OPENKRITIS

Notfallmanagement in Kritischen Infrastukturen

OpenKRITIS · 29. April 2022

Agenda heute

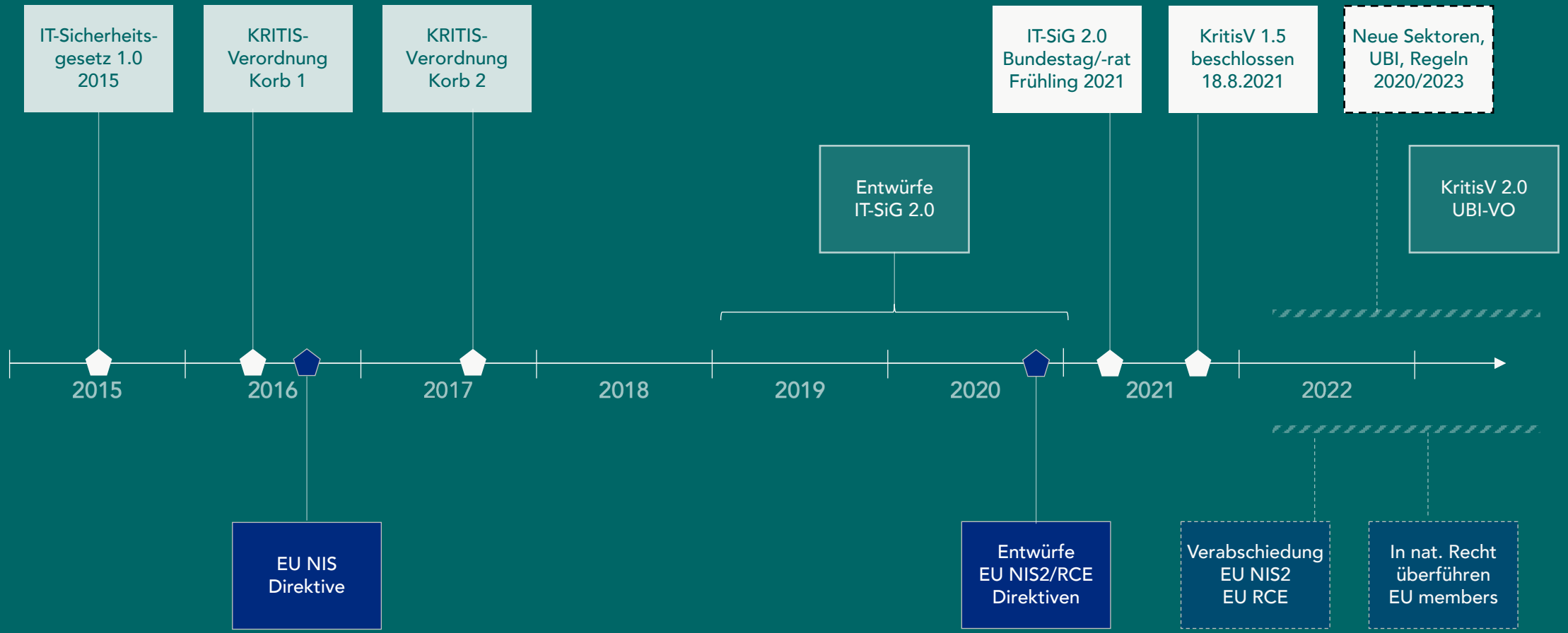
1. Kritische Infrastrukturen
2. Business Continuity
3. Diskussion und Austausch

- KRITIS-Anforderungen
- BCM in KRITIS

Kritische Infrastrukturen

OPENKRITIS

IT-Sicherheitsgesetz 2.0 und KRITIS



IT-Sicherheitsgesetz 2.0 und KRITIS

Anforderungen an Kritische Infrastrukturen

Basierend auf dem IT-Sicherheitsgesetz 2.0 und BSIG von 2021.

