Systeme zur Angriffserkennung

Klaus Hunsänger, Referent

Bundesamt
für Sicherheit in der
Informationstechnik

FACHGRUPPE
SECMGT

01. Angriffserkennung aus Compliance-Sicht

Artikelgesetz: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

IT-Sicherheitsgesetz 2.0 - IT-SiG 2.0 (2021)

§8a Abs. 1a BSIG:

„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**. Absatz 1 Satz 2 und 3 gilt entsprechend."

(analoger Text in **§11 Abs. 1e EnWG**)

Quo vadis?

NIS-2-Richtlinie (NIS2-UmsG)

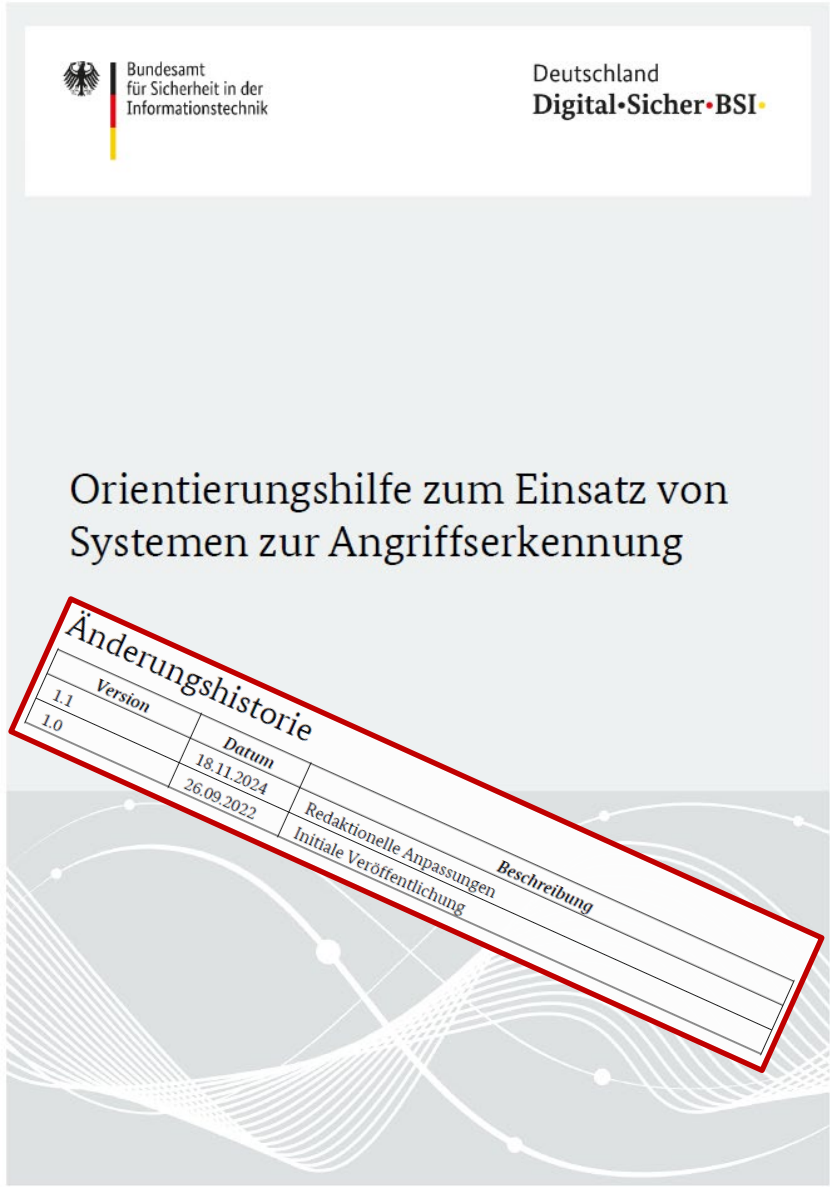
EU CER-Richtlinie (KRITIS-Dachgesetz)

Orientierungshilfe SzA

Eine Empfehlung – weder Norm noch Prüfgrundlage!

