OPENKRITIS

Angriffserkennung im IT-SiG 2.0

Webinar · 30. Juli 2021

OpenKRITIS · Dialog

OpenKRITIS-Dialoge 2021

IT-Sicherheitsgesetz 2.0

Angriffserkennung KRITIS

OT-Sicherheit in KRITIS, altern.: BCM

UNBÖFI und IT-SiG

KRITIS-Entsorgung

European Context NIS2 + RCE

Repetitorium KRITIS-Prüfungen

Sommer

Herbst

Winter

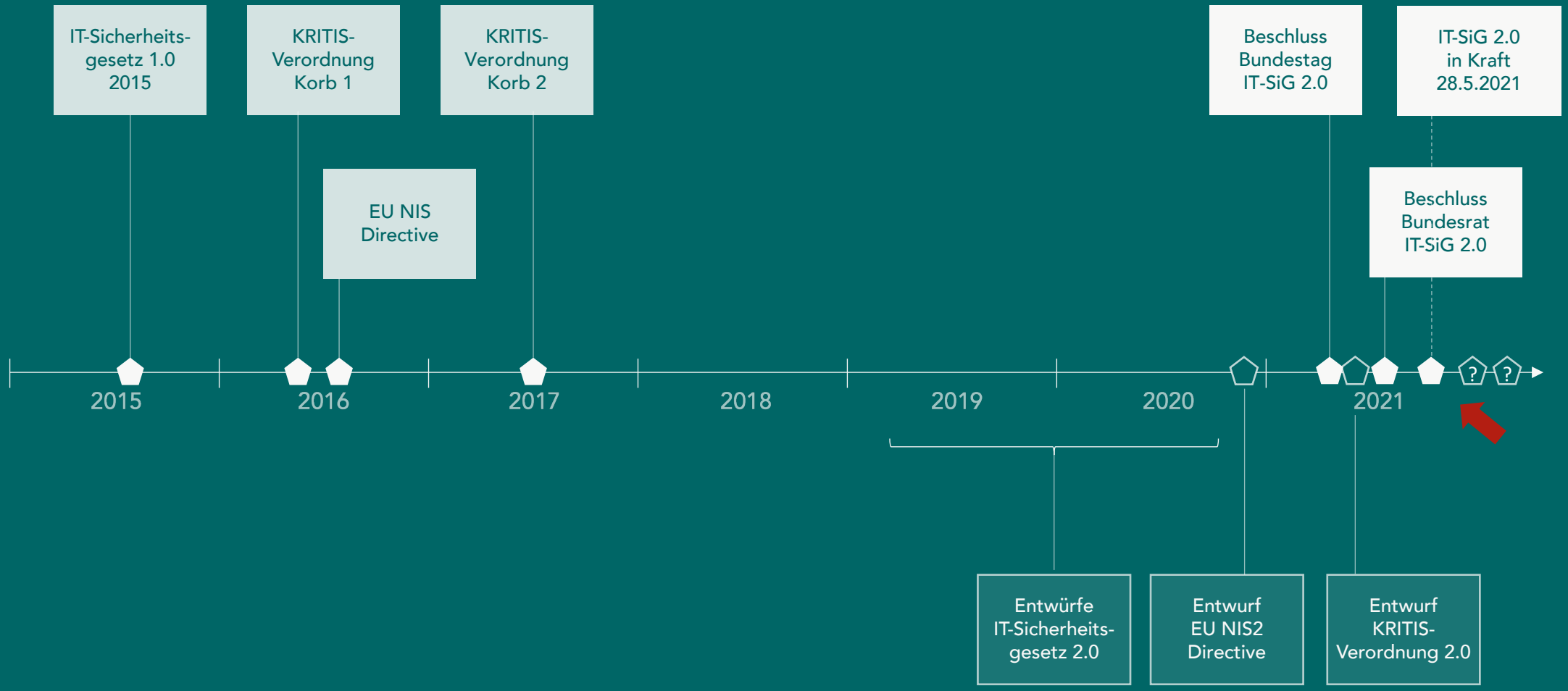
Agenda heute

1. Angriffserkennung und Gesetz
2. Die Sicht der Prüfer
3. Diskussion und Austausch

- Stand der Technik
- Und was fehlt?

