DEVK

Gesagt. Getan. Geholfen.

Sehr hübsch 2.0

Praxiserwartungen an verinice.veo

Thomas Kühr, Fachgebietsleitung ISMS, Februar 2024

IT-Grundschutz-Regelwerk
ist Mittel der Wahl,
ebenso verinice.PRO.

Standards sind Trumpf.

DEVK

Themen

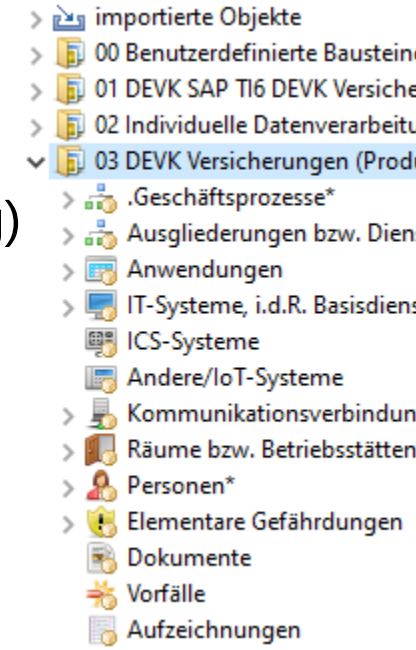
1. DEVK Versicherungen
2. ISMS-Mengengerüst
3. Cloud-Betriebsplattform
4. P e r f o r m a n c e
5. D A T E N M O D E L L
6. B e n u t z e r f r e u n d l i c h k e i t
7. Risikomanagement und -behandlung
8. Informationsverbund, Teilverbünde und individuelle Abgrenzungen
9. Referenzdokumente und B e r i c h t e
10. S a h n e h ä u b c h e n

1. DEVK Versicherungen

DEVK Deutsche Eisenbahn Versicherung Sach- und HUK-Versicherungsverein a.G.
Betriebliche Sozialeinrichtung der Deutschen Bahn

- weitere Sparten bzw. Konzerngesellschaften: Lebensversicherung, Rückversicherung, Rechtsschutzversicherung, private Krankenversicherung, Pensionsfonds und Kapitalanlagen
- seit 135 Jahren, mittlerweile für 4.2 Millionen Kunden
- 7.500 Angestellte bzw. exklusive Vertriebspartner
- 19 Regionaldirektionen bundesweit
- 400 Angestellte als „IT-Funktion“
- Sitz und DEVK-Zentrale in Köln
- IT-Grundschutz-Zertifikat vom BSI für *„IT-Betrieb Basisdienste und KRITIS-Fachanwendungen“*, gültig bis 18. Juni 2026

2. ISMS-Mengengerüst



ISMS-Zielobjekte unserer **Produktionsumgebung**, jeweils ca.:

- 160 Geschäftsprozesslandkarten bzw. Geschäftsprozesse (zur Schutzbedarfsfeststellung)
- 160 „Ausgliederungen“ bzw. Dienstleister
- 400 Anwendungen und Cloud-Services (darunter 32 *plus 2* sog. KRITIS-Anwendungen)
- 100 Basisdienste (sog. IT-Systeme, teilweise gruppiert)
- 15 Kommunikationsverbindungen (stark gruppiert)
- 17 Räume und Betriebsstätten (gruppiert, *„brutto“*)
- 1.000 Personen (Haupt-/Verantwortliche und Konsultierte, verknüpft mit Zielobjekten)
- je Zielobjekt i.d.R. zwei modellierte Bausteine bzw. 30 Anforderungen und 15 Elementargefährdungen

- 570 **IDV-Anwendungen** als „Teilverbund“ abgegrenzt („individuelle Datenverarbeitung“ lt. BaFin)
- 30 **Informationssicherheitsleit- bzw. -richtlinien** als Teil des DEVK-Regelwerks

DEVK

3. Cloud-Betriebsplattform

„Containerisiert“ auf unserer Cloud-Plattform (erste Version 1.19.1, ab 01.07.2020)

- Provider-managed Kubernetes-Cluster
- Anwendungsserver in Docker-Container
- E-Mail-Dienst in weiterem Docker-Container bzgl. Notifikation-Service (Erinnerungen nur einmalig je „GSC-Aufgabe“, d.h. nicht je Sicherheitsanforderung)
- PostgreSQL-Datenbank

