(Cyber-)Resilienz

Ralf Kneuper, IU Internationale Hochschlule

GI-FG SECMGT 03/2026

Ralf Kneuper

- PhD Computer Science, Univ. of Manchester
- LL.M. IT und Recht, Uni Saarbrücken
- Professor für Datenschutz und IT-Sicherheit, IU Internationale Hochschule
  - Kontakt: `ralf.kneuper@iu.org`
- Beratung für Datenschutz und Qualitätsmanagement
  - Kontakt: `ralf@kneuper.de`
- Mitglied im Leitungsgremium der GI-FG SECMGT

Resilienz

- Begriff kommt ursprünglich aus Pädagogik und Psychologie
- Widerstandsfähigkeit / Anpassungsfähigkeit an Herausforderungen / Belastbarkeit
- „Prozess, in dem Personen auf Probleme und Veränderungen mit Anpassung ihres Verhaltens reagieren“ (Wikipedia)

Ebenen der Resilienz

- übergreifende Infrastruktur
  - z.B. Brandanschlag auf das Berliner Stromnetz 2026
- Unternehmen
  - einschließlich Resilienz gegen Probleme der übergreifenden Infrastruktur

Cybersecurity vs. Cyberresilienz

- Cybersecurity: Abwehr von Cyber-Bedrohungen und -Angriffen
- Cyberresilienz: Widerstandsfähigkeit, auch wenn Angriffe erfolgreich sind
- Unterschiedlicher Fokus, aber keine eindeutige Trennung
- EU-Recht legt derzeit stärkeren Fokus auf die Cyberresilienz

Quelle: L. A. Bygrave, "Cyber Resilience versus Cybersecurity as Legal Aspiration,"14th International Conference on Cyber Conflict: Keep Moving! (CyCon), Tallinn, Estonia, 2022, pp. 27-43, doi: http://doi.org/10.23919/CyCon55549.2022.9811084.

Koalitionsvertrag 2025

Die Resilienz unseres Landes stärken wir, indem wir die IT-Sicherheit verbessern, besonders bei kritischen Infrastrukturen, und robuste Wertschöpfungsketten aufbauen (unter anderem in der Chip- und Halbleitertechnik). Fähigkeiten und Produkte mit dem Ziel, Schutz im Cyberraum zu gewährleisten gelten als Schlüsseltechnologien. Wir investieren in IT-Sicherheits- und anwendungsorientierte Resilienzforschung. Die öffentliche IT-Sicherheit wird durch Notfallmanagement und präventive Beratungsangebote für kleine und mittlere Unternehmen verbessert.

(Zeilen 2184-2190)

Cyberresilienz-Verordnung (CRA) und NIS2

Verwenden den Begriff der „(Cyber-)Resilienz“ im Titel, aber ohne ausdrückliche Definition
“Verordnung (EU) 2024/2847 . . . über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen . . .”

Anforderungen an Cyberresilienz nach CRA

- Forderung nach grundlegender Cybersicherheit für alle in der EU verkauften Produkte mit “digitalen Elementen”
- Betrifft
  - vernetzte Hardwareprodukte, z.B. Smartphones, Laptops, Firewalls, Smart-Meter-Gateways . . .
  - Softwareprodukte, z.B. Buchhaltungssoftware, Computerspiele, mobile Apps . . .
- Anforderungen:
  - Security by Design
  - Nachweispflichten / Konformitätserklärungen
  - Offenlegung von Schwachstellen
  - Sicherheitsupdates im gesamten Supportzeitraum

Anforderungen an Cyberresilienz nach NIS2

- Mitgliedsstaaten erstellen im Rahmen ihrer nationalen Cybersicherheitsstrategie Konzepte “zur Stärkung des Grundniveaus für Cyberresilienz und Cyberhygiene kleiner und mittlerer Unternehmen” (Art. 7 (2)(i))
- Anforderungen “genaue und vollständige Domänennamen-Registrierungsdaten” in TLD-Namenregister (Art. 28 (1) NIS2; ähnlich § 49 (1) BSI-Gesetz 2025)

DORA

Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor

„Digitale operationale Resilienz“ ist

> *die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen*

Art. 3 (1) DORA

Anforderungen nach DORA

- IKT-Risikomanagement
- Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle
- Testen der digitalen operationalen *Resilienz* einschließlich Threat-led Penetration Testing (TLPT)
- Management des IKT-Drittparteienrisikos, einschließlich Informationsregister und Anzeigepflichten
- Überwachungsrahmen für kritische IKT-Drittdienstleister
- Vereinbarungen über den Austausch von Informationen sowie Cyberkrisen- und Notfallübungen

Quelle: `https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html`

ISO 22316:2017

Security and resilience — Organizational resilience — Principles and attributes

Aktualisierung in Arbeit (“Expected to be replaced by ISO/DIS 22316 within the coming months” – Stand 2026-03-13)

organizational resilience: ability of an organization to absorb and adapt in a changing environment

ISO 22316:2017 – Grundsätze

Quelle: https://www.dinmedia.de/de/themenseiten/resilienz-in-unternehmen