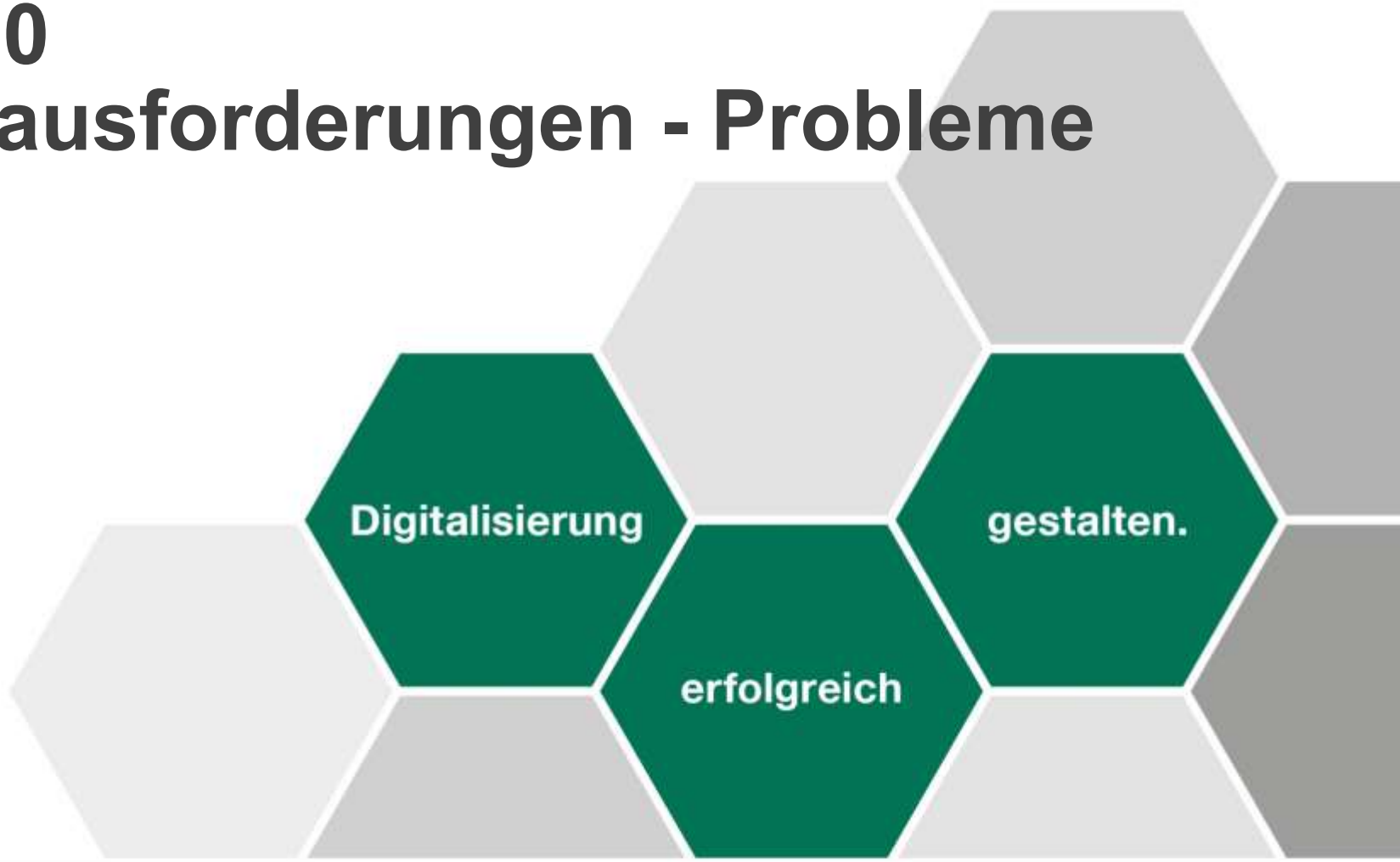
Ein Jahr IT-SiG 2.0
Umsetzung – Herausforderungen - Probleme