Identifikation	Registrierung	Meldepflichten	Cyber Security	Prüfungen
• In KRITIS-Sektor tätig? • Erbringe ich eine Kritische Dienstleistung? • Was ist meine Anlage? • Was ist alles KRITIS? • Welche Schwellenwerte?	• Nach Identifikation als Kritischer Infrastrukturen • Registrierung beim BSI als KRITIS-Betreiber • Eigene KRITIS-Anlagen, Ansprechpartner, Prüf-Zyklus	• Erkennung von Vorfällen in der KRITIS-Anlage • (Die zum Ausfall der kDL führen können/stören) • Meldung an das BSI • Vorfallsbearbeitung und Informationsaustausch	• Umsetzung Maßnahmen nach Stand der Technik • Im Geltungsbereich der KRITIS-Anlage • Sicherheitsmanagement, ISMS, techn. Maßnahmen • Angriffserkennung	• Nachweis der Umsetzung der Maßnahmen • „BSIG §8 Prüfung“ • Alle zwei Jahre durch externen Prüfer • Ergebnisse ans BSI mit Transparenz & Fragen
Geltungsbereich	Betreiber ID beim BSI	Austausch mit BSI	Risiko-Management	Compliance

und noch:
EU NIS2
EU RCE

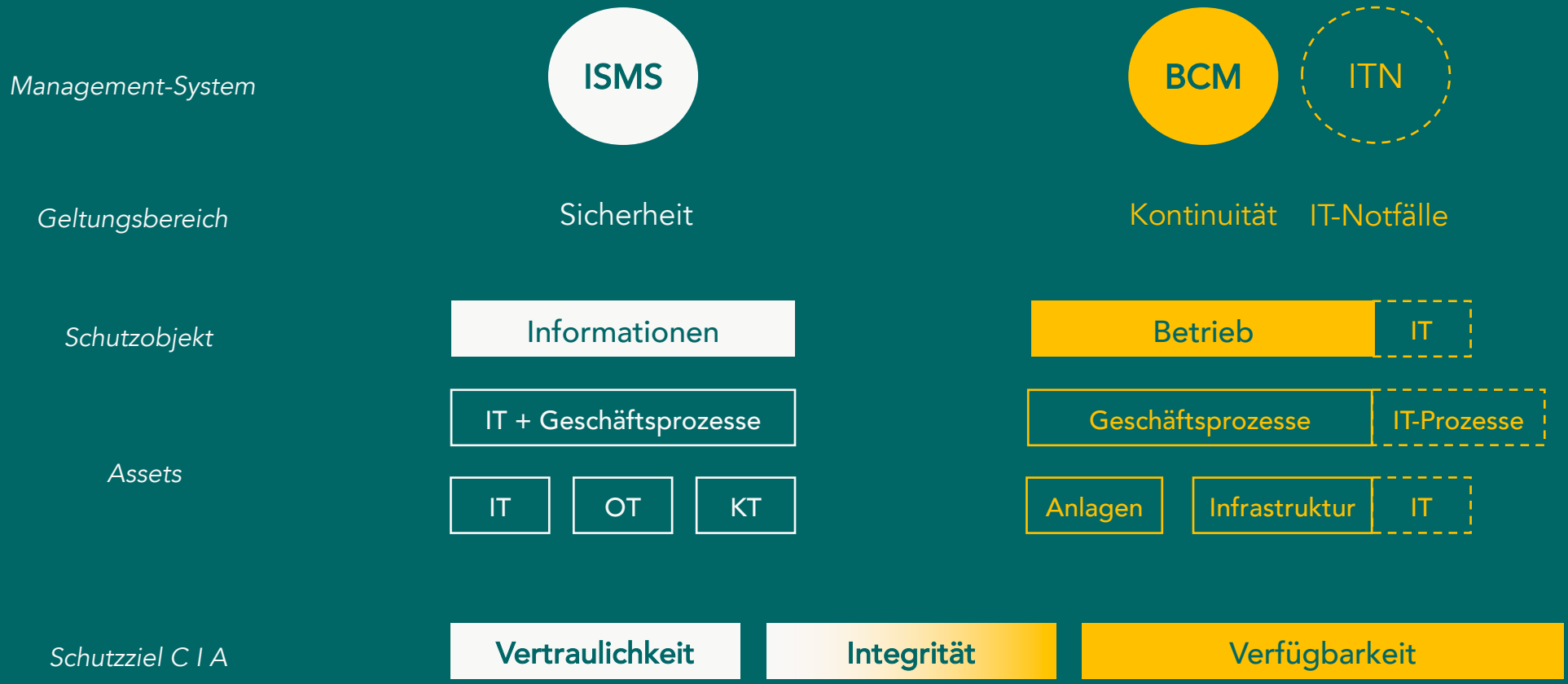
Kommende EU-Regulierung

	EU RCE	EU NIS2	IT-SiG 2.0 (DE)
Sektoren	10 Kritisch	10 Essentiell 6 Wichtig	8 Kritisch KRITIS 3 Wichtig UBI
Betreiber	Durch Regierungen festgelegt Entities an EU gemeldet	Mittlere und große Firmen Teilweise Register mit ENISA	Schwellenwerte mit Selbst-identifikation der Betreiber
Maßnahmen	Für *kritische Dienste*: a. Prävention b. Physische Sicherheit c. Krisenmanagement d. BCM und Zulieferer e. Personelle Sicherheit f. Awareness	For *Netzwerke und IT-Systeme*: a. Policies b. Vorfallsmanagement c. BCM & Krisenmanagement d. Lieferketten-Sicherheit e. Tests und Audit f. Kryptographie	Für IT in KRITIS-Anlagen: a. Sicherheitsorganisation b. Stand der Technik c. Angriffserkennung d. Kritische Komponenten
