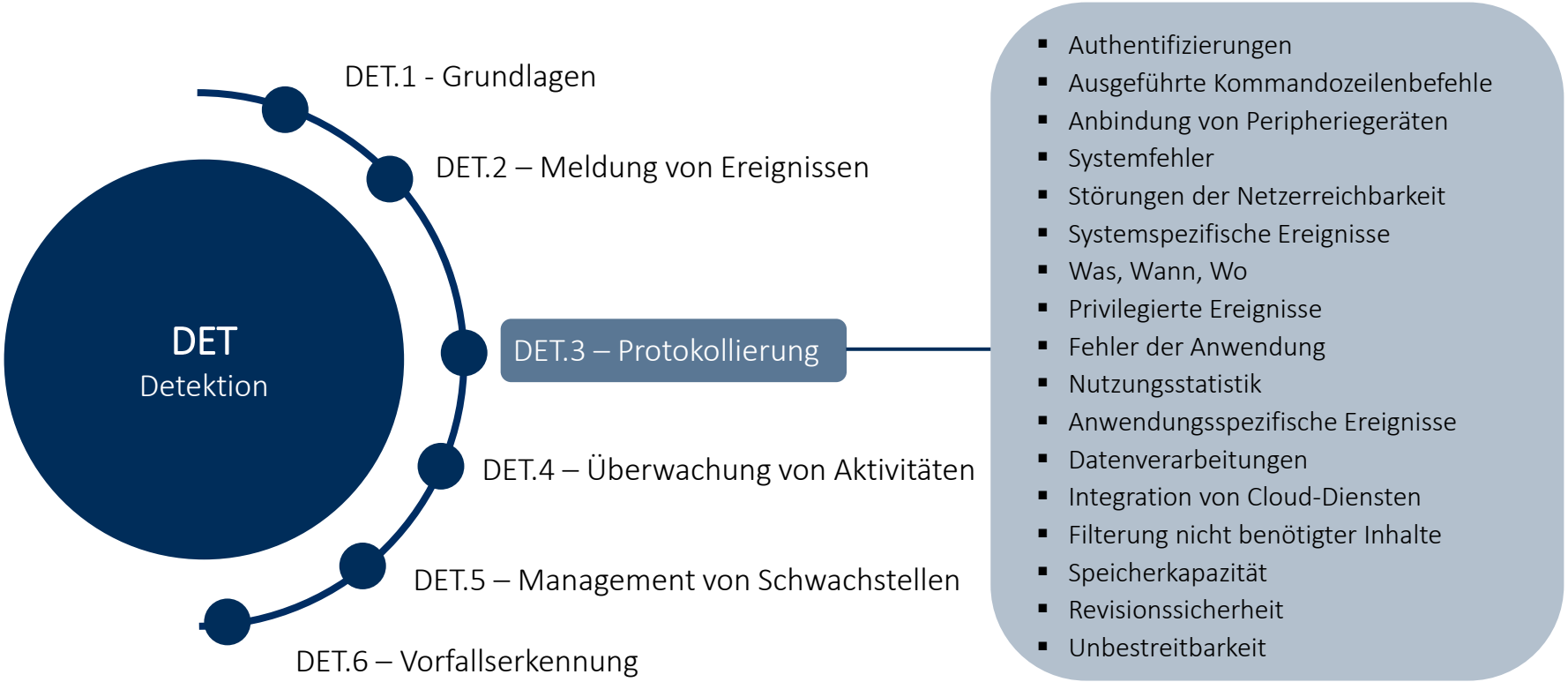
Die Zukunft (Grundschutz++)

Detektion > Protokollierung – DET.3

- 1 Hauptpraktik mit 18 **atomisierten** Anforderungen.
- Zusätzlich: Querverweise aus anderen Praktiken auf DET.3, anstatt Redundanzen aufzubauen.