Angriffserkennung im Gesetz

IT-Sicherheitsgesetz 2.0 Zeitschiene



Angriffserkennung im Gesetz

IT-SiG 1.0

§8 (1) BSIG

[KRITIS-Betreiber sind verpflichtet, ...] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden.

IT-SiG 2.0

§8 (1a) BSIG-E

Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

§2 (9b) BSIG-E

Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.

Gesetzesbegründung IT-SiG 2.0

Drucksache 19/26106, "Besonderer Teil"

Zu Nr. 12, b/c/e

§ 8a Absatz 1a ergänzt [...] ausdrücklich um Systeme zur Angriffserkennung. Diese Systeme stellen eine effektive Maßnahme zur Begegnung von Cyber-Angriffen dar und unterstützen insbesondere die Schadensreduktion.

Bereits heute ist eine große Anzahl von Systemen zur Angriffserkennung verfügbar. Diese unterscheiden sich u.a. in den Verfahren zur Detektion und sind für unterschiedliche Einsatzszenarien optimiert.

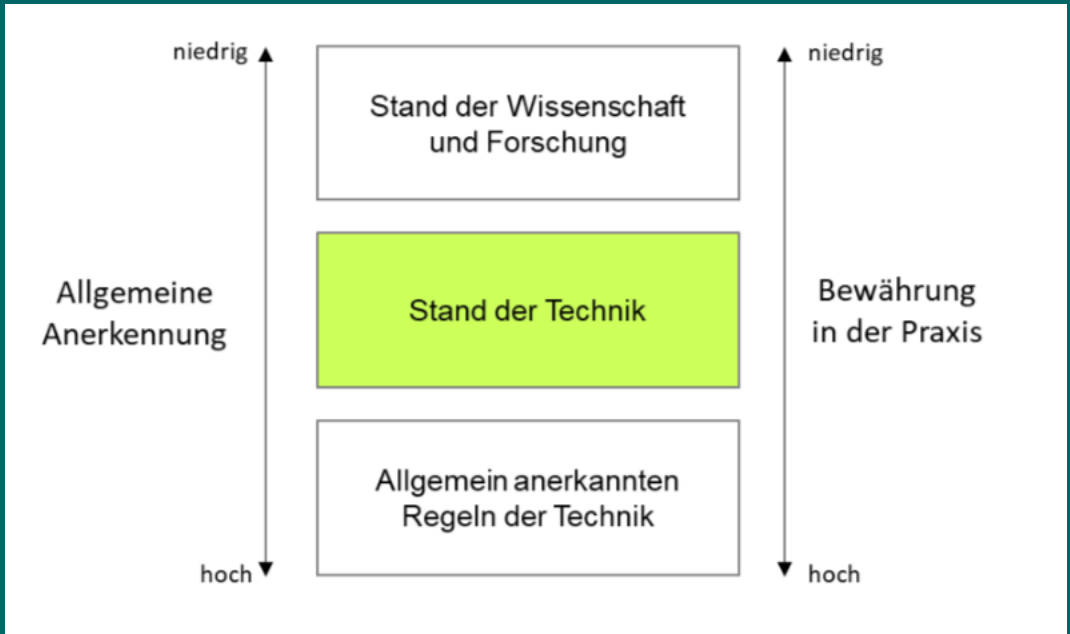
Unterschiede liegen [...] in den untersuchten Daten [...] an den Übergängen zu öffentlichen Netzen, netzwerk-internen Datenverkehr oder auch von internen Daten der IT-Systeme erhoben werden. [...]

Methodik zur Erkennung [...] Abgleich mit statischen Mustern [...] generische Muster sowie Verfahren der künstlichen Intelligenz, [...] Abweichungen [vom Störungsfreien Betrieb] zur Detektion [...] (Anomaliedetektion).