Meldungen	Vorfallsmeldungen Risiko-Analyse und Pläne	Vorfallsmeldungen	Identifikation u. Registration Vorfallsmeldungen KRITIS Geltungsbereich Nachweisprüfung
National	Behörde für Resilienz	Cyber-Behörde und CSIRT	BSI

Business Continuity

BCM in Cyber Security

Illustrative Darstellung



Business Continuity Werkzeuge

Vereinfachte Darstellung

a	**Analysen**	**Kritikalität von Geschäftsprozessen** ▪ Werkzeuge ▪ Methoden ▪ Risikoanalyse: BIA, RIA
b	**Pläne**	**Pläne und Vorbereitung** ▪ Notfallpläne ▪ Wiederanlauf/Wiederherstellung ▪ Übungen
c	**Reaktion**	**Management von Vorfällen, Notfällen, Krisen** ▪ Rollen ▪ Arbeitsstäbe ▪ Tools
d	**IT-Notfälle**	**Management von IT-Notfällen** ▪ IT-Reaktion ▪ Prävention und Governance

BCM in KRITIS

OPENKRITIS

KRITIS-Pflichten und BCM

Anforderungen an Kritische Infrastrukturen

BCM-Methoden für KRITIS.

Identifikation	Registrierung	Meldepflichten	Cyber Security	Prüfungen
• In KRITIS-Sektor tätig? • Erbringe ich eine Kritische Dienstleistung? • Was ist meine Anlage? • Was ist alles KRITIS? • Welche Schwellenwerte?	• Nach Identifikation als Kritischer Infrastrukturen • Registrierung beim BSI als KRITIS-Betreiber • Eigene KRITIS-Anlagen, Ansprechpartner, Prüf-Zyklus	• Erkennung von Vorfällen in der KRITIS-Anlage • (Die zum Ausfall der kDL führen können/stören) • Meldung an das BSI • Vorfallsbearbeitung und Angriffserkennung	• Umsetzung Maßnahmen nach Stand der Technik • Im Geltungsbereich der KRITIS-Anlage • Sicherheitsmanagement, ISMS, technische Cyber Security Maßnahmen	• Nachweis der Umsetzung der Maßnahmen • „BSIG §8 Prüfung“ • Alle zwei Jahre durch externen Prüfer • Ergebnisse ans BSI mit Transparenz & Fragen
Geltungsbereich	Betreiber ID beim BSI	Meldungen ans BSI	Gemanagte Risiken	Compliance