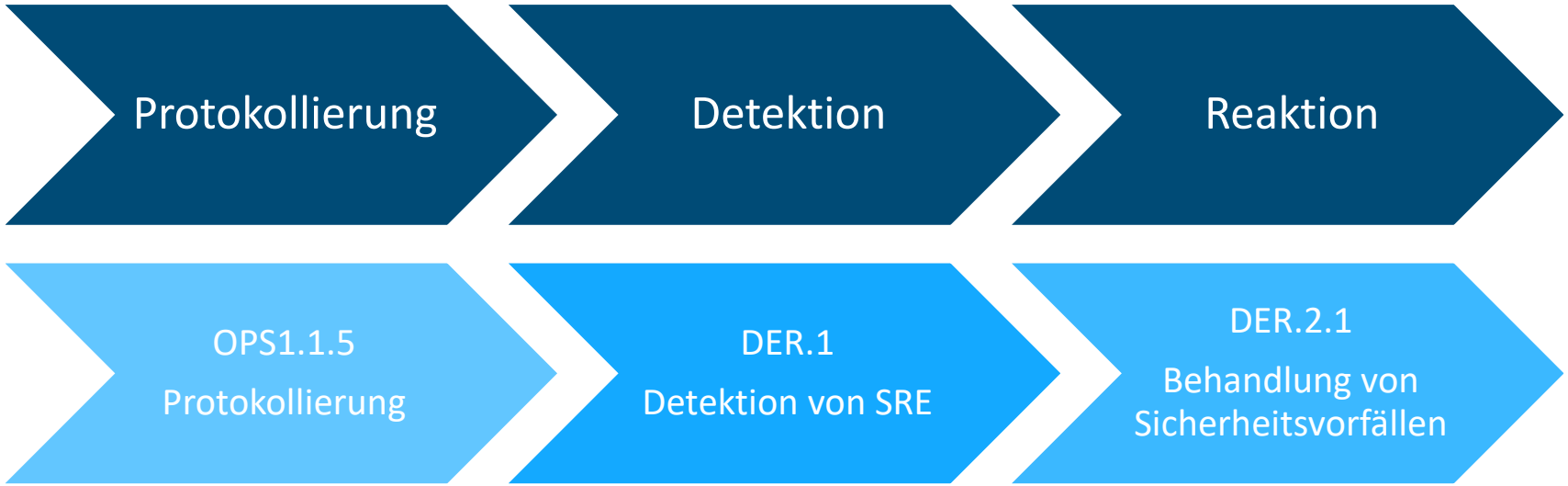
Inhalt

Unter Beteiligung von C 25



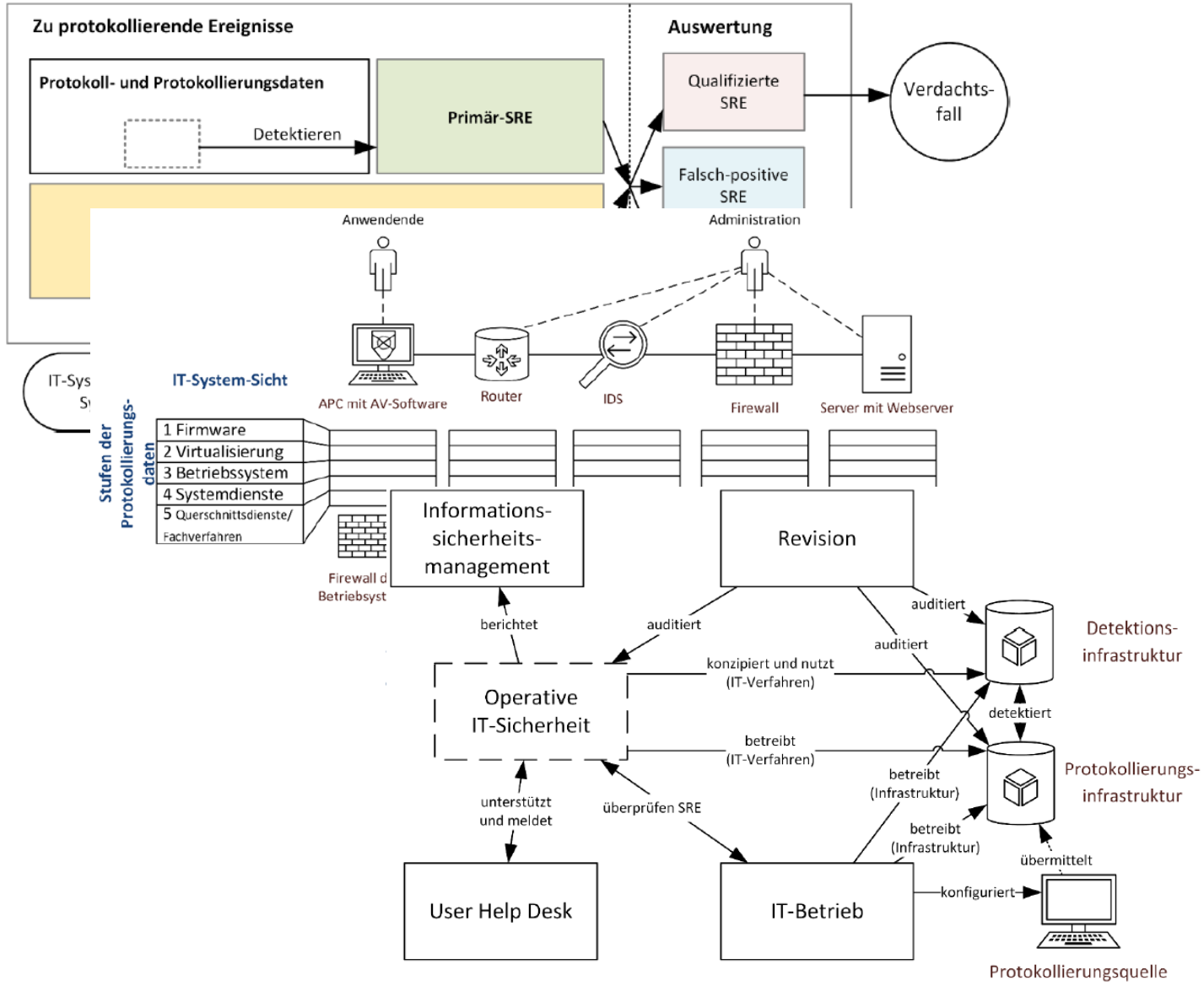
Orientierungshilfe SzA

Anforderungen



https://www.bsi.bund.de/dok/128568

* Weiterführende Literaturempfehlung



02. Angriffserkennung – ein generisches MUSS !

Angriffe im Energiesektor

EINE Ursache der Regulierung

INDUSTROYER

BLACKENERGY

Cyberangriff
NetComBW

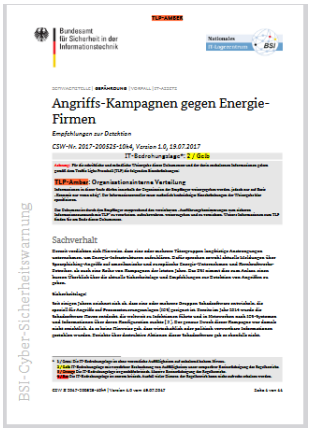
(Pressebericht in 2018)

**INCONTROLLER/
PIPEDREAM**

INDUSTROYER2*

GoldenJackal

2015 — 2016 — 2017 — 2021 — 2022 — 2024



**Diverse Einsätze des
BSI-Mobile-Incident-
Response-Team (MIRT)**

IT-SiG 2.0

- …
- …
- SzA

ENERGY

TU Foreign objects found in the power grid - right next to Norway's combat base

*https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/Archiv-Lageberichte/2022/lagebericht_node.html S.51

Einschub - Best Of: MIRT NO-GOs

Was die Kolleginnen und Kollegen vor Ort (nicht) erleben (möchten)!

Stand: 20.03.2023

Technisch:

- Keine Logs vorhanden
- Destruktive „forensische Analysen“ durch IT-Betrieb – Scheitern – Ruf nach BSI
- Keine ausreichende Kenntnis über die eigene Infrastruktur

Organisatorisch:

- Kein Ansprechpartner vor Ort / erreichbar
- Ansprechpartner ohne Verbindung zum IT-Betrieb / ohne Entscheidungsbefugnis
- Vorfall wird intern nicht prioisiert

