

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE

NIS2

- Ein Weckruf für die Cybersicherheit in Europa

-

Pascal Bliedung | Bechtle IT-Systemhaus Weimar GmbH |
Consultant

MIT SICHERHEIT AN ERSTER STELLE.

Bechtle IT-Security

Agenda

1. Historie und Entwicklung
2. Grundlagen und Begriffe
3. Sonderfälle
4. Betreiberpflichten
5. Geltungsbereiche
6. Maßnahmen der Betreiber

Vorstellung - Referent



Pascal Bliedung

Consultant

Bechtle am Standort Weimar tätig

Seit 2010 in der IT-Infrastruktur (Administration / Führungskraft)

Seit 2017 Schwerpunkte im Bereich IT-Security / Informationssicherheit

Zertifizierungen / relevante Trainings :

- ✓ 2017 **ISO/IEC 27001** Foundation | Zertifizierung
- ✓ 2020 **OWAPS TOP 10** Exploit Training
- ✓ 2020 **Greenbone** Vulnerability Management Training
- ✓ 2021 **PenTesting** & Netzwerkhacking FAU Erlangen
- ✓ 2022 **Computerstrafrecht** FAU Erlangen
- ✓ 2023 **CSP** Cyber Security Practitioner ISACA e.V. | Zertifizierung