Die Systeme zur Angriffserkennung sollen die Kommunikationstechnik der Betreiber Kritischer Infrastrukturen möglichst umfassend schützen. Gleichzeitig können Systeme zur Angriffserkennung zum Beispiel im Falle falscher Warnmeldungen auch zu Schäden führen. Gefordert wird daher – entsprechend Absatz 1 – nur ein angemessener Einsatz, dem eine Abwägung der Interessen an einem umfassenden Schutz mit bestehenden Risiken vorgeht.

Unternehmen benötigen für den Einsatz von Systemen zur Angriffserkennung Informationen, die sich als Erkennungsmuster zu Cyber-Angriffen einsetzen lassen. Der Einsatz der Systeme zur Angriffserkennung erfordert, dass die eingesetzten Erkennungsmuster ständig aktuell gehalten werden. Das Bundesamt wird dabei weiterhin [...] die Betreiber unterstützen. [...]

Stand der Technik



"Somit kann der Stand der Technik als die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann, bezeichnet werden.

Verkürzt lässt sich sagen: Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung eines Subjekts zur Erreichung eines Objekts. Subjekt ist die IT-Sicherheitsmaßnahme; Objekt das gesetzliche IT-Sicherheitsziel."

Beides aus: IT-Sicherheitsgesetz und DSGVO, Handreichung zum Stand der Technik, TeleTrusT 2021

Stand der Technik

TeleTrusT 2020

3.2.17 Netzwerküberwachung mittels Intrusion Detection System

Ein Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) erkennt und protokolliert Anomalien im IT-Netz. Das Ziel beider Systeme ist es das Eindringen und Verteilen von Schadsoftware möglichst vor Schadenseintritt zu erkennen. Im Gegensatz zum IDS, welches ausschließlich Informationen von anomalem Verhalten anzeigt und Alarme generiert, kann ein IPS auch selbsttätig eingreifen. Damit soll die weitere Ausbreitung von Schadsoftware über das Netz verhindert werden. Dabei ist zu beachten das z.B. bei Industrie- und Produktionsanlagen oder vollautomatisierten Bestell-/Lieferprozessen sowie Meldungs- und Sicherheitsprozessen (u. a. Brandschutz) ein direkter Eingriff durch ein IPS die Verfügbarkeit unmittelbar beeinflusst

3.2.22 Endpoint Detection & Response Plattform

Der Schutz der Endgeräte (z.B. PCs, Laptops, Smartphone oder Tablets) erfordert inzwischen weit mehr als nur ein Antivirus-Programm. Moderne Lösungen (Endpoint-Detection & Response Plattformen, EDR) vereinen neueste Schutztechnologien um alle Arten von Cyber-Angriffen auf Client und Server Systemen betriebssystemübergreifend zu stoppen und die Urheber zu identifizieren. Im Gegensatz zu konventionellen Lösungen ist kein spezifisches Vorwissen, wie z. B. Signaturen oder ein erstes Opfer nötig.

TeleTrusT 2021

+

3.2.24 Angriffserkennung und Auswertung (SIEM)

Für die Auswertung von Anomalien und Erkennung von Angriffen der Unternehmensinfrastruktur werden sogenannte Security Information and Event Management Systeme (kurz: SIEM) eingesetzt. Sie ermöglichen ganzheitlich, sicherheitskritische Events der IT-Infrastruktur in Echtzeit zu erkennen und geeignete Maßnahmen (teilweise automatisiert) durchzuführen.

Alles aus: Handreichung zum Stand der Technik, TeleTrusT 2021 und 2021

Die Sicht der Prüfer

Relevante Prüfstandards

IDW Prüfungshinweis

Prüfung der gemäß §8a Abs. 1 BSIG umzusetzenden Maßnahmen PH 9.860.2

- Prüfhinweis für Wirtschaftsprüfer
- 100 Kontrollen (Nr. 1-100), basierend auf BSI C5
- Mit beispielhaften Prüfungshandlungen für Angemessenheit und Wirksamkeit
- Methodik und Schwerpunkte für Wirtschaftsprüfer (Auftragsannahme, Typen, Urteile ...)

