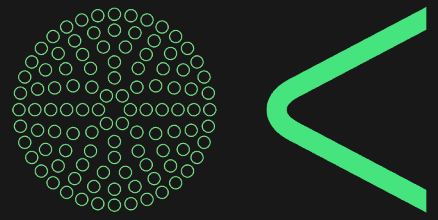
OPENKRITIS



KRITIS-Betreiber und Systeme zur Angriffserkennung (SzA)

Mai 2023 · OpenKRITIS

Vorgaben zu Angriffserkennung in KRITIS

seit 2021

IT-Sicherheitsgesetz 2.0

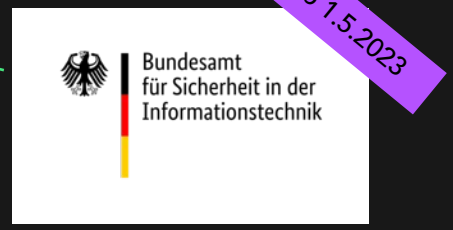
- IT-Sicherheit in KRITIS
- KRITIS-Betreiber
- §8a Absatz 1a: SzA als Stand der Technik
- SzA ab 1.5.2023

seit 2020

Konkretisierung §8a

- “Prüfstandard KRITIS”
- Konkretisierung der §8a Maßnahmen (100)
- Angriffserkennung in 2.8 und 2.9 vorhanden

seit 2022



ab 1.5.2023

Orientierungshilfe SzA

- “Prüfstandard SzA”
- Konkretisierung §8a (1a) in Einzelmaßnahmen
- Logging, Detektion und Reaktion + Rahmenwerk

+ Standards

Angriffserkennung im Gesetz

BSIG Stand 2021

§8a BSIG
Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) [Maßnahmen nach Stand der Technik ...]

(1a) 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.

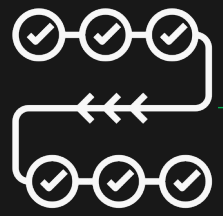
Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

Was ist zu tun? Angriffserkennung

Logging

Ereignisse protokollieren
Logs zentral speichern/behandeln
Indizien erkennbar machen

Detektion



Angriffe erkennen (können)
Signaturen, Muster, IOCs

Reaktion

Auf Ereignisse/Vorfälle reagieren
Integration SIM/BCM/ITN
Meldeketten

Die Orientierungshilfe OH SzA

Inhalt

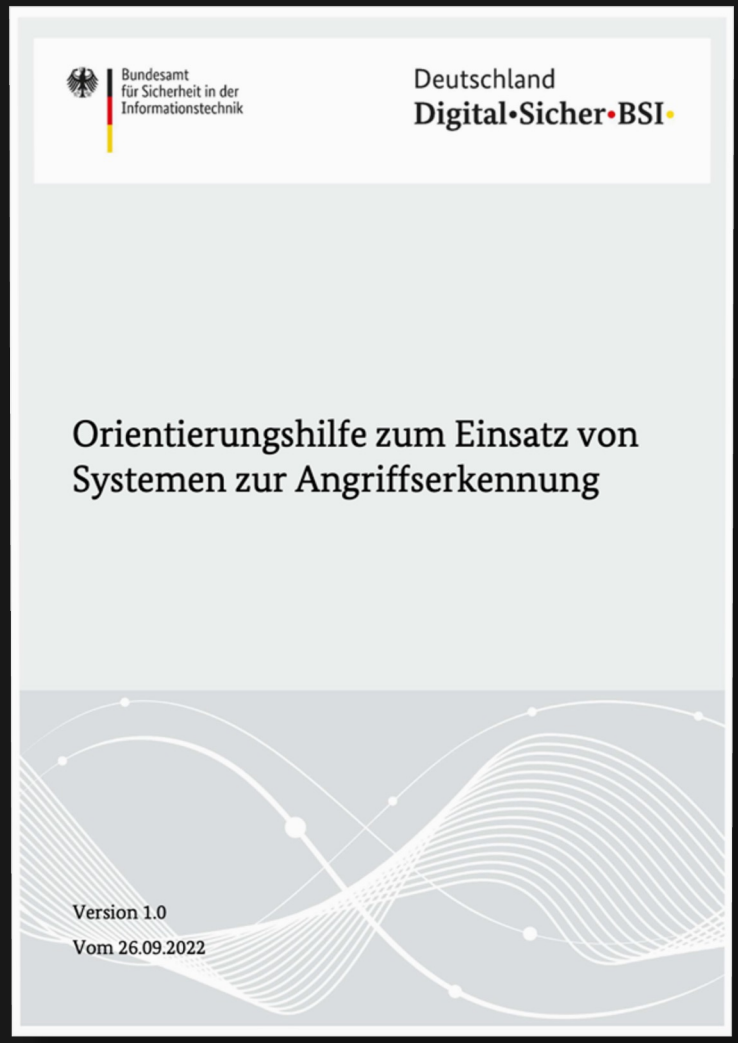
- Anforderungen an Systeme und Prozesse zur Angriffserkennung bei KRITIS-Betreibern
- Allgemein, Logging, Detektion, Reaktion + Details

