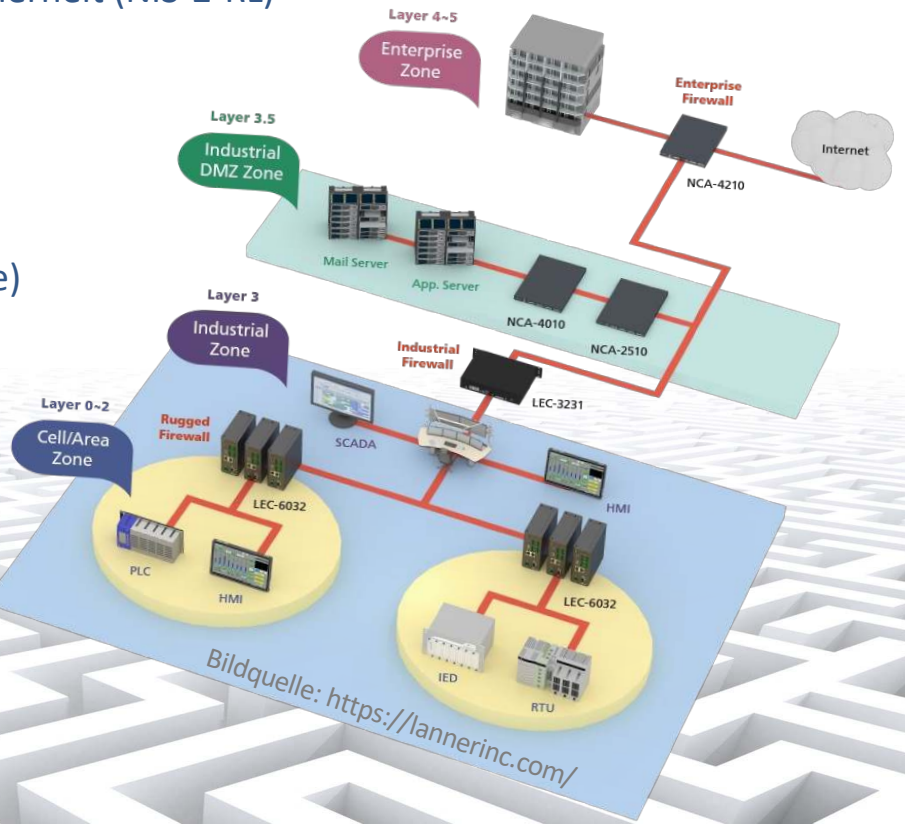
Umsetzung von NIS2 in Deutschland – Status und Ausblick

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Die Vielfalt der aktuellen EU-Regulierung zur Cybersicherheit

- Richtlinie zur Netz- und Informationssicherheit (NIS-2-RL)
- Cyber Solidarity Act (CSA)
- Cyber Resilience Act (CRA)
- Digital Services Act (DSA)
- Artificial Intelligence Act (AI Act)
- CER-Richtlinie (Critical Entities Resilience)
- …



NIS2
CSA
CRA
DSA
AI Act
CER

Richtlinie zur Netz- und Informationssicherheit (NIS-2-Richtlinie)

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27. Dezember 2022, S. 80, im Folgenden NIS-2-Richtlinie)

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

NIS2
CSA
CRA
DSA
AI Act
CER

- Ziel der NIS-2-Richtlinie: EU-weite Harmonisierung der Cybersicherheit nach EU-Vorgaben
  - »Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft, mit denen in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll.«

    https://www.bundestag.de/dokumente/textarchiv/2024/kw45-pa-inneres-cyber-1026336

- Struktur
  - 73 Seiten, 144 Erwägungsgründe, 9 Kapitel, 46 Artikel, 3 Anhänge

Umsetzung der NIS-2-RL durch die EU-Mitgliedstaaten bis zum 17.10.2024

Richtlinie zur Netz- und Informationssicherheit (NIS-2-Richtlinie)

- Methoden
  - Definition von Schwellenwerten für die Sektoren
  - Ergreifen von geeigneten Sicherheitsmaßnahmen
  - Verpflichtung zur Unterrichtung über schwerwiegende Vorkommnisse

- Maßnahmen
  - Aufbau von Computer Security Incident Response Teams (CSIRT)
  - Aufbau einer nationalen Netz- und Informationssystembehörde (NIS)
  - Aufbau einer Kooperationsplattform zum Informationsaustausch zwischen den EU-Mitgliedstaaten
  - Aufbau einer sektorübergreifenden Sicherheitskultur

