Richtlinien sind gefüllte Lückentexte

Vorgabe + Variablen = Richtlinie

Speaker

Thomas Lundström

BSI zertifizierter
„Sicherheitsbeauftragter für die öffentliche Verwaltung“

ISO 27001 Lead Auditor (TÜV Nord)

verinice Partner

Agenda

1) Ausgangssituation
2) ISO 27001
3) BSI IT-Grundschutz / Grundschutz++
4) Lösungsansätze

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), …

Abbildung 1: Dokumentationspyramide

Dokumentenpyramiden

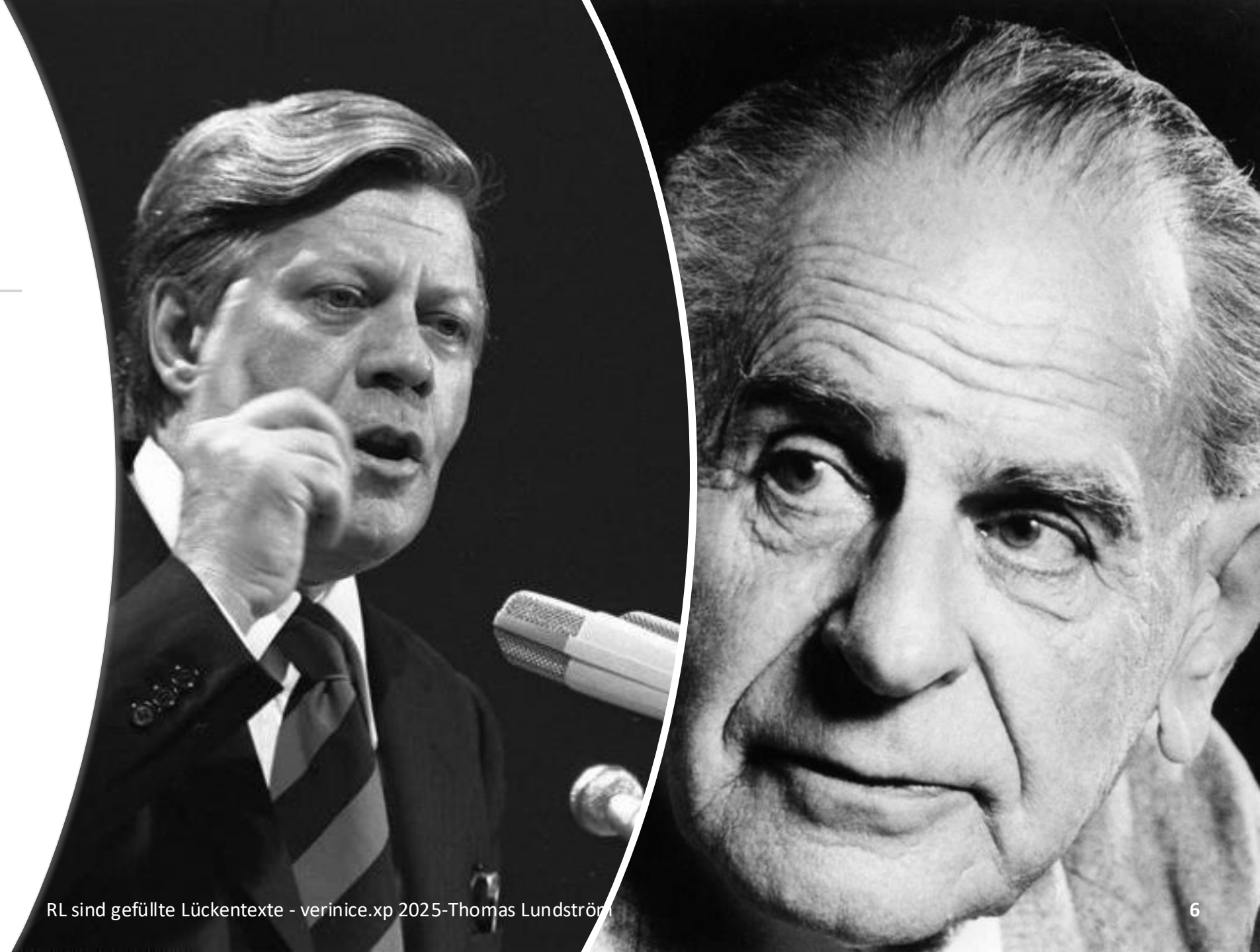
- Strategisch Top
  - KI, **Informationssicherheit**, Cloud
- Strategisch II - Leitlinien
  - Leitlinie Informationssicherheit
  - Datenschutzrichtline
  - …
- Operativ
  - Richtlinie für Backup, Archivierung und Löschung
  - Kryptografie- Richtlinie
  - Richtlinie MuFu & Co.
  - Richtline Serverräume