Umgebungen fürs „Staging“ (aktuelle Version 1.27.0 „Siargao“, seit 31.01.2024)

1. Entwicklung
2. Vorproduktion
3. Produktion

Benutzer

- Rich-Clients für ISMS-Kernteam, Revision und IT-Architekten
- sonstige Benutzer über Internet-Browser insb. für dezentrale IT-Grundschutz-Checks (GSC)

4. P e r f o r m a n c e

Z ö g e r l i c h …

- Verknüpfen der Zielobjekte untereinander und mit Personen
- insbesondere bei Änderung von Verknüpfungsarten (z.B. „benötigt“ > „nötig für“)
- Änderungen problemlos (auf dem Anwendungsserver)
- aber Aktualisierung der geänderten Client-Darstellung teilweise s e h r s t a r k v e r z ö g e r t
- Referenzdokumente brauchen Zeit … (insb. A.4 IT-Grundschutz-Check ca. 10 min)
- „Konsolidator“ insb. für inflationär modellierten Baustein APP.6 „Allgemeine Software“
- VNA-Dateiexports brechen ab (Timeout)

Das *Tuning* ist ausgereizt.

- Systemausstattung mittlerweile max. 2.500 milliCPU (entspricht 2 ½ physischen Prozessoren) und max. 8 GB Arbeitsspeicher (beides nicht limitierend gemäß Tests „on premises“ mit max. 32 CPU, 64 GB RAM und SSD-Plattenspeicher in RAID-Level 5)
- zusätzliche Datenbank-Indizes für Datenbanktabellen > verlangsamt Schreiben unmerklich aber beschleunigt Abfragen
- Datenbankbereinigung skriptgesteuert, um „verwaiste“ Aufgaben ohne (gelöschten) Personenzuordnung monatlich zu löschen
- Formulierungsänderungen u.a. für Nachrichten des Notification-Service und die [blaue Bestätigungsmeldung] nach Speichervorgängen im Browser

5.1 Datenmodell > Strukturanalyse / Zielobjekte

- **GEMEINSAMES Datenmodell insb.** der Domänen BCM, DSM und ISM hinsichtlich Strukturanalyse bzw. Zielobjekten
- unterschiedliche Werte nur im Sinne der **Herleitung** (ggf. gemäß verschiedener Schutzbedarfs-perspektiven bzw. Managementdomänen)
- **Schutzbedarf** (möglicherweise unterschiedliche „Schutz- bzw. Gewährleistungsziele“; quasi generischste Soll-Anforderungen auf der Metaebene; vgl. folgende Folie)

Ggf. getrennte Schutzbedarfsfeststellungen o.g. **Managementdomänen** müssten im Sinne des für **DIESELBEN Zielobjekte** umzusetzenden **EINEN Sicherheitsniveaus MAXIMERT** werden.

Ableitung des Schutzbedarfs nach:

M	Maximumprinzip
V	Verteilungseffekt
K	Kumulationseffekt
	keine Ableitung

DEVK

5.2 Datenmodell > Schutzbedarfsperspektiven

„Schutzziele“ bzw. Grundwerte gemäß BSI-Standard 200-2 „IT-Grundschutz-Methodik“

1. Vertraulichkeit
2. Integrität *(noch inkl. Authentizität)*
3. Verfügbarkeit (vgl. Zeitkritikalität gemäß BCM bzw. BIA)

„Gewährleistungsziele“ gemäß Standard-Datenschutzmodell (SDM)

1. Datenminimierung
2. Vertraulichkeit
3. Integrität *(noch inkl. Authentizität)*
4. Verfügbarkeit
5. Nichtverkettung
6. Transparenz
7. Intervenierbarkeit

Zum Ersten können die Gewährleistungsziele quantitativ näher bestimmt werden. Beispiele für Präzisierungen sind Antworten auf folgende Fragen: Für welchen Zeitraum ist der Verlust der Verfügbarkeit der Daten für die Betroffenen in welchem Grad tolerabel? Mit welcher Verzögerung soll die Aktualität der Daten garantiert werden? Mit welcher zeitlichen Präzision muss die Verarbeitung im Nachhinein nachvollzogen werden können? In welchem zeitlichen Rahmen muss der Verantwortliche in der Lage sein, die jeweiligen Betroffenenrechte zu gewähren? Wie lange dürfen Daten zu welchen Zwecken verarbeitet werden, bevor diese von der Verarbeitung ausgeschlossen oder gelöscht werden?