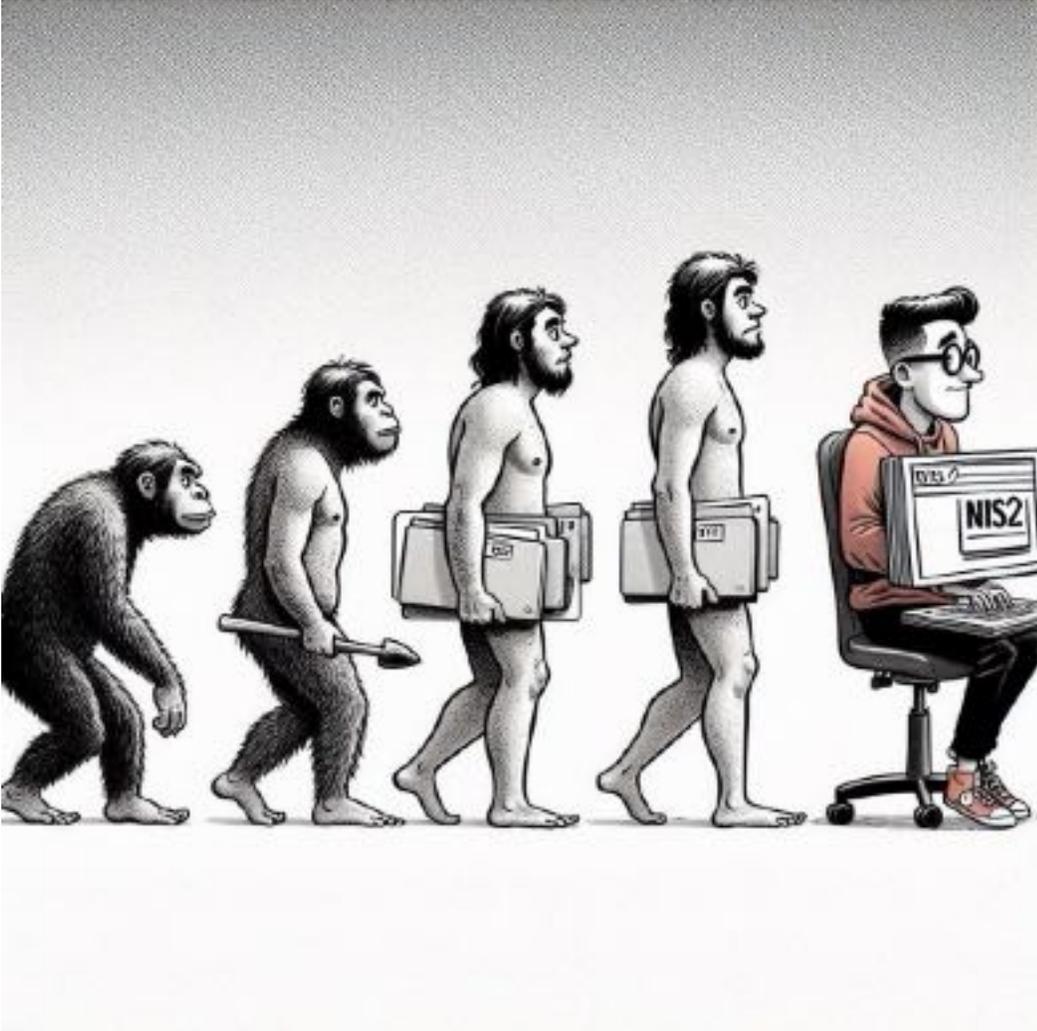
Historie & Entwicklung

IT-Sicherheitsgesetz

- 17.06.2015 – IT-Sicherheitsgesetz
- 18.05.2021 – IT-Sicherheitsgesetz 2.0
- Oktober 2024 – KRITIS-Dachgesetz

NIS1 und NIS2 (NIS2UmsuCG)

- NIS1-Richtlinie 08.08.2016
- 1. Entwurf im April 2023
- 2. Entwurf im Juli 2023
- 3. Entwurf (Diskussionspapier) September 2023
- 1. Referentenentwurf Dezember 2023
- 2. Referentenentwurf Mai 2023



Wichtige Grundlagen

Begriffe und Schwellwerte

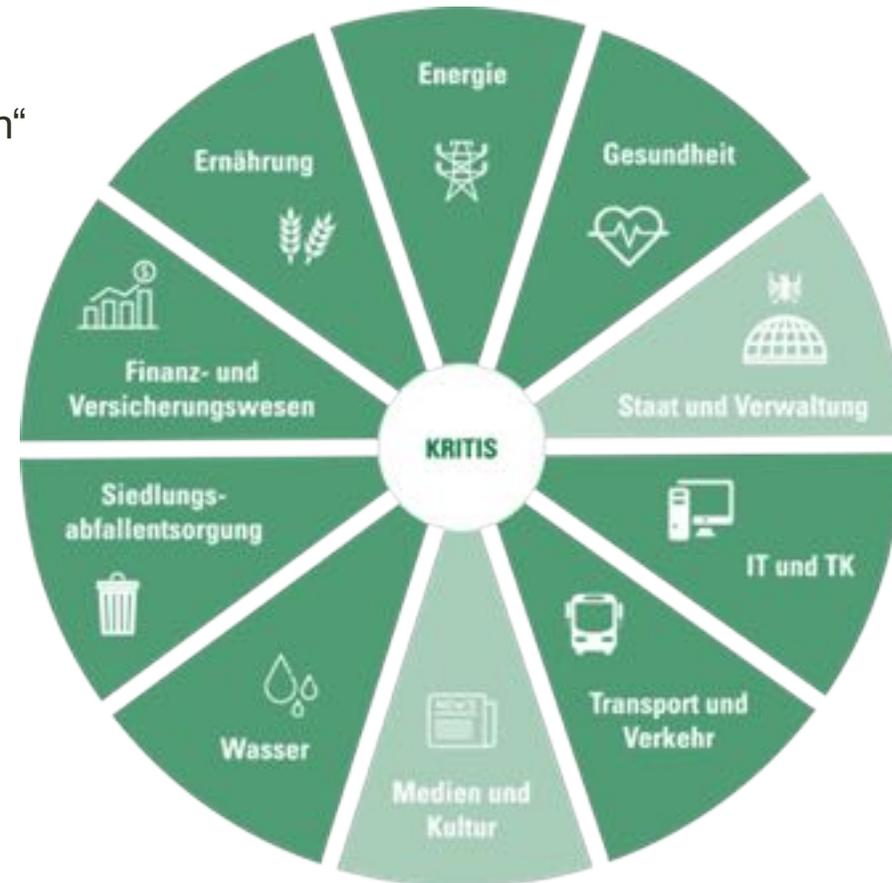
- BSIG: „besonders wichtige Einrichtungen“ = NIS2: „wesentliche Einrichtungen“
- NIS2: „wesentliche Einrichtungen“ („besonders wichtige Einrichtungen“)
 - ab 250 Mitarbeitern **oder**
 - ab 50 Mio. EUR Umsatz und Bilanz ab 43 Mio. EUR
 - **Ausnahmen** sind: qualifizierte Trusted Service Provider (z.B. GlobalSign), TLD-Registrare, DNS-Anbieter, TK-Anbieter (ab 50 Mitarbeiter oder Jahresbilanz & Jahresumsatz von jeweils über 10 Mio. EUR)
 - Kritische Anlagenbetreiber sind gleichgestellt
- NIS2: „wichtige Einrichtungen“
 - ab 50 Mitarbeitern **oder**
 - Ab 10 Mio. EUR Umsatz und Bilanz ab 10 Mio. EUR
 - **Ausnahmen:** Trusted Service Provider, TK-Anbieter (bis 50 Mitarbeiter oder Jahresbilanz & Jahresumsatz von jeweils bis 10 Mio. EUR)