Normativ

- Quasi-Prüfstandard, prüferisches Urteil notwendig
- Nachweis von SzA in Prüfungen ab 1. Mai 2023

Anwendung

- Prüfer: Erweiterung Prüfkatalog und Vorbereitung
- Betreiber: Umsetzung im Betrieb + Control Set



Reifegradmodell OH SzA

Grad	*Maßnahmen*	*KVP*	*Zusatz*	
0	Keine Maßnahmen umgesetzt Keine Pläne vorhanden			
1	Planungen vorhanden Noch keine konkrete Umsetzung			
2	Umsetzung wurde in allen Bereichen begonnen, jedoch noch nicht erfüllt			
3	Alle MUSS-Anforderungen umgesetzt	KVP umgesetzt oder in Planung		erster Zyklus
4	Alle MUSS-Anforderungen umgesetzt Alle SOLL-Anforderungen umgesetzt oder stichhaltig begründet ausgeschlossen	KVP etabliert		dann Pflicht
5	Alle MUSS-Anforderungen umgesetzt Alle SOLL- und KANN-Anforderungen umgesetzt oder stichhaltig begründet ausgeschlossen	KVP etabliert	“Sinnvolle” zusätzliche Maßnahmen umgesetzt	

Inhalte der Orientierungshilfe

OH SzA Anforderungen an KRITIS-Betreiber

Formalien

- OH SzA Anforderungen
  - **MUSS**
  - SOLLTE
  - KANN
- BSI IT-Grundschutz
  - DER.1
  - OPS.1.1.5
  - DER.2.1
- Reifegradmodell
  - 3: MUSS ab 2023
  - 4: MUSS/SOLLTE
- **Quasi-normativ**

Allgemein

- Rahmen + Ausstattung bei KRITIS-Betreibern
- Ausreichend Budget
- Ausreichend Personal
- Passende Technologie
- Aktueller Stand der IT
- Aktuelle Muster und Signaturen
- Aktive Konfiguration

Protokollierung

- Vorgaben zum Logging in der IT
- Speicherung v. Daten
- Funktionen zum Logging von SREs
- Filtern, aggregieren, korrellieren
- Umfangreiche Planung
- Geltungsbereich KRITIS abdecken
- Zentrale Speicherung
- Protokollierung auf System- und Netzebene
- Regulatorik