Strategie - Vision

- "Wer Visionen hat, sollte

  zum Arzt gehen!„

  » ** Vielleicht Helmut Schmidt, vielleicht Karl Popper, vielleicht bei beiden ironisch gemeint.*



"Wer keine Vision hat, hat im Management nichts verloren!„

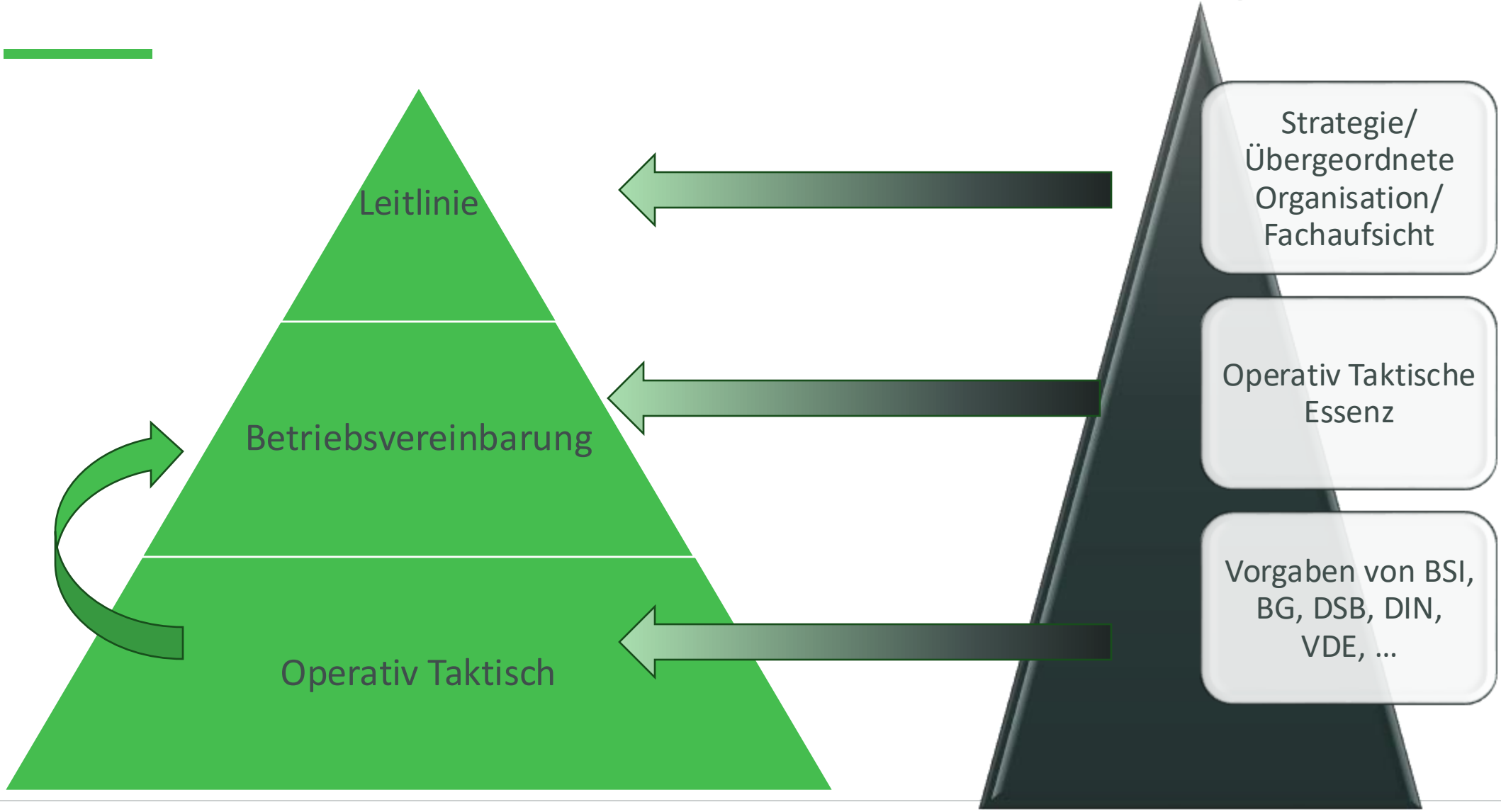
+ Pro

- Treibende Kraft
- Nachweis der Notwendigkeit von Veränderung und Innovation
- Führungsnachweis

- Contra

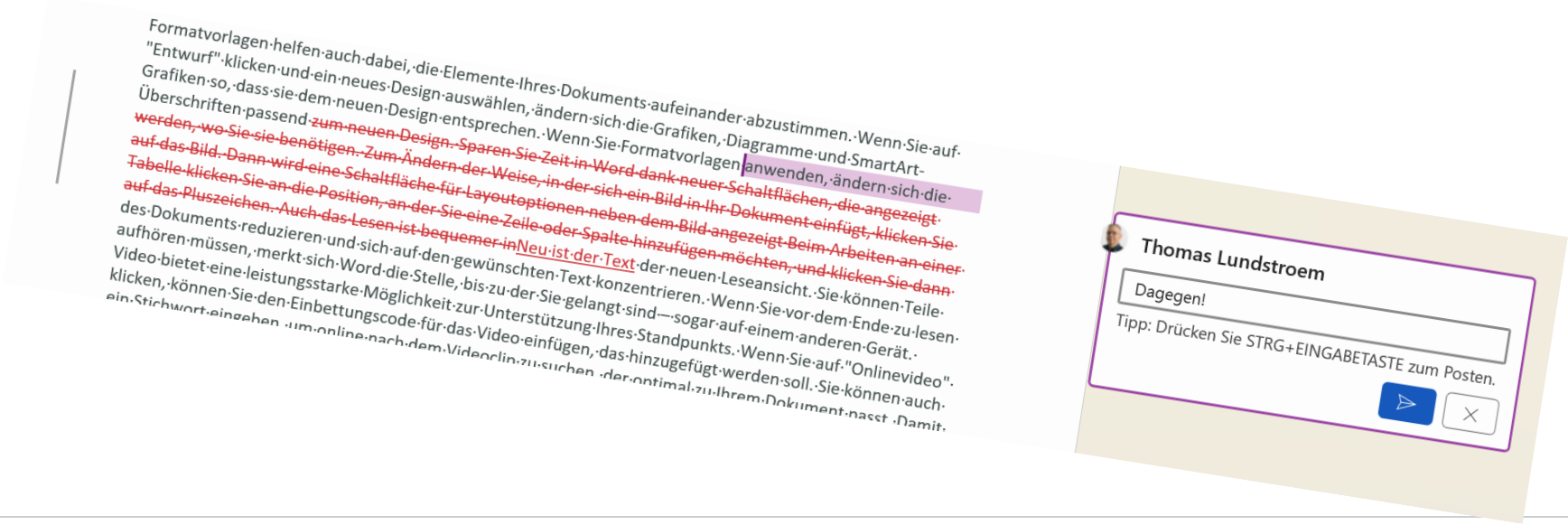
- Realitätsferne
- Kurzfristziele
- Fehlende Verbindung von Vision und Realität

Dokumentenpyramide Öffentliche Verwaltung



Richtlinienerstellung 2024 mit Vorversion

- Überarbeitungsbedarf feststellen
- Diskussion beginnen
- Konsens bilden
- Freigabe starten.