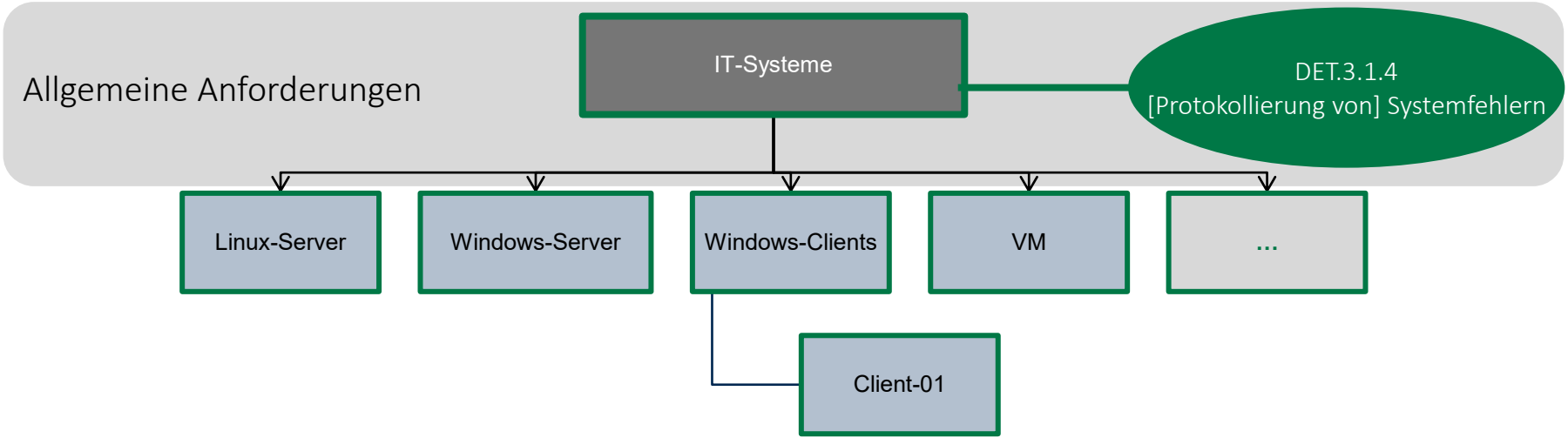
Auflösung der m:n-Beziehungen durch Zentralisierung der Anforderungen in einer atomaren Praktik.

Aufbau einer Praktik am Beispiel DET (Detektion)



Vererbung statt Redundanz

Allgemeine Anforderungen werden auf dem passenden Abstraktionsniveau definiert und dann an alle Unterkategorien vererbt.