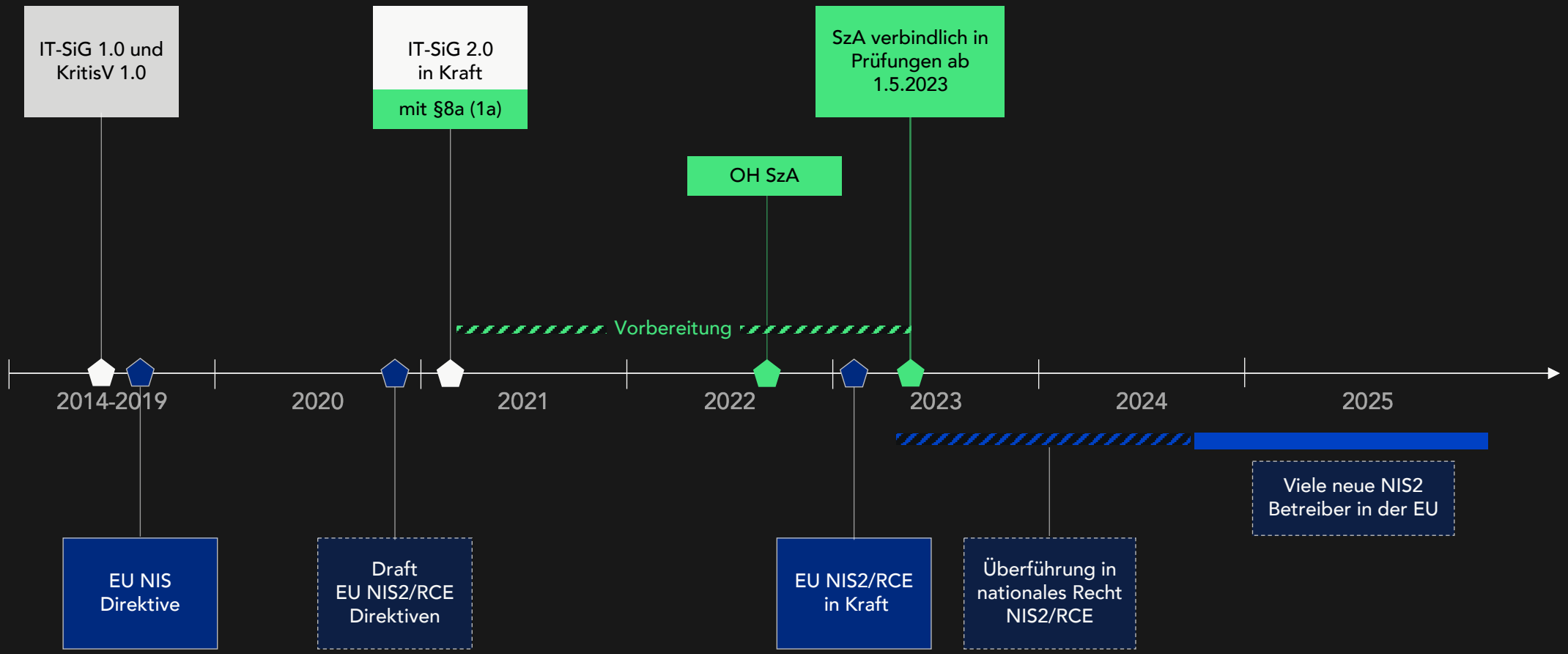
Erkennung

- Vorgaben zur Detektion in der IT
- Erkennung von Bedrohungen
- Abdeckung von Risiken
- Kontinuierliche Überwachung
- Schadecode/Malware
- Netze und IDS
- Zentrale Detektion
- Dauerhafte Auswertung
- Angriffsmuster + extern
- Meldungen
- Regulatorik

Reaktion

- Vorgaben zur Reaktion im Unternehmen
- Behebung
- Wiederherstellung
- Automatische Reaktion
- Behandlung
- Meldungen
- Regulatorik

Roadmap


IT-SiG 1.0 und KritisV 1.0
IT-SiG 2.0 in Kraft
mit §8a (1a)
SzA verbindlich in Prüfungen ab 1.5.2023
OH SzA
Vorbereitung
2014-2019
2020
2021
2022
2023
2024
2025
EU NIS Direktive
Draft EU NIS2/RCE Direktiven
EU NIS2/RCE in Kraft
Überführung in nationales Recht NIS2/RCE
Viele neue NIS2 Betreiber in der EU

Und in der Praxis?

Umsetzung von SzA in drei Schritten

Umsetzung

Prüfung

analog

Steuerung

Controls

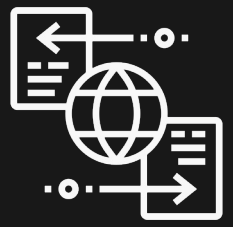
Umsetzung zentral
Umsetzung dezentral

Umsetzung: Governance in der Praxis

Steuerung

Rahmen für Angriffserkennung

- Budget
- Personal und Rollen
- Programm/Projekte
- IT-Vorraussetzungen



Governance

- ISMS bzw. Sicherheitsprozess
- SOC/CSIRT
- Policies, Standards
- Zentrale Prozesse (SIM, BCM, ...)