Link IDW PH 9.860.2

BSI Konkretisierung

Konkretisierung der Anforderungen an die gemäß §8a Absatz 1 BSIG umzusetzenden Maßnahmen

- "Orientierungsmaßstab" und "Hilfestellung"
- 100 Kontrollen (BSI 1-100), angelehnt an IDW PH
- Deutlich erweiterte Kontrolltexte und deskriptive Anforderungen
- Mögliche Grundlage für BSIG-Prüfer, wenn kein B3S oder sonstige Standards anwendbar sind

Link BSI Konkretisierung

BSI Konkretisierung - Angriffserkennung

Governance Sicherheitsvorfälle	Systeme und Auswertung	Schwachstellen und Tests
BSI 77-79	BSI 80	BSI 95-96
BSI 81-82	BSI 90-94	
Prozesse und Verantwortlichkeiten für Sicherheitsvorfälle	Systeme und Methoden zur systematischen Auswertung	Regelmäßige Penetrationstests und Umgang mit Schwachstellen

aus OpenKRITIS Angriffserkennung

Governance von Angriffserkennung

Governance
Sicherheitsvorfälle

BSI 77-79

- ❑ Verantwortlichkeiten und Vorgehensmodell (Richtlinien, Anweisungen)
- ❑ Bearbeitung von Sicherheitsvorfällen (Personal, Prozesse)
- ❑ Dokumentation und Berichterstattung über Sicherheitsvorfälle

BSI 81-82

- ❑ Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen (SIM)
- ❑ Auswertung und Lernprozess (+ Meldungen, Verbesserung)

Systeme und Auswertung von Logs

Systeme
und Auswertung

BSI 80

- ❑ Security Incident Event Management (SIEM)
- ❑ (Korrelation, Regeln, Beurteilung, Behandlung, SIM-Prozess)

BSI 90-94

- ❑ Systematische Log-Auswertung (Richtlinien, Anweisungen, Prozesse)
- ❑ Erkennung von Ereignissen auf kritischen Assets (KRITIS-Anlage)
- ❑ Protokollierung, Aufbewahrung der Daten
- ❑ Besonderer Schutz der Systeme, Konfiguration und Zugänge

Und was fehlt?