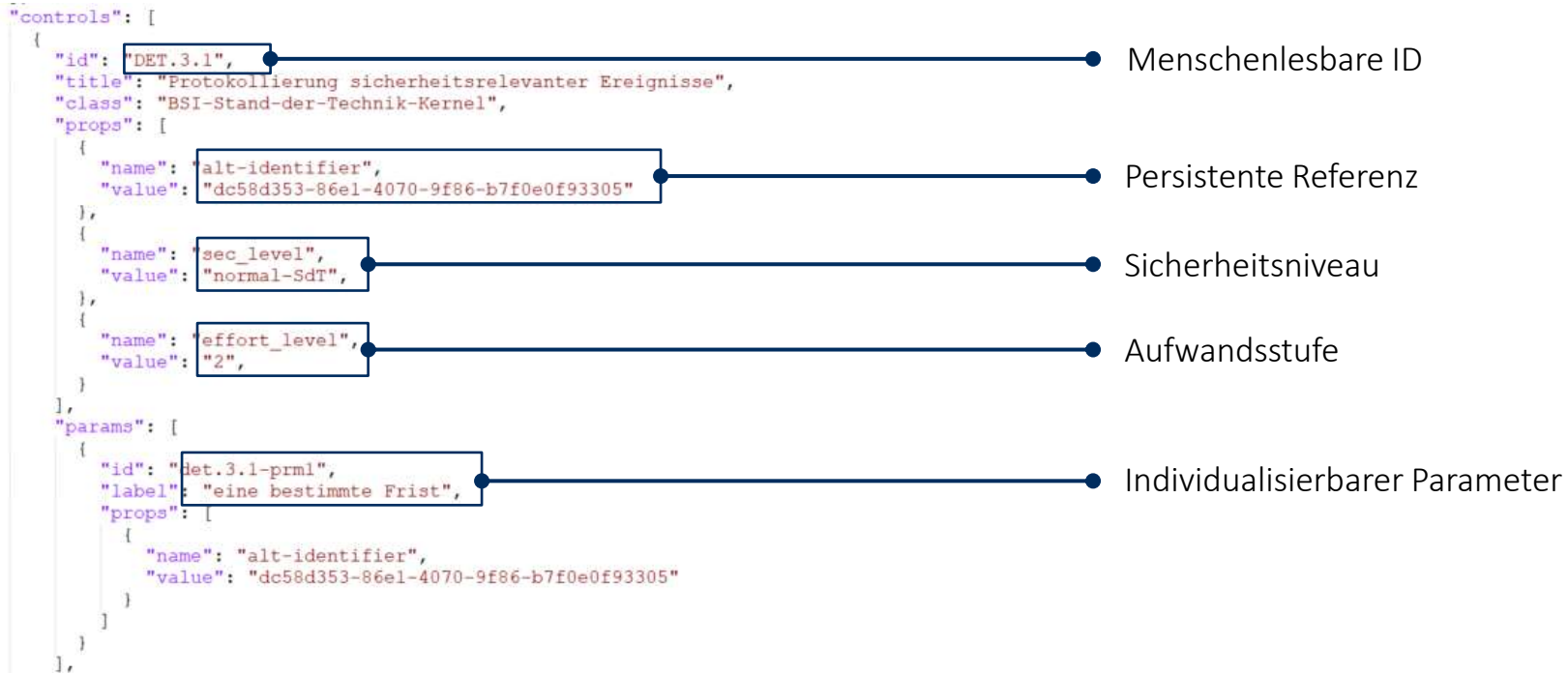


Anforderungen vererben sich entlang definierter Zielobjekt-Hierarchien.

Der Blick in den Code: Eine Anforderung im Rohformat


```
"id": "DET.3.1",
"title": "Protokollierung sicherheitsrelevanter Ereignisse",
"props": [
 { "name": "alt-identifier", "value": "dc58d353-86e1-4070-9f86-b7f0e0f93305" },
 { "name": "sec_level", "value": "normal-SdT" },
 { "name": "effort_level", "value": "2" }
],
"params": [
 { "id": "det.3.1-prm1", "label": "eine bestimmte Frist",
],
"parts": [
{
"id": "DET.3.1_stm",
"name": "statement",
"props": [
 { "name": "target_objects", "value": "Anwendungen" },
 { "name": "documentation", "value": "Detektions-Konzept" },
 { "name": "ergebnis", "value": "Sicherheitsrelevante Ereignisse" },
 { "name": "präzisierung", "value": "mindestens für {{eine bestimmte Frist}}" },
 { "name": "handlungsworte", "value": "protokollieren" },
 { "name": "modalverb", "value": "SOLLTE" }
],
"prose": "Detektion für Anwendungen SOLLTE Sicherheitsrelevante Ereignisse mindestens für {{ insert: param, det.3.1-prm1 }}
protokollieren." },
{
"id": "DET.3.1_gdn",
"name": "guidance",
"prose": "Für die Definition eines Sicherheitsrelevanten Ereignisses, siehe Glossar (Namensräume des Grundschutz++). Relevant sind hierbei
insbesondere die Protokollierung auf zentralen Diensten und Servern. Dazu gehören auch vorhandene Cloud-Anwendungen oder -Dienste. Hier
besteht ein enger Bezug zur Praktik Änderungen und Tests."
```