Umsetzung: OH SzA zu Standards und Controls

Beispiel OpenKRITIS

Cluster bilden

OH SzA	Thema	BSI KRITIS	C5:2020	ISO 27002 2022
SZA-A	**Allgemeine Anforderungen**			
A1	Rahmenbedingungen	BSI-2 BSI-17	OIS-02 BCM-01	5.2 5.24 5.31
A2	Angriffsmuster	BSI-96	OPS-20	8.8 5.7
A3	Plattform	BSI-25	OPS-23	8.19 8.8
A4	Signaturen	BSI-21	OPS-05	8.7
A5	Konfiguration	BSI-93	OPS-15	8.9
SZA-G	**Governance**			
G1	Richtlinie Protokollierung	BSI-2	OIS-02	5.1 5.24
G2	Richtlinie Detektion	BSI-2 BSI-77	OIS-02 SIM-01	5.1 5.24

Am „ehesten“ passende bzw. zu erweiterende Kontrollen

Kein 1:1 Mapping!

Zuordnungen in Arbeit, nicht immer 100% n:m

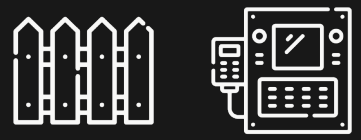
Stand 19.10.2022, Link OpenKRITIS

Umsetzung: Aktuelle Praxis im Betrieb

Zentral

Umsetzung in Zentralfunktionen

- SOC (SIEM) ermächtigen/aufbauen
- Zentrales Onboarding-Programm
- Schnittstellen integrieren (SIM/BCM)
- Unterstützung der Fläche



Dezentral

Umsetzung in der Fläche

- Anforderungen im Betrieb (Logs)
- Anforderungen in der IT
- Dezentrale Prozesse
- Onboarding ans SOC/SIEM

Prüfungen: Wie läuft SzA?

Lange Vorbereitung notwendig

- Mapping auf Standards und Controls
- Mapping auf KRITIS-Prüfprogramm
- Self-Assessment SzA
- Gaps identifizieren
- Vorbereitung mit SOC/SIEM

Integriertes Prüfprogramm

- KRITIS-Anforderungen
  - SzA-Gaps zu KRITIS
  - SzA-Gaps zu int. Controls
- Eigener SzA-Block im Programm
- Eigene SzA-Findings

Fokusthemen Prüfung

1. Vorgaben und CISO
2. Zentrale Angriffserkennung
3. SzA im Betrieb dezentral

= wenige Hauptfeststellungen

Aktuelle Erfahrungen

Compliance

Standards und OH SzA

- Teils deutlich spezifischer als C5/ISO
- Interne Mapping-Arbeit notwendig
- Meist Anpassung und Erweiterungen am eigenen Rahmenwerk notwendig
- Sonderthema mit großem Detailumfang

Umsetzung

Betrieb und Prüfung

- Viel spezifischer Nachholbedarf
- Anforderungen nicht immer verständlich
- Unklare Verantwortung Zentrale vs. Fläche
- Unklare Verantwortung IT, Security, SOC
- Umfangreichere Prüfungen

Viel Vorbereitung notwendig
Aber – schaffbar!

Danke!

Nichts zu Kritischen Infrastrukturen verpassen:

OpenKRITIS.de

Systeme zur Angriffserkennung auf OpenKRITIS: OH SzA

Angriffserkennung auf OpenKRITIS: Angriffserkennung in KRITIS

OpenKRITIS Mapping auf Standards: OH SzA auf KRITIS, C5 und ISO 27002

Neuigkeiten: OpenKRITIS auf LinkedIn

KRITIS-Angriffserkennung

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

KRITIS-Betreiber und Systeme zur Angriffserkennung (SzA)

Stand: 3. Mai 2023

Version: 1.1

Impressum

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn

https://www.openkritis.de · ISSN 2748-565X

info@openkritis.de · +49 176 58952135