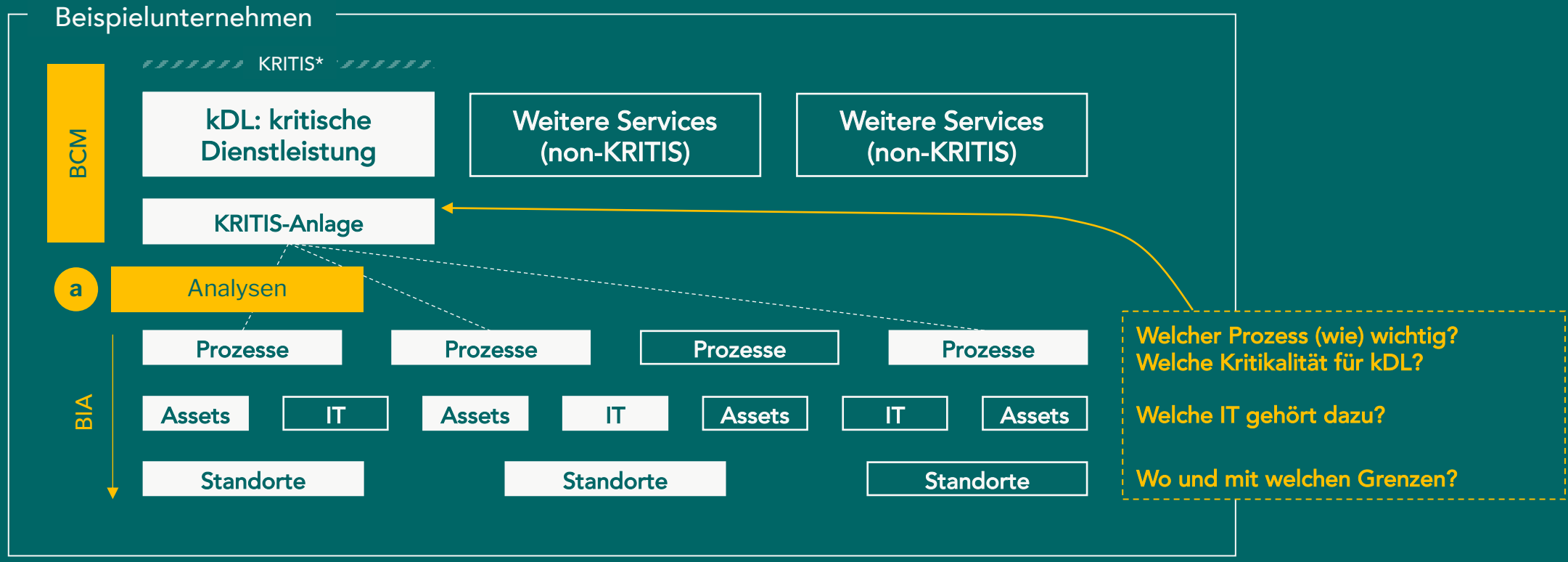
- a Analysen
- a Risiken
- b Pläne
- c Reaktion
- d IT-Notfälle
- a Risiken
- b Pläne

OPENKRITIS

Identifikation KRITIS mit BCM

Was im Unternehmen ist eigentlich KRITIS?

BSI Orientierungshilfe Nachweise, Anhang C: Anforderungen Geltungsbereich (G01-G13)