Anatomie einer Anforderung zur Protokollierung – Teil 1



Anatomie einer Anforderung zur Protokollierung – Teil 2

Die Bausteine einer Anforderung (Props & Namespaces)

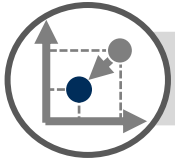
	Definition	Beispiele
Dokumentationsempfehlungen	Arten von Dokumenten, die zum Nachweis der Erfüllung der Anforderungen genutzt werden können.	Freigabeplan, Ergebnisprotokoll, Arbeitsanweisung, Übungsplan, Audit Log
Ergebnis	Enthält das zu erreichende Schutzziel oder den Zielzustand, also den eigentlichen Inhalt der Anforderung.	Vertraulichkeit, Verfügbarkeit, Zugangskonto, Geschäftsprozess, Zutritt, Asset
Handlungsworte	Tätigkeitsarten, die ermöglichen, eine Filterung nach Aktivitäten vorzunehmen.	aktivieren, ausführen, sensibilisieren, überwachen, zuweisen, verschlüsseln, …
Themen	Untergruppen innerhalb einer Praktik, dienen der thematischen Zusammenfassung von Anforderungen.	Abnahme, Bedarfserfassung, Identitätsmanagement, Reaktion, …
Zielobjekte	Von einer Menge an Anforderungen betroffene IT-Produkte, Verträge oder Adressatengruppen.	IT-Systeme, Cloud-Dienste, Führungskräfte, Gebäude, Nutzende, …

Standardisierte Attribute ermöglichen toolgestützte Filterung, Zuweisung und Auswertung.

JSON/OSCAL: Struktur, die Workflows und Auswertungen ermöglicht

Trennung von Pflicht und Hinweis
statement (normativ) vs. guidance (erläuternd)

Nachweise werden adressierbar
Dokumentationsempfehlungen als strukturierte Referenzen



Filter & Priorisierung über Metadaten
props: sec_level, effort_level, tags, modalverb …

Bessere Ableitung von Arbeitslisten
aus Filtern → Tasks, Maßnahmenpakete, Audit-Checks

JSON/
OSCAL

Struktur ersetzt nicht den Inhalt, sondern macht ihn nutzbar (Tooling, Updates, Reports).

Verpflichtende MUSS-Anforderungen im Grundschutz++

ISMS & Governance

- Ersteinrichtung des ISMS
- Analyse der Stakeholder
- Sicherheitsorganisation
- Leitlinie & Freigabe

Risikomanagement

- Einheitliche Methodik
- Kritikalitätskriterien
- Risikoakzeptanzkriterien
- Freigabe durch die Leitung