6. Benutzerfreundlichkeit

Umsetzungsdefizite und Risikobehandlung

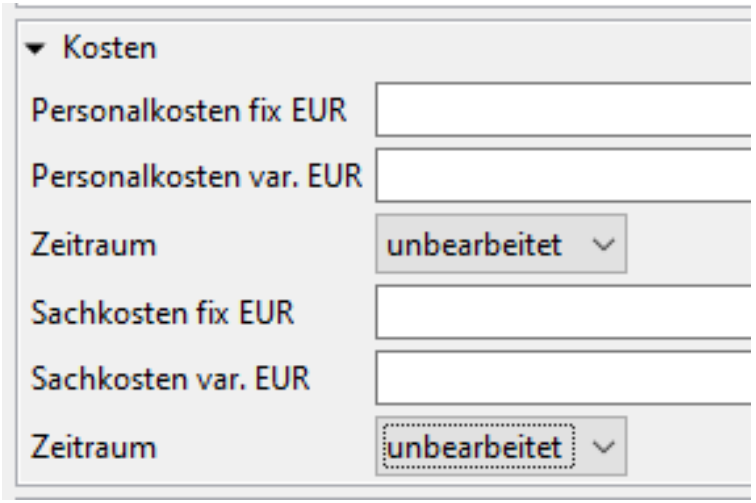
- Aufgabenbearbeitung mittels Internet-Browser ist guter Workaround zur dezentralen ISMS-Dokumentation.
- Schwerpunktaufgabe sind IT-Grundschutz-Checks (GSC) je Zielobjekt durch Fach- und/oder Betriebsverantwortliche.
- Aufgabensortierung leider nur über Anforderungsbezeichnungen, *alphabetisch ansteigend*. (Besser anhand der Anforderungsnummern sowie -klassen „BASIS“, „STANDARD“ und „ERHÖHT“.)
- Umsetzungsstatus „Entbehrlich oder „Nein“, „Teilweise“ und dann „Ja“ sind im Browser nicht visualisiert (Orientierung bzw. Überblick für Adressaten der GSC-Aufgaben mangelhaft).
- Automatische Speicherfunktion fehlt.

DEVK

7. Risikomanagement und -behandlung (Option)

Risikomodell zur wertmäßigen Konsolidierung bzw. Aggregierung

- Risikoverteilung bzw. -zuordnung gemäß Konzernstrukturen bzw. -gesellschaften
- entsprechende DORA-Berichtsanforderungen bzgl. u.a. gesellschaftsbezogenen und übergreifenden Daten zum Sicherheitsniveau (Ist-Stand aktuell)



DEVK

8. Informationsverbund, Teilverbünde und individuelle Abgrenzungen für Abfragen

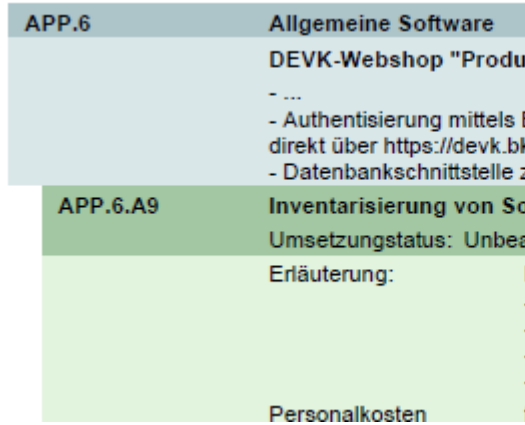
Informationsverbund und Teilverbünde (z.B. für Konzernstrukturen oder/und gemäß Umgebungs-management)

KRITIS-Nachweise unserer Kompositversicherung zu sog. KRITIS-Anwendungen und -Ausgliederungen gemäß BSI-Kritisverordnung für VERTRAGSVERWALTUNG, SCHADENBEARBEITUNG und AUSZAHLUNG

„Basisdienste“ bzw. nicht-fachliche IT-Infrastruktur, insb. bestehend aus (u.U. schichtübergreifend):

- Betriebsplattformen (physische, virtualisierte Server-Gruppen und Cloud-Services),
- Netzwerkkomponenten und Gateways,
- „Systeme zur Angriffserkennung“ (SzA, lt. BSI KRITIS-relevant seit Mai 2023) sowie
- Netzwerkstruktur bzw. -segmente.