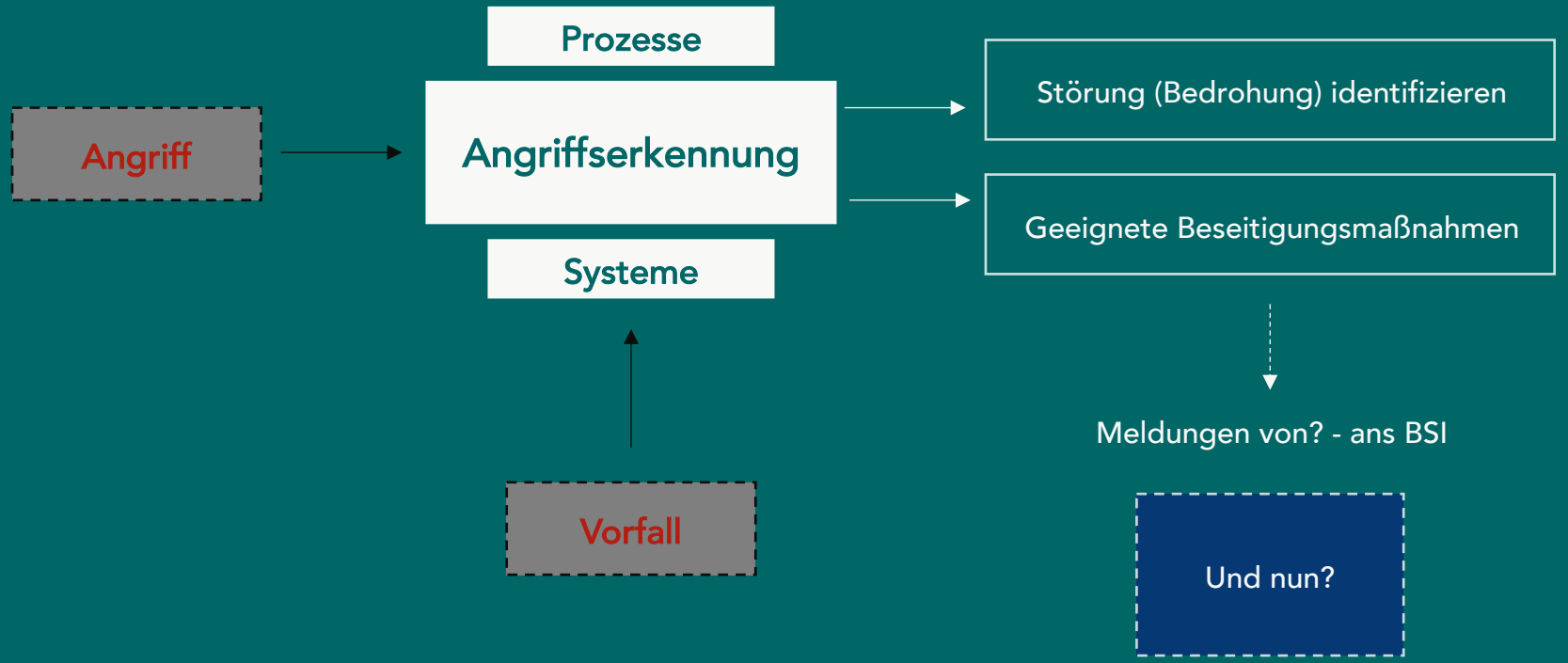


* für ISMS analog

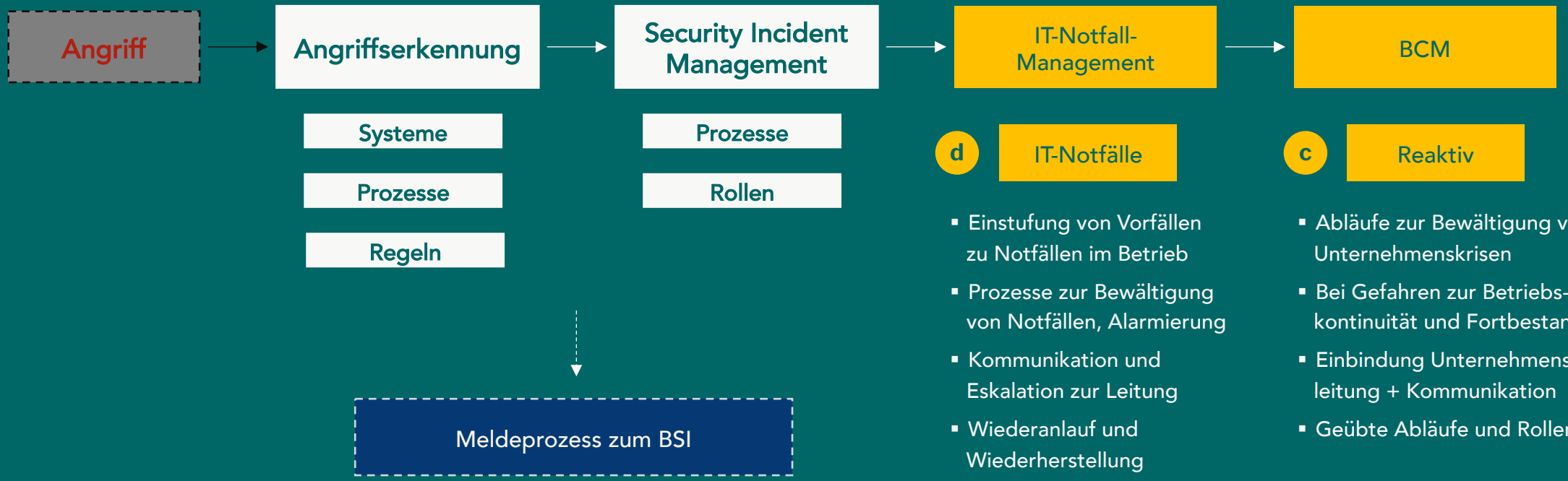
KRITIS-Meldepflichten - und dann?

Was müssen Betreiber erkennen und melden?