Bedeutung

Angriffserkennung
ab 2023 verpflichtend

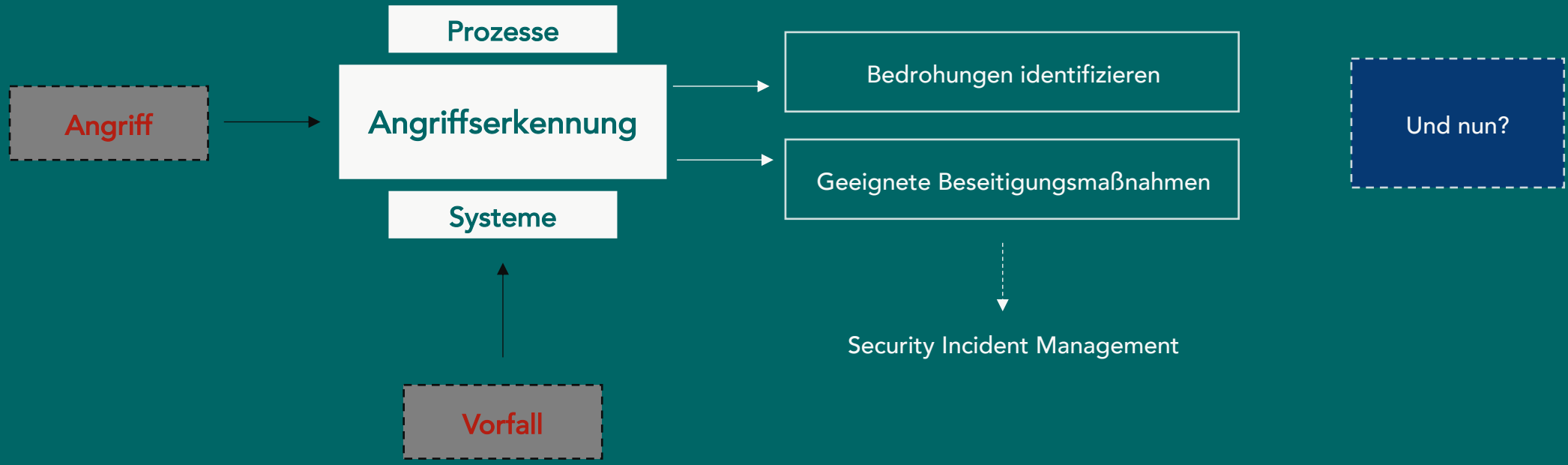
Gesetz
IT-SiG 2.0 und BSIG-E

- ❑ "Systeme zur Angriffserkennung"
  → Technische Werkzeuge und Prozesse mit organisatorischer Einbindung
- ❑ Automatische, kontinuierliche Auswertung vom laufenden Betrieb
- ❑ Bedrohungen identifizieren *und vermeiden*
- ❑ Geeignete Beseitigungsmaßnahmen vorsehen

Prüfungen
Nachweise und Standards

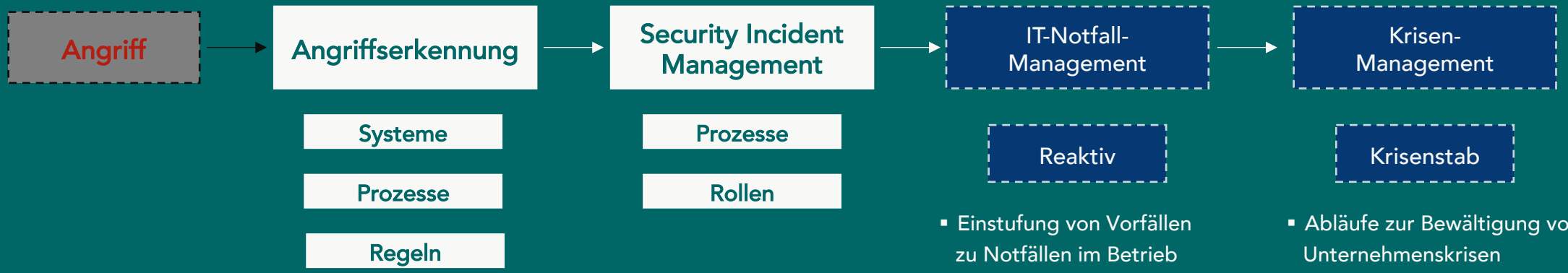
- ❑ Governance Sicherheitsvorfälle
- ❑ Richtlinien, Prozesse, Rolle f. SIM
- ❑ Systeme zur Erhebung/Auswertung, SIEM und Log-Auswertung
- ❑ Protokollierung und Dokumentation
- ❑ Meldeprozesse

Ablauf der Angriffserkennung



Organisatorische Reaktion

tw. in BSI 17-19 (BCM 01, 03, 04)



Reaktiv

- Einstufung von Vorfällen zu Notfällen im Betrieb
- Prozesse zur Bewältigung von Notfällen, Alarmierung
- Kommunikation und Eskalation zur Leitung
- Wiederanlauf und Wiederherstellung

Krisenstab

- Abläufe zur Bewältigung von Unternehmenskrisen
- Bei Gefahren zur Betriebs-kontinuität und Fortbestand
- Einbindung Unternehmens-leitung + Kommunikation
- Geübte Abläufe und Rollen