Sonderfälle

Bundesverwaltung und KRITIS

- KRITIS-Betreiber werden „Betreiber kritischer Anlagen“
- Betreiber „erben“ Pflichten von „besonders wichtigen Einrichtungen“
- ausgenommen:
 - Institutionen der sozialen Sicherung
 - berufsständische Körperschaften (öR)
 - Industrie- und Handelskammern (IHK)



Pflichten von Betreibern und Einrichtungen

Pflicht	KRITIS	Wesentliche Einrichtungen	Wichtige Einrichtungen
Geltungsbereich	lt. KRITIS-Methodik	gemäß Schwellwerten	gemäß Schwellwerten
Risikomanagement	*	✓	✓
§31 (1): Erhöhte Anforderungen Risikomanagement	✓		
§31 (2): Erhöhte Anforderungen Risikomanagement	✓		
Meldepflichten	*	✓	✓
Registrierung	✓	✓	✓
Unterrichtungspflicht (Kunden)	*	✓	✓
Leitungsorgane	*	✓	✓
Nachweise	✓		

* implizit aus wesentlichen Einrichtungen

Geltungsbereich

§30 NIS2UmsuCG

- **Ziel:** Störungen der Verfügbarkeit, Integrität und Vertraulichkeit verhindern
- **Scope:** sämtliche IT-Systeme, Komponenten und Prozesse, die für die Erbringung der Dienste genutzt werden
- **Dienste:** sämtliche Aktivitäten der Einrichtung, für die IT-Systeme eingesetzt werden (auch Büro-IT & oder andere IT-Systeme einer Einrichtung)
- **Maßnahmen:** angemessen und je nach Risiko ausgerichtet (gemäß Risikoexposition)

Unklarheiten für KRITIS-Betreiber

- **Ursprünglich:** „IT-Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind“



notwendige Maßnahmen

§30 NIS2UmsuCG (abgeleitet aus Artikel 21 NIS2-Richtlinie)

- Risikoanalyse & -management
- Bewältigung von Sicherheitsvorfällen (Incident Response)
- Aufrechterhaltung & Wiederherstellung,
- Backup-Management, Krisen-Management
- Sicherheit der Lieferkette & der Entwicklung, Beschaffung & Wartung
- Management von Schwachstellen
- Bewertung der Effektivität von Cybersicherheit
- Schulungen Cybersicherheit & Cyberhygiene
- Kryptografie & Verschlüsselung
- Zugriffskontrolle und MFA
- Sichere Kommunikation (Sprach, Video- und Text)



Zeit für Ihre Fragen.

Weitere Infos:
[bechtle.com](https://www.bechtle.com)

