

NIS-2 – und was dann?

Der aktuelle Stand der IKT- und der Sicherheit kritischer Infrastruktur in Deutschland

Florian Achnitz, LL.M.

Clyde & Co Europe LLP

Herbstakademie 2026

Bedrohungslage & Verwundbarkeit

Bedrohungslage 2025/2026

Anhaltend hohe Bedrohung

SBI & ENISA verzeichnen angespannte Lage: Trend weg von wenigen Großangriffen hin zu vielen kleineren, hochfrequenten Attacken.

KMU im Fokus

Rund 80 % der Angriffe richten sich gegen kleine und mittlere Unternehmen. Phishing (-as-a-Service) & Schnelle Ausnutzung von Schwachstellen dominieren.

Doppelte Verwundbarkeit

Kritische Infrastrukturen stehen digital und physisch unter Beschuss (z. B. Brandanschlag Stromnetz Berlin Jan. 2026).

Digitalisierung als Risikoverstärker

-  **Wachsende Angriffsflächen:** Cloud, IoT, Industrie 4.0 und vernetzte Lieferketten schaffen kontinuierlich neue Einfallstore.
-  **Neue KI-Risiken:** Bedrohungen durch Indirect Prompt Injections & Evasion Attacks auf LLMs erfordern neue Schutzmechanismen.
-  **Ganzheitliche Resilienz gefordert:** Fokus wandelt sich von punktueller IT-Sorge zur strategischen Daueraufgabe für Staat & Wirtschaft.



Der aktuelle Rechtsrahmen

NIS-2 & CER-Umsetzung in Deutschland



NIS-2-Umsetzungsgesetz

In Kraft seit 6. Dezember 2025, ins. in Form des überarbeiteten BSIG:

- Erweitert Anwendungsbereich massiv auf ca. 29.500 Einrichtungen.
- Regulierung von "besonders wichtigen" & "wichtigen" Einrichtungen.
- Gesetzliche Pflichten zu Risikomanagement, Meldewesen & Geschäftsleitungshaftung.



KRITIS-Dachgesetz

Umsetzung der EU-CER-Richtlinie:

- Fokus auf physische & organisatorische Resilienz kritischer Anlagen.
- Abdeckung essenzieller Sektoren (Energie, Wasser, Transport, Entsorgung etc.).
- Verpflichtung zu angemessenem physischen Schutz & Notfallvorsorge.

Weitere Säulen der EU-Regulierung

Cyber Resilience Act (CRA):

Verordnet horizontale Sicherheitsanforderungen für Hardware & Software entlang der gesamten digitalen Wertschöpfungskette.

DORA (Finanzsektor):

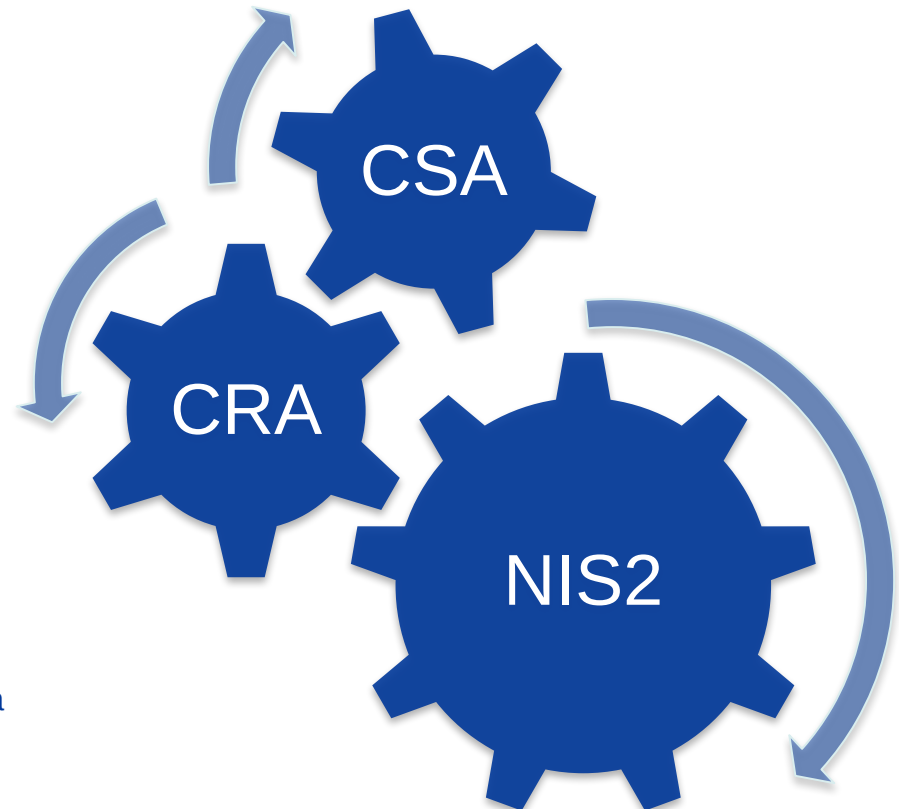
Stärkt die digitale operationale Resilienz für Banken, Versicherungen und deren IT-Drittdienstleister.