Strukturmodellierung

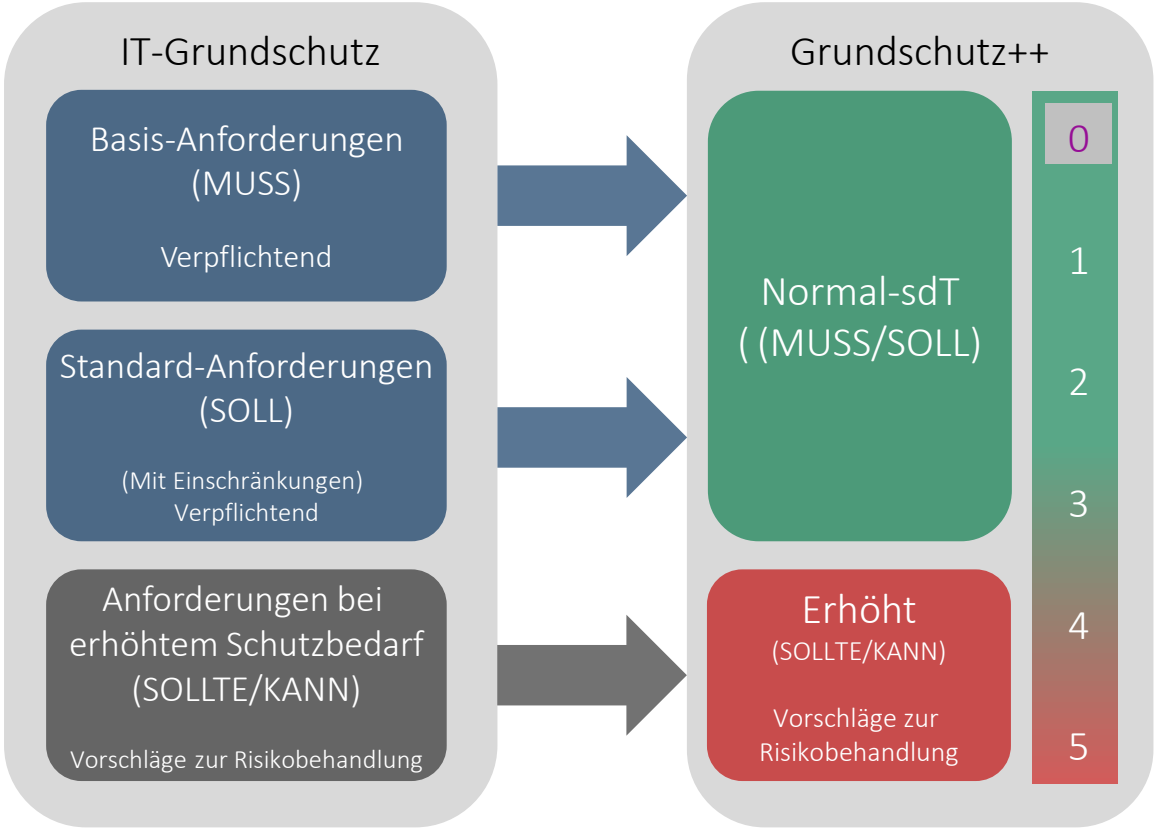
- Anforderungspaket
- Risikobetrachtung
- Umsetzungsplanung
- Freigabeverfahren

Überwachung & Verbesserung

- Auditprogramm
- Managementbewertung
- Nichtkonformitäten
- Korrekturmaßnahmen

Statt organisatorischen/technischen Mindestanforderungen wird das Managementsystem initiiert.

Vereinfachung der Anforderungsstufen



Anforderungen werden nur noch zwischen Normal und Erhöht unterschieden.