9.1 Referenzdokumente und Berichte



Referenzdokumente bitte stets zielobjektbezogen
(nicht von IT-Grundschutz-Bausteinen ausgehend, wie der A.6-Realisierungsplan)!

Berichte flexibel abgrenzbar und gestaltbar bzgl. (über Attribute oder Tagging):

- Informationsverbund bzw. „Produktionsumgebung“ gesamt (Konzernsicht),
- Teilverbünde (KRITIS-Perspektive oder/und für Gesellschaften, Geschäftsfelder bzw. Standorte),
- Zielobjektgruppen (z.B. Gateways und SzA),
- Verantwortlichkeiten (*Zielobjekte meiner Organisationseinheit?*) oder/und
- Status (z.B. „Betrieb“).

Exportfunktionen sind hiervon abzugrenzen!

9.2 Berichtsanforderung (Beispiel / Exkurs)

E-Mail-Zitat vom 19.02.2024:

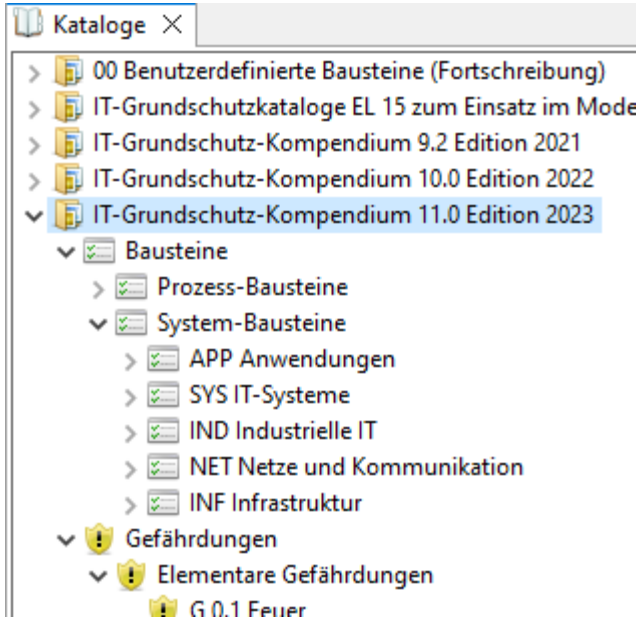
*„Hintergrund ist der zyklische **Informationsbedarf zum Sicherheitsniveau** seitens unseres Vorstands anhand von ggf. detaillierenden **KPI**. Diese würden sich naturgemäß auf unserer **Risikoinventar** beziehen müssen (bislang außerhalb von verinice.PRO), das wiederum **ISMS-Umsetzungsdefizite** zum Gegenstand hat.*

*Die **Informationssicherheitsrisiken** für Umsetzungsdefizite sollten – neben den unabdingbaren **Bruttoverlusten und Eintrittsintervallen** – noch stärker bezüglich ihrer **Schutzzielrelevanz** (perspektivisch lt. BaFin übrigens gerne inkl. Authentizität) und dem entsprechendem **Schutz-bedarf analysiert und berichtet**, bestenfalls visualisiert werden.“*

10. Übergreifende Funktionen und Automatismen

„Sahnehäubchen“ wären:

- **Neumodellierung** künftiger IT-Grundschutz-Editionen vom BSI (denkbar mit SaaS-Releases, zumindest, soweit bisherige Modellierungen fortbestehen) und
- zentral auslösbare **Review-Aufforderungen** an alle mit Zielobjekten „verantwortlich“ verknüpften Personen bzw. Accounts.
- …
- Ausbau der Verzeichnisdienstanbindung (ADDS-Rollen und -Gruppen zur Benutzer-berechtigung sowie „Single Sign-on“)



DEVK

IT-Grundschutz-Regelwerk
ist (noch immer) unser
Mittel der Wahl, ebenso
verinice.*!

DEVK

Gerne zur Nachbereitung!

Thomas Kühr

Fachgebietsleitung ISMS

thomas.kuehr@devk.de

+49 (0)221-757-4597

www.devk.de