Produktsicherheit & KI-Verordnung:

Verpflichtende Risikomanagementmaßnahmen und Sicherheitsvorgaben für Künstliche Intelligenz.

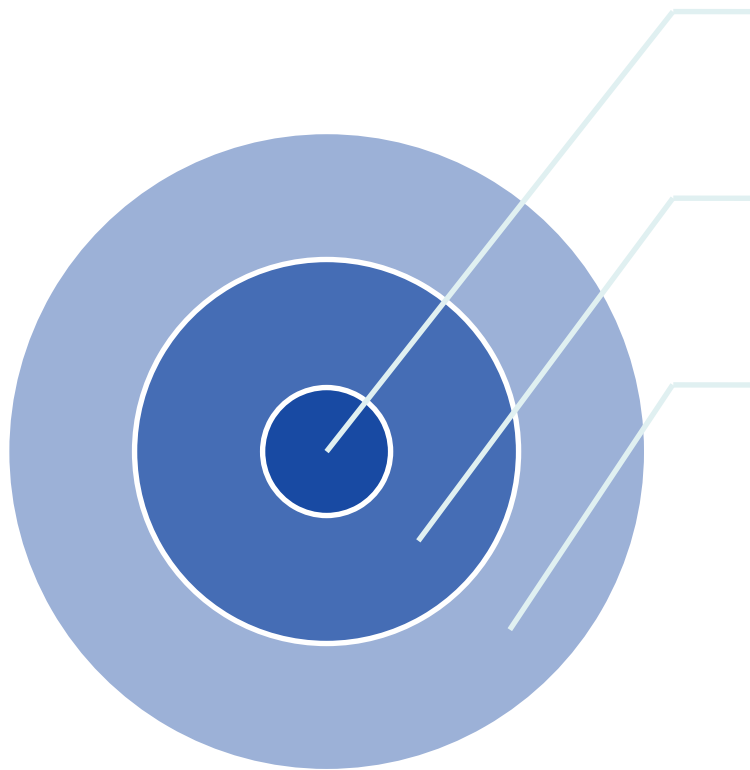
EU-Cybersicherheitsverordnung:

Schafft EU-weit harmonisierte Zertifizierungsschemata und definiert die Rolle der ENISA.



Fortentwicklung der EU-Architektur

Cybersecurity Act 2 & NIS-2-Refit

**Stärkung der ENISA:**

Operative Rolle beim Schutz vor Ransomware, Standardisierung & zentrale Anlaufstelle für Vorfälle.

Sichere IKT-Lieferketten:

EU-weites Verfahren zur Risikobewertung & Schutz vor Hochrisiko-Anbietern, insb. im Bereich Telekommunikation.

NIS-2-Präzisierung:

Rechtsklarheit, KMU/Mid-Cap-Entlastungen und Anpassung des Anwendungsbereichs, z.B. zur Erfassung unterseeischer Kabelinfrastrukturen.

Cybersicherheit im Kontext der „Digital Decade“

**Digitale
Transformation
der EU bis zum
Jahr 2030**

**Cybersicherheit als Schutzinstrument und
Ermöglichungsbedingung**

**Hohe Sicherheitsstandards als Grundpfeiler
der Ziele des Politikprogramms 2030 für die
Digitale Dekade**

**Cybersicherheit als
Querschnittsvoraussetzungen für das
Erreichen der Ziele**

Institutionelle und praktische Maßnahmen der Cybersicherheit



BSI & Lagezentrum

24/7 Nationales IT-Lagezentrum verarbeitet
ca. 2.800 Meldungen/Jahr; verstärkte
Aufsichts- & Koordinierungsrolle.



Public-Private- Partnerships

Allianz für Cyber-Sicherheit (>8.800
Mitglieder) & UP KRITIS als essenzielle
Austauschplattformen von Staat &
Wirtschaft.



Operative EU- Reserve

Cyber Solidarity Act (seit Feb. 2025)
etabliert EU-Cybersicherheitsreserve &
EU Cyber Blueprint für Krisenreaktion.

Fragen und Diskussion

Vielen Dank für Ihre Aufmerksamkeit!



Florian Achnitz, LL.M.
Senior Associate
Düsseldorf

Florian.Achnitz@clydeco.com
[LinkedIn](#)