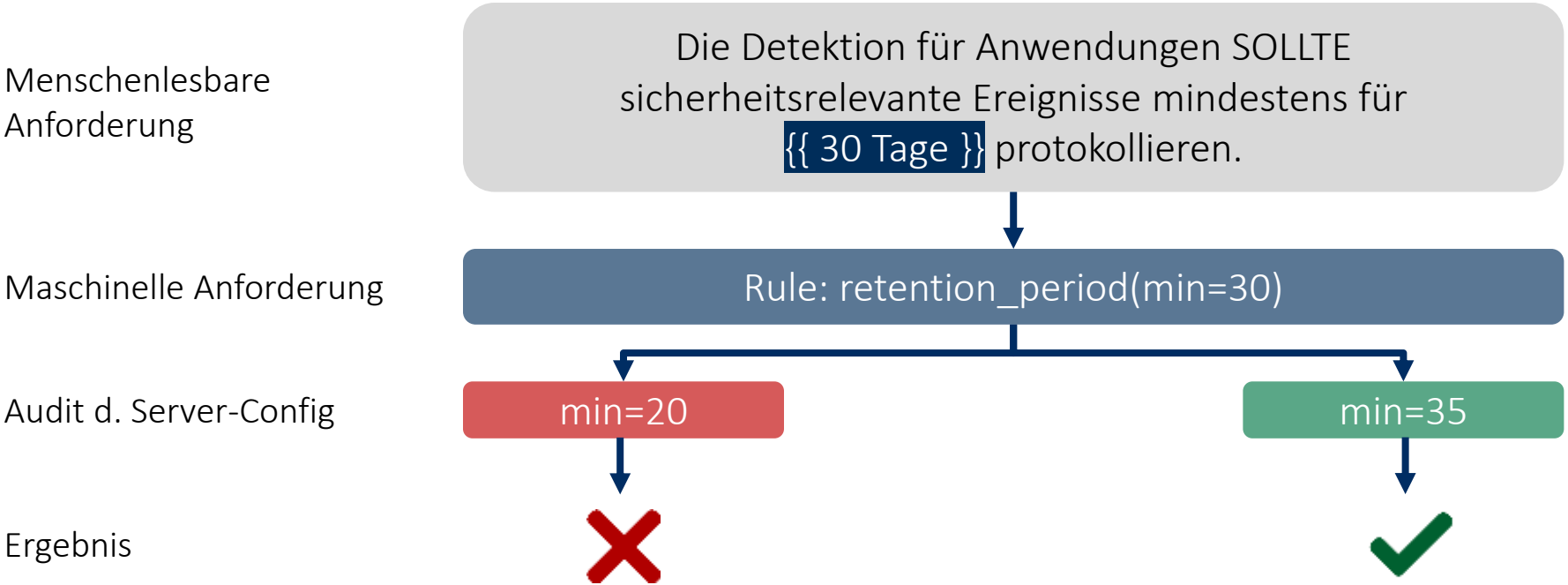
Die Effort-Level 1-5 geben dabei den (vom BSI geschätzten) Aufwand für Umsetzung und Aufrechterhaltung.

Effort-Level 0 bildet die Ausnahme – diese Anforderungen sind verpflichtend umzusetzen.

Die Effort-Level im Detail

	(Zeitlicher) Aufwand	Unterstützungsbedarf	Beispiel
Effort-Level: 0	Keine Bewertung - **Pflichtumsetzung**	Keine Bewertung - **Pflichtumsetzung**	Bestellung eines ISB
Effort-Level: 1	Am selben Tag/mit wenig Aufwand	Mit eigenen Mitteln	Aktivierung einer System-funktion
Effort-Level: 2	Innerhalb einer Woche/geringer Aufwand	Mit eigenen Mitteln	Erstellung eines Konzepts
Effort-Level: 3	Mehrere Wochen bis einige Monate	Zuhilfenahme von externen Dienstleistern	Unterbringung von Systemen im Serverraum
Effort-Level: 4	Längerfristige Umsetzung und Aufwände	Expertenwissen und externe Dienstleister	Initiierung und Umsetzung von Baumaßnahmen
Effort-Level: 5	Aufwändige und komplexe Umsetzung	Expertenwissen und externe Dienstleister	Aufbau georedundantes RZ

Parameter zur Individualisierung der Sicherheitsanforderungen



Anforderungen lassen sich mittels Parameter individualisieren und (automatisiert) prüfen.

Zusammenfassung: Evolution zur Revolution

- Von unstrukturierten PDF-Dateien zu strukturierten Daten im OSCAL-Format.
- Konsolidierung der Anforderungen und starke prozessuale Ausrichtung.

- Atomisierte Anforderungen mit UUIDs und maschinenlesbaren Metadaten.
- Verringerung der Anzahl und der Detailtiefe der umzusetzenden Anforderungen.

- Von manueller Pflege zu Continuous Compliance durch häufige Aktualisierung der Anforderungen und Git-Pipeline.
- Anforderungen sind nun stark prozessorientiert ausgerichtet.

- Compliance soll kein Papierkrieg mehr sein, sondern ein Nebenprodukt eines sicheren IT-Betriebs – **hierfür sind noch methodische und technische Schritte zu gehen.**

Haben Sie Fragen?

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com