NIS2
CSA
CRA
DSA
AI Act
CER

Erfasste Einrichtungen nach Art. 3 NIS-2-RL

- Wesentliche Einrichtungen (Art. 3 Abs. 1)
  - proaktive Aufsicht durch die Aufsichtsbehörden
  - nicht nur anlassbezogene Pflichten

»Geldbußen mit einem Höchstbetrag von mindestens 10 000 000 EUR oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens« (Art. 34 Abs. 4)

- Wichtige Einrichtungen (Art. 3 Abs. 2)
  - reaktive, anlassbezogene Aufsicht durch die Aufsichtsbehörden

»Geldbußen mit einem Höchstbetrag von mindestens 7 000 000 EUR oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes« (Art. 34 Abs. 5)

NIS2
CSA
CRA
DSA
AI Act
CER

Pflicht zur Registrierung nach Art. 3 Abs. 3:

Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine **Liste von wesentlichen und wichtigen Einrichtungen** und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen.

Aktualisierung der Liste alle zwei Jahre (Art. 3 Abs. 5)

18 Sektoren nach Art. 2 Abs. 1 der NIS-2-RL

- Anhang I Sektoren mit hoher Kritikalität
  - Energie: Elektrizität, Fernwärme und -kälte, Erdöl, Erdgas, Wasserstoff
  - Verkehr: Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr
  - Bankwesen
  - Finanzmarktinfrastrukturen
  - Gesundheitswesen
  - Trinkwasser
  - Abwasser
  - Digitale Infrastruktur
  - Verwaltung von IKT-Diensten (Business-to-Business)
  - öffentliche Verwaltung
  - Weltraum

Anmerkung: In Art. 2 findet sich häufiger die Formulierung »unabhängig von der Größe der Einrichtungen«.

- Anhang II Sonstige kritische Sektoren
  - Post- und Kurierdienste
  - Abfallbewirtschaftung
  - Produktion, Herstellung und Handel mit chemischen Stoffen
  - Produktion, Verarbeitung und Vertrieb von Lebensmitteln
  - Verarbeitendes Gewerbe/Herstellung von Waren
  - Anbieter digitaler Dienste
  - Forschung

NIS2
CSA
CRA
DSA
AI Act
CER

- Herstellung von Medizinprodukten und In-vitro-Diagnostika
- Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
- Herstellung von elektrischen Ausrüstungen
- Maschinenbau
- Herstellung von Kraftwagen und Kraftwagenteilen
- sonstiger Fahrzeugbau

Erfasste Einrichtungen nach Art. 3 NIS-2-RL

Unternehmensgröße als Kriterium kann ebenfalls greifen. In Art. 2 findet sich häufiger die Formulierung »unabhängig von der Größe der Einrichtungen«.

NIS2
CSA
CRA
DSA
AI Act
CER

- Beispiel:
  - Anbieter öffentlich zugänglicher Telekommunikationsdienste
    - besonders wichtige Einrichtung: (§ 28 Absatz 1 Ziffer 3)

      a) >= 50 Mitarbeiter **oder**

      b) Jahresumsatz/Jahresbilanz >10 Mio. Euro
    - wichtige Einrichtung: (§ 28 Absatz 2 Ziffer 2)

      a) < 50 Mitarbeiter **und**

      b) Jahresumsatz/Jahresbilanz <=10 Mio. Euro

Gliederung der NIS-2-Richtlinie

Kap. 1 Allg. Best.

Art. 1	Gegenstand
Art. 2	Anwendungsbereich
Art. 3, 4	Wesentliche und wichtige Einrichtungen
Art. 5	Mindestharmonisierung (Mindeststandards an die Cybersicherheit)
Art. 6	Begriffsbestimmungen

K2-3 Koordinierungsrahmen

Art. 7	Nationale Cybersicherheitsstrategie
Art. 8	Zuständige Behörden und zentrale Anlaufstellen
Art. 9	Nationale Rahmen für das Cyberkrisenmanagement
Art. 10-11	Computer-Notfallteams (CSIRTs)
Art. 12	Koordinierte Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank
Art. 13	Zusammenarbeit auf nationaler Ebene
Art. 14-19	Zusammenarbeit auf Unions- und internationaler Ebene

Kap. 4

Art. 20-23	Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit
Art. 24-25	Cybersicherheitszertifizierung und Normung