SoftED SYSTEMS

Richtlinienerstellung 2024 from scatch

- Baustein im Kompendium suchen, umformulieren

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.1.A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (B)

Bevor Drucker, Kopierer und Multifunktionsgeräte beschafft werden, MUSS der sichere Einsatz geplant werden. Dabei SOLLTEN folgende Kriterien berücksichtigt werden:

- Unterstützung sicherer Protokolle zur Datenübertragung und Administration,
- Verschlüsselung der abgespeicherten Informationen,
- Authentisierung der Benutzenden direkt am Gerät,
- Nutzung physischer Schutzmechanismen, wie Ösen zum Diebstahlschutz oder Geräteschlösser,
- Existenz eines zuverlässigen und leistungsfähigen automatischen Seiteneinzugs der Scaneinheit,
- Unterstützung geeigneter Datenformate,
- Bei Bedarf Unterstützung von Patch- sowie Barcodes zur Dokumententrennung und Übergabe von Metainformationen,
- Existenz einer Funktion zum sicheren Löschen des Speichers sowie
- Verfügbarkeit von regelmäßigen Updates und Wartungsverträgen.

Es MUSS festgelegt werden, wo die Geräte aufgestellt werden dürfen. Außerdem MUSS festgelegt sein, wer auf die Drucker, Kopierer und Multifunktionsgeräte zugreifen darf. Die Ergebnisse SOLLTEN in einem Basiskonzept dokumentiert werden.

SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte (B)

Der IT-Betrieb MUSS Drucker, Kopierer und Multifunktionsgeräte so aufstellen und absichern, dass nur befugte Personen die Geräte verwenden und auf verarbeitete Informationen zugreifen können. Außerdem MUSS sichergestellt sein, dass nur berechtigte Personen die Geräte administrieren, warten und reparieren können. Mit Dienstleistenden (z. B. für die Wartung) MÜSSEN schriftliche Vertraulichkeitsvereinbarungen getroffen werden.

Drucker, Kopierer und Multifunktionsgeräte MÜSSEN mit Gerätepasswörtern versehen sein, um so den Zugriff auf Webserver und Bedienfeld für die Administration zu sperren. Diese MÜSSEN die Vorgaben des Identitäts- und Berechtigungsmanagements der Institution erfüllen.

Richtlinienerstellung 2024 from scatch

- Regelungsbedarf extrahieren, referenzieren
- Bezeichnung „IT-Betrieb“ durch „Abteilung IT“ ersetzen
- Ergänzung der RL um Fax, Scanner und Officedrucker
- Vormerkung von Details mit Nutzerinteraktion für Betriebsvereinbarung/ Dienstvereinbarung IT

SYS.4.1.A5 Erstellung von Nutzungsrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten (S) [Informationssicherheitsbeauftragte (ISB)]

Für die Institution SOLLTE der oder die ISB eine Nutzungsrichtlinie erstellen, auf der alle Sicherheitsvorgaben zum Umgang mit den Geräten übersichtlich und verständlich zusammengefasst sind. Die Nutzungsrichtlinie SOLLTE allen Benutzenden bekannt sein.