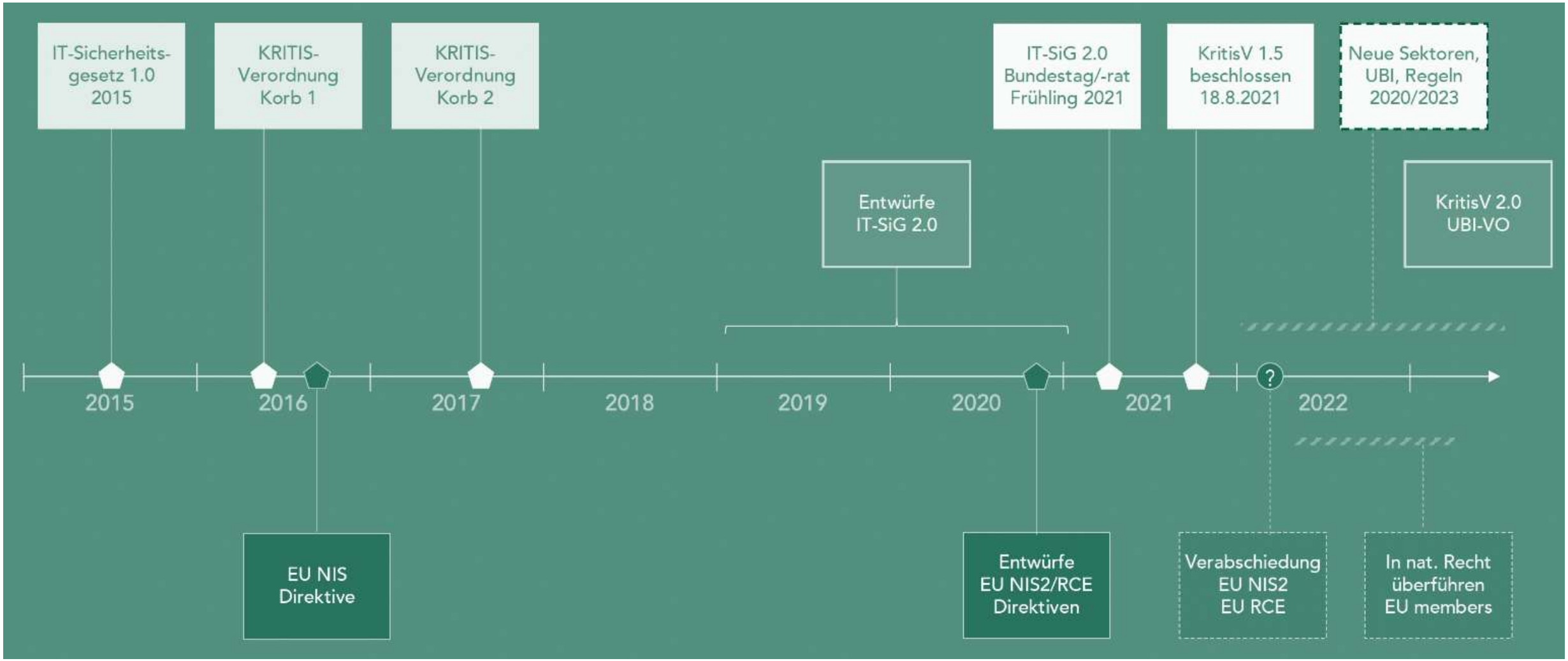
Nico Werner
Head of Cybersecurity

telent
service • commitment • value

Agenda

- Rückblick
- Umsetzungen
- Herausforderungen
- Probleme

Rückblick


IT-Sicherheits-gesetz 1.0 2015
KRITIS-Verordnung Korb 1
KRITIS-Verordnung Korb 2
IT-SiG 2.0 Bundestag/-rat Frühling 2021
KritisV 1.5 beschlossen 18.8.2021
Neue Sektoren, UBI, Regeln 2020/2023
Entwürfe IT-SiG 2.0
KritisV 2.0 UBI-VO
2015
2016
2017
2018
2019
2020
2021
?
2022
EU NIS Direktive
Entwürfe EU NIS2/RCE Direktiven
Verabschiedung EU NIS2 EU RCE
In nat. Recht überführen EU members

Rückblick

Neue Pflichten KRITIS-Betreiber

Angriffserkennung
Neue Meldepflichten
Kritische Komponenten
Unmittelbare Registrierung

Mehr betroffene Unternehmen

KRITIS-Sektor Entsorgung
Unternehmen im besonderen öffentlichen Interesse
Niedrigere Schwellenwerte (↓ 6)
Mehr Anlagen (+17)