Kap. 5-9

Art. 25-28	Zuständigkeit, Territorialität, Domänennamen-Registrierungsdatenbanken
Art. 29-30	Informationsaustausch und freiwillige Meldung relevanter Informationen
Art. 31-37	Aufsicht und Durchsetzung, Verhängung von Geldbußen, Saktionen, Amtshilfe
Art. 38-46	Rechtsakte und Schlussbestimmungen

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

- Ausgangslage
  - Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324)
  - Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122)

NIS2
CSA
CRA
DSA
AI Act
CER

- Änderungsbedarf durch NIS-2
  - von NIS-2 neu vorgegebene Einrichtungskategorien
  - signifikante Ausweitung des bisher beschränkten Anwendungsbereichs
  - bisher ca. 4.500 verpflichtete Organisationen in Deutschland
    - Betreiber Kritischer Infrastrukturen
    - Anbieter digitaler Dienste
    - Unternehmen im besonderen öffentlichen Interesse
  - künftig ca. 29.500 verpflichtete Organisationen in Deutschland aus den 18 Sektoren
    - 11 Sektoren mit hoher Kritikalität (Anhang I), 7 Sonstige kritische Sektoren (Anhang II)

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

- Änderungsbedarf durch NIS-2 (Fortsetzung)
  - Katalogs der Mindestsicherheitsanforderungen aus Art. 21 Abs. 2 NIS-2 in das BSI-Gesetz
  - Meldepflicht bei Vorfällen: bisher einstufig, nun dreistufig (Art. 23 Abs. 4 NIS-2-RL)
    - innerhalb von 24 Stunden Frühwarnung
    - nach 72 Stunden erste Bewertung des Vorfalls
    - spätestens nach 1 Monat Abschlussbericht
  - erweiterte Aufsichtsmaßnahmen des BSI
  - gesetzliche Anforderungen an das Informationssicherheitsmanagement des Bundes
    - Abbildung der zugehörigen Rollen und Verantwortlichkeiten auf Bundesebene
    - Etablierung eines CISO Bund als zentraler Koordinator auf Bundesebene

NIS2
CSA
CRA
DSA
AI Act
CER

- Quellen und weiterführende Infos
  - https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html
  - https://www.heise.de/news/Cyberresilienz-muss-in-die-Koepfe-kommen-Bundestag-beraet-ueber-NIS2-9978158.html

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Umsetzungsstand zum NIS2UmsuCG

14.12.2022 Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

07.05.2024 Veröffentlichung des Referentenentwurfs
https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE.pdf

28.05.2024 Stellungnahme der Gesellschaft für Informatik (GI) zum Referentenentwurf
https://gi.de/meldung/gi-sieht-baustellen-im-nis2-umsetzungsgesetz

24.07.2024 Verabschiedung eines Regierungsentwurfs
https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf

02.10.2024 Veröffentlichung Regierungsentwurf als Bundestagsdrucksache 20/13184
https://dserver.bundestag.de/btd/20/131/2013184.pdf

11.10.2024 1. Lesung des NIS-2-Umsetzungsgesetz im Deutschen Bundestag

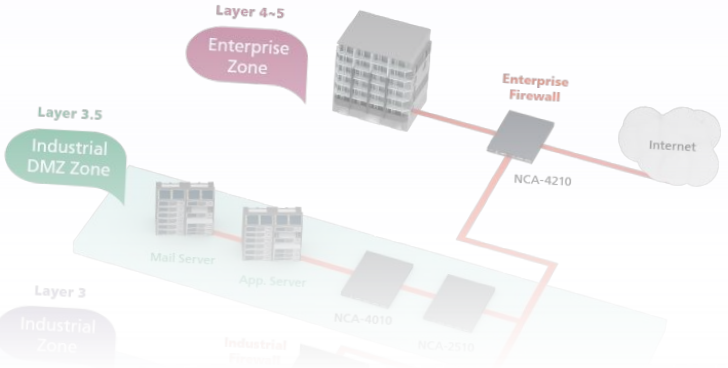
17.10.2024 Umsetzungsfrist der RL durch die EU-Mitgliedstaaten

04.11.2024 Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages
https://www.bundestag.de/dokumente/textarchiv/2024/kw45-pa-inneres-cyber-1026336

28.11.2024 EU leitet Vertragsverletzungsverfahren 22 EU-Mitgliedstaaten ein

Weitere Gesetze mit Wechselwirkungen

- Cyber Solidarity Act (CSA)
- Cyber Resilience Act (CRA)
- Digital Services Act (DSA)
- Artificial Intelligence Act (AI Act)
- CER-Richtlinie (Critical Entities Resilience)
- …
- Kritis-Dachgesetz: Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen)