Ergebnis:

- Ausschöpfen Frustrationspotential
- Änderungsbedarfe und Referenzen sind im ISMS zu pflegen

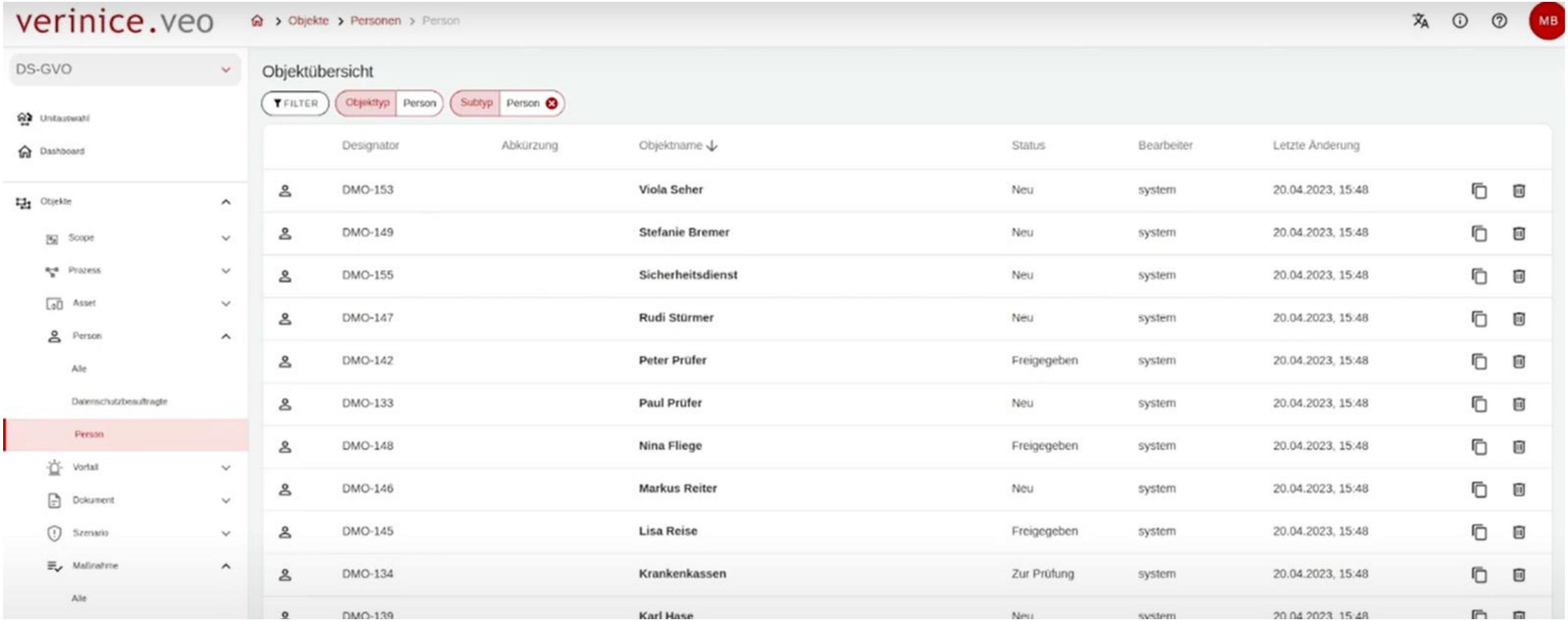
Richtlinienerstellung 2026 from scatch

- Anforderungen an die Richtlinien ergeben sich aus der JSON Datei Grundschutz++.json
- Sprachregeln und Bezeichnungen ergeben sich aus ISMS Tool wie verince.veo
- Gestaltung ergibt sich aus CSS oder DOT Datei
- Referenzieren passiert in der Erstellung

Zutat 1 – Grundschutz++

Stufe	Praktik	Zielobjekt	Modalverb	Ergebnis	Präziser	Handlungswort	C	I	A	Hinweis
1	Planung	MuFu	SOLLTE	sichere Protokolle	besser TLS 1.1	unterstützen	6	6	0	TR-02102-2 e

Zutat 2 Bereiche, Rollen und Personen



SoftED SYSTEMS

Zutat 3 – CD - Gestaltungsregeln

- XML/ JSON bringt den Text und Formatinfos
- CSS/ DOT bringt Schriftart, Farben, Logo