IT-SiG 2.0

Mehr Befugnisse für das BSI

Zentrale Meldestelle
Tiefere Untersuchungen
Schutz der Bundesnetze
Mehr Personal

Sanktionen und Verbraucherschutz

Höhere Sanktionen für Betreiber
Mehr mögliche Verstöße
Neue Gütesiegel

Umsetzung

Bestehende KRITIS-Betreiber	Neue Betreiber & Entsorger	KRITIS Telekommunikation	UBI/UNBÖFI
Angriffserkennung SIEM SOC	KRITIS-Anlagen identifzieren	Kritische Kompo-nenten identifizieren	Als UNBÖFI beim BSI registrieren
ab 2023			ab 2021/23/24
Neue KRITIS-Anlagen prüfen	Als KRITIS beim BSI registrieren	Krit. Komponenten melden & freigeben	Cyber Security umsetzen
			ab 2023/24
Tiefere Schwellen-werte prüfen	Cyber Security umsetzen		Meldepflichten ans BSI
			ab 2021/23/24
Neue Meldepflichten ans BSI	Meldepflichten ans BSI		Alle: Auf EU Regulierung vorbereiten
			from ~2022

Umsetzung – Angriffserkennung

- Innerhalb von zwei Jahren müssen
  - Systeme zur Angriffserkennung (IDS/IPS) nach **Stand der Technik** eingeführt werden
  - Monitoring (SIEM/SoC) der kritischen Komponenten
  - Patchen durch der BSI muss gewährleistet werden
  - Auch Hersteller und Systemintegratoren sind im „Boot“
  - Zertifizierung von Herstellern bei kritischen Komponenten

- BSI veröffentlicht (06/22): Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung inklusive Formulare für den Nachweis zu § 8a (1a) BSIG und § 11 (1d) ENWG
- Aufgabenbereiche: Protokollierung, Detektion und Reaktion

Umsetzung - Katalog von Sicherheitsanforderungen 2.0

Bundesnetzagentur

Themen Verbraucherservice Bundesnetzagentur Presse

Telekommunikation | Anbieterpflichten | Öffentliche Sicherheit | Katalog Sicherheitsanforderungen

Katalog von Sicherheitsanforderungen

Nach § 109 Absatz 6 Satz 1 TKG hat die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Version 2.0 des Kataloges von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach § 109 Absatz 4 TKG erstellt.

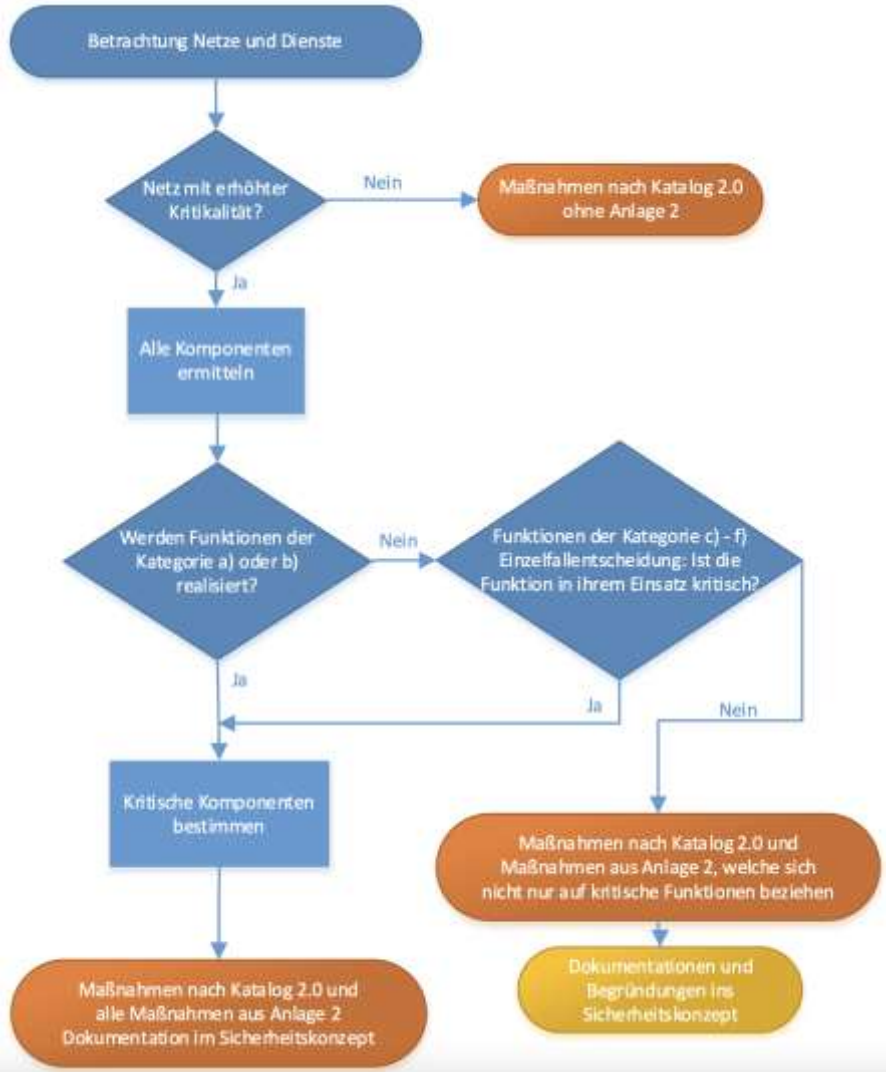
Der Katalog wurde gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1) notifiziert. Das Verfahren ist abgeschlossen und der Katalog von Sicherheitsanforderungen **Version 2.0** ist mit der Veröffentlichung im Amtsblatt Nr. 24 der Bundesnetzagentur **am 23.12.2020 in Kraft getreten**. Er enthält Anpassungen gegenüber der Vorgängerversion aufgrund technischer Entwicklungen und aktueller Sicherheitsbelange. Die Verpflichteten haben die Anforderungen des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, soweit im Katalog keine speziellen Übergangsregelungen genannt sind.