Szenario zur Destabilisierung mittels Einflussoperationen

3. Störung kommunaler Dienstleistungen und Versorgung

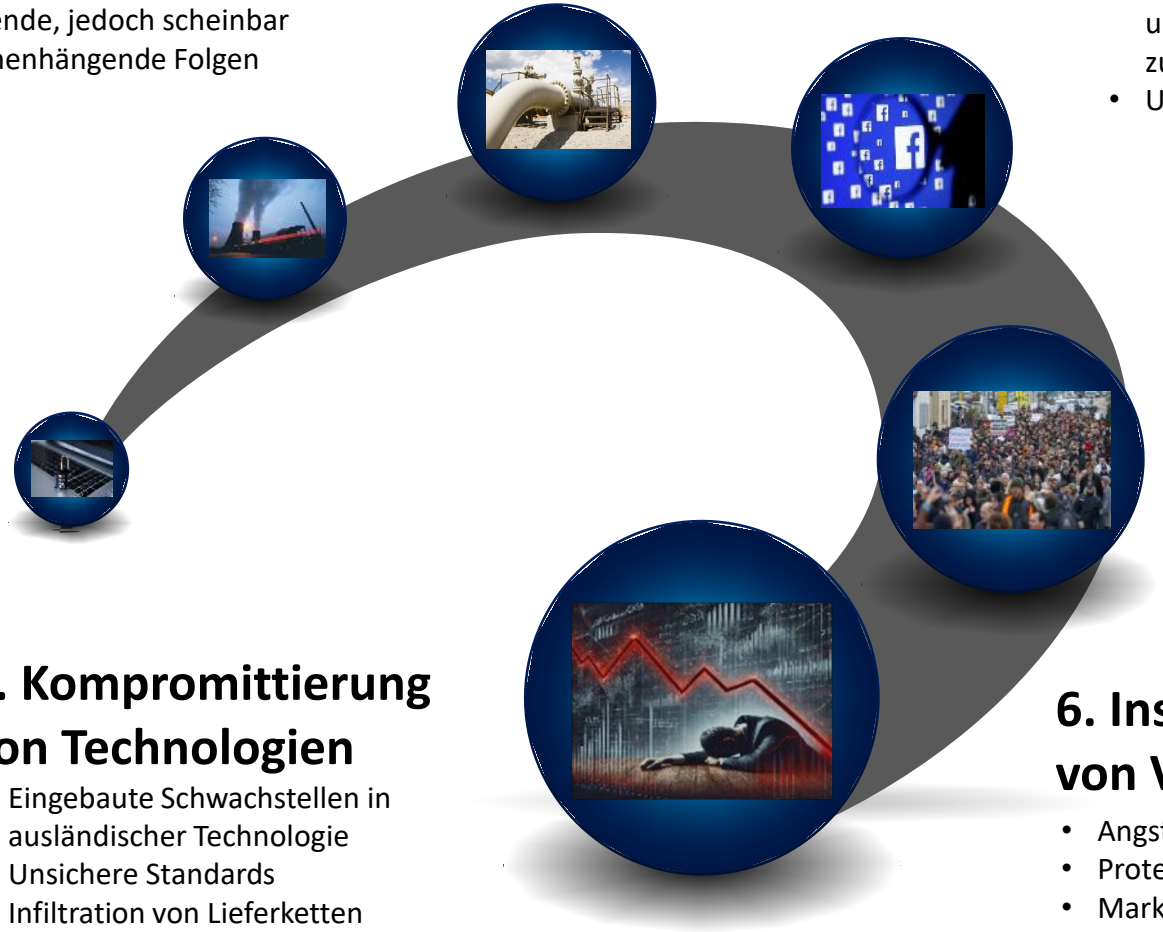
- Nutzen der Informationen für weitere Angriffe
- Kaskadierende, jedoch scheinbar unzusammenhängende Folgen

4. Gefälschte Kommunikation und KI-manipulierte Inhalte

- Erbeutende Informationen werden genutzt um Informationsoperationen glaubwürdiger zu machen
- Unterstützung durch KI

2. Cyberangriffe auf Unternehmen

- Nutzung von Schwachstellen für APTs
- Spear-Phishing mit Social Engineering
- (Pseudo-)Ransomware zur Ausspähung und Sabotage
- DDoS
- Erbeutung von Informationen von Kunden, Dienstleistern und Zulieferern



5. Desinformation in sozialen Medien / Fake-Webseiten

- Überflutung mit massenweiser Desinformation
- Nutzung verteilter und umfangreicher Infrastruktur
- Erschwerte Gegenmaßnahmen

1. Kompromittierung von Technologien

- Eingebaute Schwachstellen in ausländischer Technologie
- Unsichere Standards
- Infiltration von Lieferketten

6. Inszenierung und Verschärfung von Verunsicherung

- Angst und Unmut in der Bevölkerung wächst
- Proteste, Aufstände
- Marktverunsicherung
- Verändertes Konsumverhalten

Bildquellen: CNET, FAZ,Tagesschau, Rigzone

Fazit

Glauben sie noch oder suchen sie schon?

Protokollierung

- Sichere Identifizierung des initialen Angriffsvektors,
- Kenntnis über die Verbreitung der Schadware im Netzwerk

Detektion

- Signaturen
- Indicators of Compromise
- Tactics, Techniques @ Procedures
- Anomalien
- KI? Gerne – aber bitte mit Bedacht!

Reaktion

- Prozesse klar definiert / Übungen
- Ohne ausreichende Protokollierung ggf. sehr schwer / erfolglos

Noch Fragen?

Bundesamt
für Sicherheit in der
Informationstechnik

Vielen Dank für Ihre Aufmerksamkeit!

Klaus Hunsänger
Industrielle Steuerungs- und Automatisierungssysteme

klaus.hunsaenger@bsi.bund.de
Tel.: +49 (0) 228 9582 6470
Mobil: +49 160 9079 1274

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de/ics

Follow us: