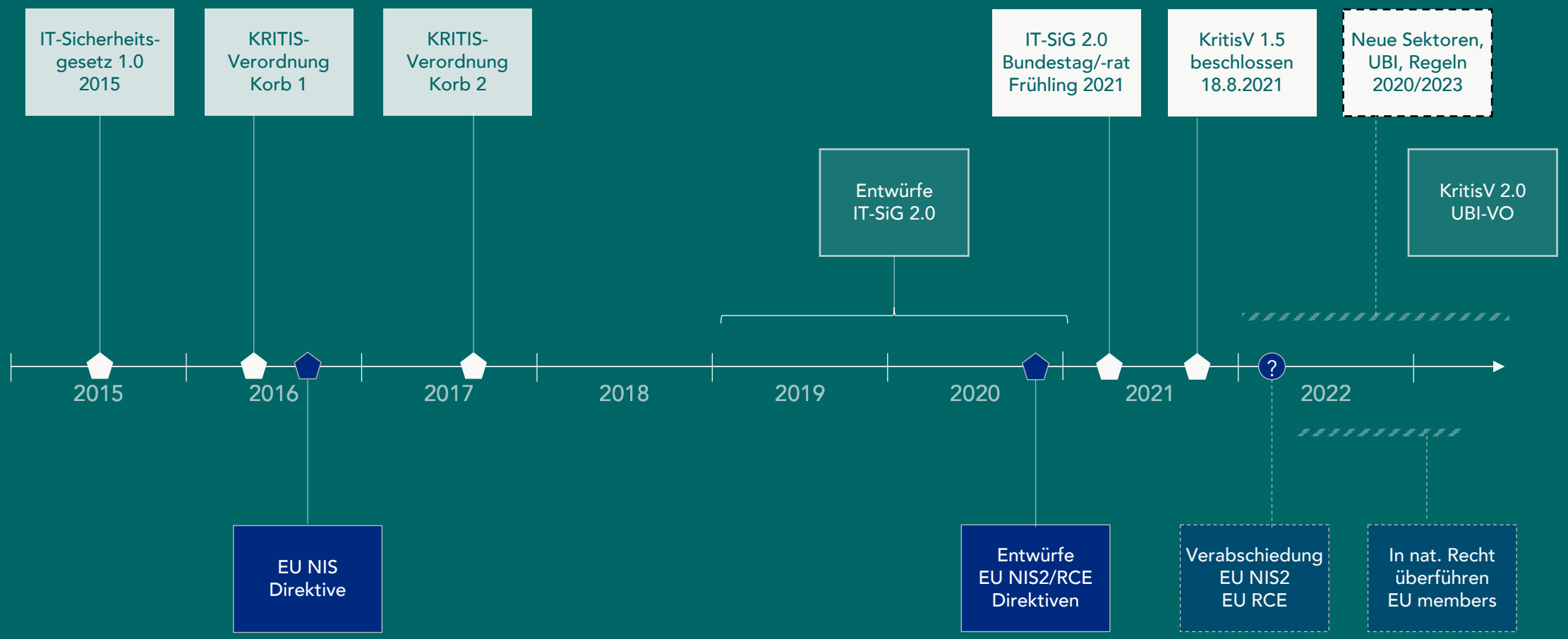
OPENKRITIS

IT-Sicherheitsgesetz 2.0

Briefing

14. Januar 2022 · OpenKRITIS.de

IT-Sicherheitsgesetz 2.0 und KRITIS



Neuerungen im IT-Sicherheitsgesetz 2.0

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)

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

Mehr Cyber Security Pflichten

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

Neu reguliert: Entsorgung und UBI

Mehr Unternehmen im Scope

Entsorgung

- Neuer KRITIS-Sektor Siedlungsabfallentsorgung
- Dienstleistung *Entsorgung von Siedlungsabfällen:*
  - a. Sammlung
  - b. Beseitigung
  - c. Verwertung
- Anlagen und Schwellenwerte noch offen

UBI (UNBÖFI)

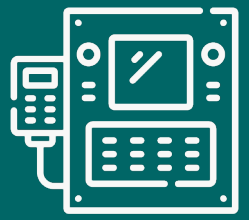
- Unternehmen im besonderen öffentliche Interesse
- Schützenswert aber ≠ KRITIS, in drei Gruppen:
  1. UBI Rüstung, Waffen und VS-IT (nach AWV)
  2. UBI Volkswirtschaftliche Bedeutung
  3. UBI Gefahrstoffe (Betriebsbereiche obere Kl.)
- Eigene UBI Cyber Security Pflichten

Mehr KRITIS-Anlagen und Betreiber

Sinkende Schwellenwerte

- ❑ Tiefere Schwellenwerte = mehr Betroffenheit bei KRITIS-Anlagen
- ❑ 5 Schwellenwerte sinken ↓
- ↓ Stromerzeugung deutlich tiefer
- ↓ IT Hosting/Housing/Exchanges tiefer
- ❑ 3 anderweitig geänderte Werte

Mehr KRITIS-Anlagen



- ❑ Neue KRITIS-Anlagen in Sektoren = mehr Betroffenheit bei Betreibern

→ Energie: 6 neue, 2 wegfallende
→ Gesundheit: 1 neue, 2 wegfallende
→ Transport: 6 neue, 1 wegfallende
→ IT und TK: 1 neue
→ Finanzen: 3 neue

Mehr KRITIS-Betreiber

- ❑ Die Regierung schätzt deutlich mehr KRITIS-Betreiber im IT-SiG 2.0
- ❑ +270 zu den ca. 1.600 bestehenden
- ❑ Vor allem bei Energie und Finanzen
- ❑ UBI, KRITIS-Entsorgung noch nicht berücksichtigt

Höhere Sanktionen

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)

Wer muss nun was machen?

Bestehende KRITIS-Betreiber

- Angriffserkennung SIEM SOC
  ab 2023
- Neue KRITIS-Anlagen prüfen
- Tiefere Schwellen-werte prüfen
- Neue Meldepflichten ans BSI

Neue Betreiber & Entsorger

- KRITIS-Anlagen identifzieren
- Als KRITIS beim BSI registrieren
- Cyber Security umsetzen
- Meldepflichten ans BSI

KRITIS Telekommunikation

- Kritische Kompo-nenten identifizieren
- Krit. Komponenten melden & freigeben

UBI/UNBÖFI

- Als UNBÖFI beim BSI registrieren
  ab 2021/23/24
- Cyber Security umsetzen
  ab 2023/24
- Meldepflichten ans BSI
  ab 2021/23/24

Alle: Auf EU Regulierung vorbereiten

from ~2022

Nichts verpassen zu Kritischen Infrastrukturen:

OpenKRITIS.de

(40+ Artikel, Webinare, Podcast)

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

Briefing Kit IT-Sicherheitsgesetz 2.0
Stand: 14. Januar 2022
Version: 1.6

© Copyright Paul Weissmann 2021-2022

Impressum

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn

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

Annex – Paragraphen

§8a (1a)	**Angriffserkennung**	§8b (3) §8b (3a)	**Registrierungspflicht KRITIS: unmittelbar BSI-Befugnis zur Einsicht & Festlegung**
§8b (4a)	Meldepflichten	§14 (1-4)	Mehr Sanktionen bis 20 Mio EUR Mehr Verstöße bei Betreibern(+11)
§9b	Kritische Komponenten	§4b §5c	BSI als zentrale Meldestelle IT-Sicherheit Informationsbedarf TK-Daten
§2 (10)	KRITIS-Siedlungsabfallentsorgung	§7a-§7d	BSI Untersuchungen von Produkten, Port-Scans bei Betreibern, Anordnungen TK/TMG
§8f	Unternehmen im besonderen öffentlichen Interesse: UNBÖFI und Cyber Security	§9a §9c	Zertifizierungen (Konformität) BSI Gütesiegel IT-Sicherheit
KritisV	Niedrigere Schwellenwerte (↓7) Mehr Anlagen (+14)	§4a §5a	Schutz der Bundesnetze durch das BSI, Zugriff auf Protokolldaten Bundes-IT

Annex – Quellen

- IT-Sicherheitsgesetz 2.0: Bundesgesetzblatt, .pdf, 27.5.2021
- Beschlussempfehlung IT-SiG 2.0: 19/28844, .pdf
- Entwurf IT-SiG 2.0 Regierung: 19/26106, .pdf
- Entwurf KritisV 2.0: 26.4.2021, .pdf
- Alle verfügbaren Versionen: AG KRITIS
- Das neue IT-Sicherheitsgesetz 2.0: OpenKRITIS