Katalog von Sicherheitsanforderungen (Version 2.0) (pdf / 1 MB)

Im Zusammenhang mit der Notifizierung steht der Katalog ebenfalls in englischer Sprache unter folgendem Link zur Verfügung:
https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2020&num=496

- Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten überarbeitet

Umsetzung - Katalog von Sicherheitsanforderungen 2.0



- Prozess zur Identifikation von kritischen Komponenten im konkret betriebenen Netz oder erbrachten Dienst

Herausforderungen

Angriffserkennung

- Systeme zur Angriffserkennung
- Verpflichtender Einsatz von Systemen und Prozessen
- → SOC, SIEM, Auswertungen

Meldepflichten

- Mehr Meldepflichten ans BSI
- Informationen bei erheblichen Störungen zur Bewältigung
- Auch personenbezogene Daten

Komponenten

- Kritische Komponenten in KRITIS-Anlagen
- Nur mit Genehmigung durch das Innenministerium
- Bisher nur im TK-Sektor

Registrierung

- Unmittelbare Registrierung beim BSI als KRITIS-Betreiber
- Bennennung Kontaktstelle
- BSI darf Betreiber auch selbst registrieren

telent

Herausforderungen

Mehr Tatbestände

- 17+ Tatbestände im IT-SiG 2.0 definiert
- Vorsätzliche oder fahrlässige Verstöße gegen Vorgaben = Ordnungswidrigkeit
- Fehlende KRITIS-Nachweise, fehlende Registrierung, fehlende Maßnahmen ...

Höhere Bußgelder

- Deutlich erhöhte Bußgelder für die o.g. Ordnungswidrigkeiten
- Zwischen 100 Tsd. und 2 Mio. EUR
- Bis zu 20 Mio. für jur. Personen (Organe)