§8a (1a) BSIG: "Die Verpflichtung ... umfasst ... auch den Einsatz von Systemen zur Angriffserkennung" (IT-SiG 2.0, ab 2023)
§8b (4) BSIG: "Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich ... an das BSI zu melden"



Mitigation von Angriffen mit BCM



BCM im Stand der Technik

Ist BCM Stand der Technik?

§8a (1) BSIG: "Betreiber Kritischer Infrastrukturen sind verpflichtet ... angemessene organisatorische und technische Vorkehrungen ... zu treffen. Dabei soll der Stand der Technik eingehalten werden"

Fokus bei KRITIS-Betreibern und Projekte häufig: Management Risiken = IT-Sicherheit
Ergo: Umsetzung ISO 27001, BSI IT-Grundschutz, Branchenstandards = Stand der Technik

ISMS

IT

BCM

a Analysen

Vollständiges Risikobild

- Nicht "nur" IT-Risiken in der KRITIS-Anlage
- Nicht "nur" Informationssicherheit und Vertraulichkeit/Integrität
- Klärung: Was ist für den Betrieb und Prozesse wie wichtig
- = Ausfallrisiken und Kritikalitäten

b Pläne

BCM-Maßnahmen

- Aktuelle und geübte Pläne (neuer als 2005)
- Verantwortung im Unternehmen für Ausfälle
- Verantwortung in Prozessen für Resilienz
- Maßnahmen und Pläne werden Teil vom KRITIS-Management – nicht nur IT/IS

BCM in KRITIS-Prüfungen*

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

IDW Prüfungshinweis PH 9.860.2
Prüfung von Betreibern Kritischer Infrastrukturen §8a BSIG Maßnahmen

- ❑ Prüfhinweis für Wirtschaftsprüfer
- ❑ 100 Kontrollen (Nr. 1-100), basierend auf BSI C5
- ❑ Anlagen und Schwerpunkte für Wirtschaftsprüfer
- ❑ 5 BCM-Kontrollen

Bundesamt
für Sicherheit in der
Informationstechnik

Konkretisierung der Anforderungen an die §8a BSIG Maßnahmen

- ❑ "Orientierungsmaßstab" und "Hilfestellung"
- ❑ 100 Kontrollen (BSI 1-100), basierend auf IDW/C5
- ❑ Grundlage für BSIG-Prüfer, wenn kein (anwendbarer) B3S
- ❑ 3 Continuity Management Kontrollen

a Analysen

b Pläne

➡ Managementsystem für BCM (BCMS) nötig (eigentlich)

** analog für ISO 27001 etc.*

Der Case

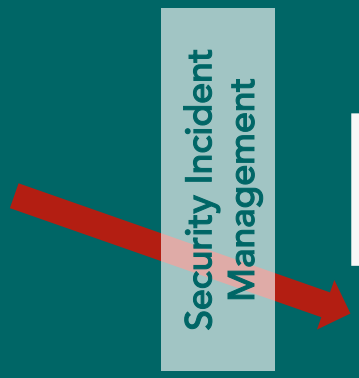
warum BCM sich lohnt

OPENKRITIS

Der Case am Beispiel Angriffserkennung

Normative Neuerung im Gesetz

Bei wörtlicher Auslegung zu enger Fokus auf Systeme zur Erkennung (IDS, IPS, SIEM, SOC)



Umgang mit IT-Notfällen

IT-Notfall-Management

Prozesse

Angriffserkennung*

Systeme

Prävention (BCM, IT-SCM)

Verhindern von Ausfällen

Krisen bewältigen

Krisen-Management

Beitrag von BCM

Kontinuität:
Prozesse, Rollen und zur Bewältigung von Notfällen und Krisen (durch Vorfälle).

Prävention:
Pläne, Übungen und Entscheidungen (wer ist betroffen, wer darf eigentlich was?) und Prävention!

* ebenso anwendbar auf ISMS, IT-Maßnahmen, IT-Prozesse, etc.

Diskussion

Nichts verpassen zu Kritischen Infrastrukturen:

OpenKRITIS.de

(60+ Artikel, Webinare, Podcast)

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

Notfallmanagement in Kritischen Infrastrukturen
Stand: 29. April 2022
Version: 1.0

Impressum

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn

https://www.openkritis.de · ISSN 2748-565X
info@openkritis.de · +49 176 58952135