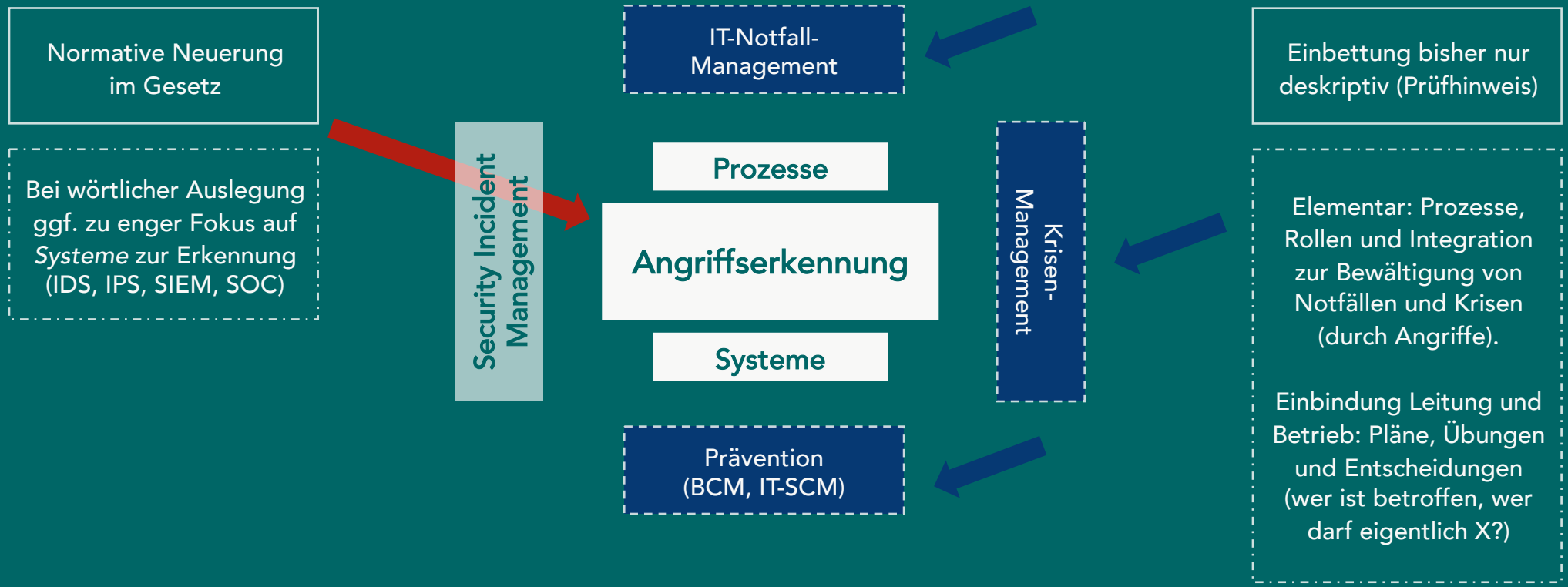
Präventiv

- Pläne für IT-Notfälle
- Priorisierung + IT-Assets
- KVP Prozesse (IT)

BCM

- Pläne für Aus-/Notfälle
- Business Impact, Assets
- KVP Prozesse (Betrieb)

Aufbau Erkennung und Reaktion



Ausblick

The road ahead 2021+

IT-Sicherheitsgesetz 2.0	Gesetzliche Grundlage Änderungsgesetz BSIG etc.	In Kraft seit Mai 2021
KRITIS-Verordnung 2.0	Überarbeitung der KRITIS-Sektoren mit Anlagen und Schwellenwerten	Entwurf publik seit April Verabschiedung geplant Juni
KRITIS Entsorgung	Definition Sektor Entsorgung mit Anlagen und Schwellenwerten	Weitere Änderungsverordnung?
UNBÖFI Gruppe 2	"Volkswirtschaftliche Bedeutung" – Methoden und Schwellenwerte	Zusätzliche Rechtsverordnung?
EU NIS2 und RCE	16 Sektoren essential/important 10 Sektoren critical	Verabschiedung in der EU in 2021 Weiteres Änderungsgesetz?
Prüfzyklus 2023	Einsatz von Angriffserkennung ab 1.5.2023 verpflichtend	Aufbau und Inbetriebnahme bis vor den Prüfungen – dann Nachweise

Diskussion

Informationen zu KRITIS aus einer Hand:

openkritis.de – Die freie Plattform mit 40+ KRITIS-Artikeln

Fragen bei der Umsetzung?

Ich helfe gern: insignals.net

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

Angriffserkennung im IT-SiG 2.0 – OpenKRITIS-Webinar
Stand: 30. Juli 2021
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