Ergebnis

- ***2.2 → Auswahl·eines·MDM-Produktes·und·Festlegung·erlaubter·↵***

  mobiler·Endgeräte¶

Im·Landesamt·für·Musterlösungen·werden·je·nach·Erfordernis·mobile·Endgeräte·und·Betriebssysteme·für·den·Einsatz·zugelassen.·Nur·Geräte,·die·den·technischen·Sicherheitsanforderungen·und·der·MDM-Strategie·der·Institution·entsprechen,·werden·aufgenommen.·Betriebssysteme·werden·ebenso·regelmäßig·geprüft·und·im·Fall·eines·EOL·durch·den·Hersteller·neu·bewertet.·Das·Mobile·Device·Management·(MDM)·System·wird·so·konfiguriert,·dass·ausschließlich·freigegebene·und·zugelassene·Geräte·Zugriff·auf·institutionelle·Informationen·erhalten.·Bei·der·Auswahl·und·Beschaffung·von·MDM-Software·wird·sichergestellt,·dass·diese·alle·in·der·MDM-Strategie·definierten·Sicherheitsmaßnahmen·umsetzen·kann·und·die·Verwaltung·sämtlicher·zugelassener·mobiler·Endgeräte·unterstützt.·Durch·diese·Maßnahmen·wird·gewährleistet,·dass·nur·sichere,·institutionell·genehmigte·Geräte·verwendet·werden·und·die·Integrität·und·Sicherheit·der·Unternehmensdaten·stets·geschützt·sind.¶

Normverweis:·SYS.3.2.2.·A2·(B)¶

Normverweis:·SYS.3.2.2.·A3·(B)¶

¶

KI - Ergebnistuning

- „Das Landesamt für Musterlösungen“ vs. „Recplast GmbH“
- Leitung IT vs. Abteilungsleitung Bereich 9 vs. Abteilungsleiter X78

Nutzung

- Richtlinien liegen als XML/ JSON vor – Referenziert auf veo
- Freigabepush erzeugt PDF – A Version 3.4
- Freigabeworkflow erzeugt Freigabe-TAG wie „Freigegeben durch Max Muster“ „Zurückgestellt zur erneuten Überarbeitung“ …
- Mit erfolgreicher Freigabe Aktualisierung Praktiken in veo Grundschutz++, DSGVO, …

Grundschutz++ push

- verinice.veo meldet neue, referenzierte github repos
- Überarbeitung wird aus veo angestoßen
- Freigabeprozess wird angetriggert

ToDo

- Relevante Richtlinien als XML bereitstellen
- ISMS – veo API lesen
- RL Stati und Inhalte an veo per API schreiben

Fazit

- „Prosa“ von Richtlinien liegt vor oder kann aus Vorgabe wie BSI-Grundschutz direkt abgeleitet werden
- Globale Variablen sind benennbar und zumeist in verinice.veo abgelegt (Bezeichnung der Organisation, der Organe, der Rollen und handelnden Personen)
- Richtlinienspezifische Variablen wie zugelassene Mobilgeräte, Backupstrategie,… können im Grundschutz –Check / Gap Analyse abgefragt werden
- Ergebnis ist automatisch referenziert – Ready for Audit!

©

- Die Bilder der Folien 5, 10, 13, 14, 17 und 22 wurden von Gemini, einem großen Sprachmodell von Google, erstellt.
- Alle Aussagen in dieser Präsentation beruhen auf einer Reihe von Annahmen die sich naturgemäß in der Zukunft als zutreffend oder nicht zutreffend herausstellen können.
- Ob und welche Funktionen von wem bereitgestellt werden ist noch nicht final entschieden.
- Feedback willkommen.

Vielen Dank für Ihr Interesse. Umsetzungswünsche gern per Mail an:

Thomas Lundström
security@softed.de

www.softed.de

SoftED SYSTEMS