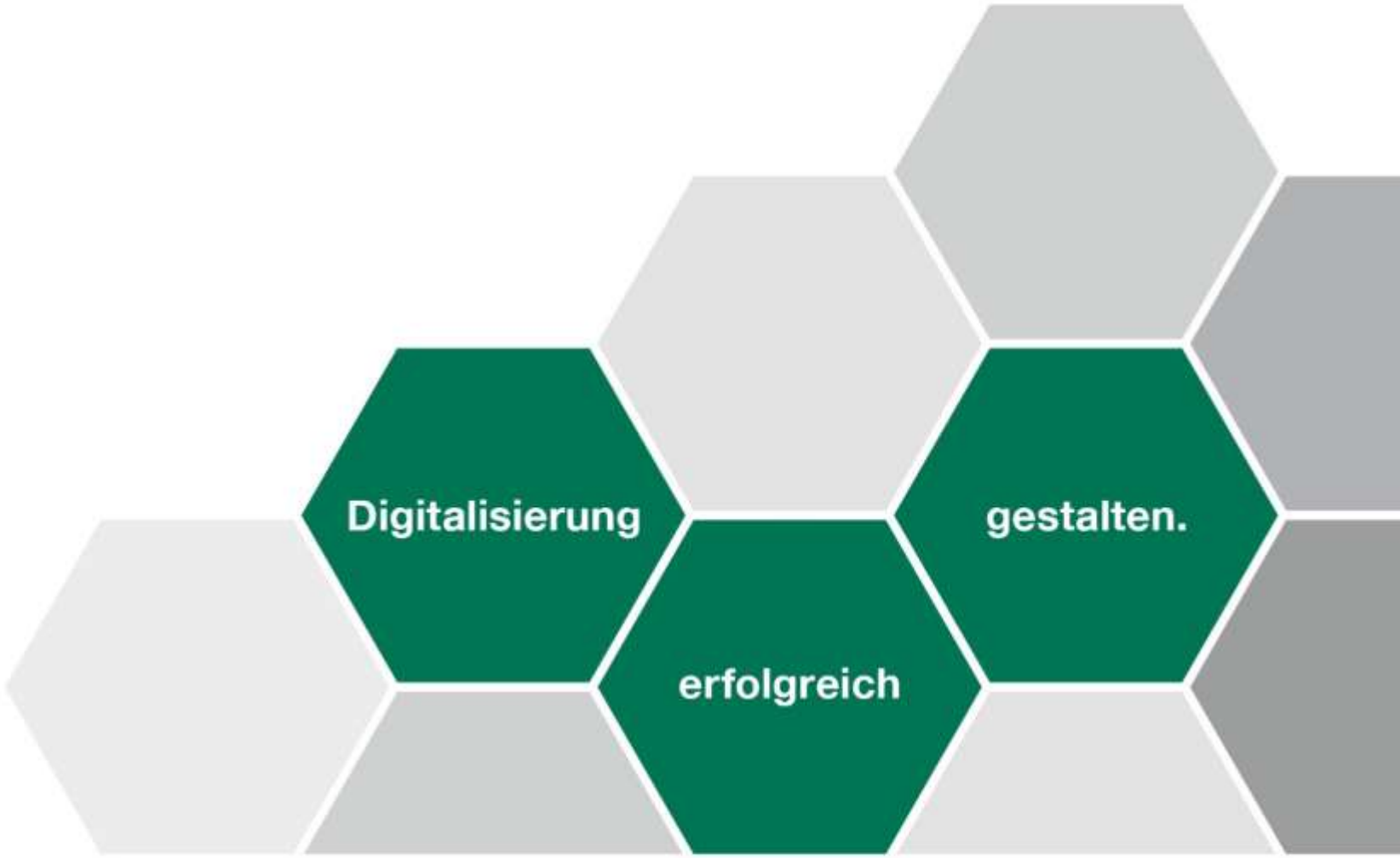
Probleme

- Fehlende Dokumente / Prozesse
  - Liste kritischer Komponenten (§9b, §2 (13))
    - **Aktuell nur für den Sektor Telekommunikation**
  - Garantieerklärung
    - **Kein gelebter/definierter Prozess/Vorgabe**
    - **Erster Entwurf von der BNetzA wurde zurückgezogen**

- Mehr Befugnisse für den Staat (§3)
  - Tiefere Untersuchungen (§7a, §7b, §7c)
    - Portscans, Patching und Abwehr – **Noch keine Prozesse definiert / Rechtlichkeit wird geprüft!**
  - Stärkerer Schutz der Bundesnetze (§4a, §5a, §8)
  - Neue Zertifizierungen – **Noch keine Prozesse definiert!**
  - Mehr Personal

Fazit

- Vieles ist noch offen nicht geklärt!
- Technisch/Orga Maßnahme müssen bis zum 1. Mai 2023 umgesetzt werden
  - Meldepflichten
  - Angriffserkennung
  - Komponenten
  - Registrierung



Kontaktdaten:
Nico Werner
Head of Cybersecurity
Tel. 0151 65255796
Mail: nico.werner@telent.de

telent
service • commitment • value