NIS2
CSA
CRA
DSA
AI Act
CER

»Analoges Pendant zur NIS-2-Richtlinie« (Heise.de)

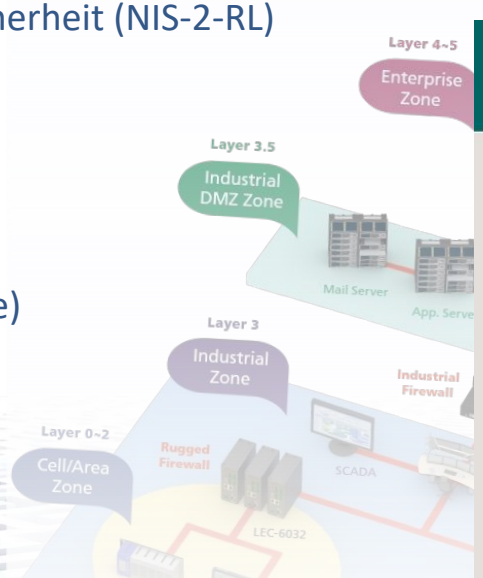
27.12.2022 Richtlinie (EU) 2022/2557 (CER-Richtlinie)
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557

21.12.2023 Veröffentlichung des Referentenentwurfs
https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG-2.pdf

06.11.2024 Verabschiedung eines Regierungsentwurfs
https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/KM4/regentwurf-kritisDachG.pdf

Die Vielfalt der aktuellen EU-Regulierung zur Cybersicherheit

- Richtlinie zur Netz- und Informationssicherheit (NIS-2-RL)
- Cyber Solidarity Act (CSA)
- Cyber Resilience Act (CRA)
- Digital Services Act (DSA)
- Artificial Intelligence Act (AI Act)
- CER-Richtlinie (Critical Entities Resilience)
- …



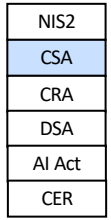
A. Herb: Die Digitale Dekade der EU. Wegweiser zum neuen Datenrecht und Datenschutzrecht in Deutschland und Europa, Boorberg Verlag, 2025

Leitfäden und Übersichten zu Data Governance Act - Digital Markets Act - Digital Services Act - Data Act - Artificial Intelligence Act - KI-Verordnung - Datenschutz-Grundverordnung - Mediendatenschutz - und weitere europäische Verordnungen sowie deutsche Begleitgesetze (z.B. DDG)

Cyber Solidarity Act

- Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)

Der CSA wurde am 15.01.2025 im Amtsblatt der EU veröffentlicht.



- Ziel
  - Prävention, Erkennung und Reaktion auf Cyber-Sicherheitsvorfälle verbessern

- Methoden
  - Aufbau von sog. Security Operations Centres (SOCs) innerhalb der EU-Mitgliedsländer
  - Zusammenfassung der SOCs in länderübergreifenden Cyber-Hubs
  - Etablieren eines Cybersecurity Emergency Mechanism (Cybernotfallmechanismus)
  - Cybersecurity Incident Review Mechanism (Mechanismus zur Überprüfung von Vorfällen)

Cyber Resilience Act (CRA)

- Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), *engl. Cyber Resilience Act*

Der CRA tritt am 10.12.2024 in Kraft und gilt ab 11.12.2027.

- Ziel
  - Cybersicherheit für den gesamten Produktlebenszyklus
  - definiert Sicherheitsanforderungen für Produkte mit sog. digitalen Elementen
  - digitale Elemente: Hardware und Software

- Methoden
  - Schwachstellen-Management, Update-Management
  - Updates für die gesamte Laufzeit eines Produkts

NIS2
CSA
CRA
DSA
AI Act
CER

Cyber Resilience Act (CRA)

- Fokus
  - private digitale Geräte wie Computer, Handys, Router, IoT-Devices, smarte Haushaltsgeräte, smartes Spielzeug, aber auch Industrial IoT

- Classification of products with digital elements
  - CRA Art. 7 Important products with digital elements
  - CRA Art. 8 Critical products with digital elements
  - Verweis auf Annex III

- Querbezüge zu
  - NIS-2-RL (Annex III)
  - High-Risk AI Systems (CRA Art. 12)
  - AI Act

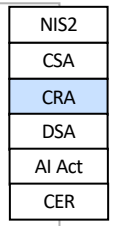
Class 1

- Identity management systems
- Standalone and embedded browsers
- Password managers
- Malware detection systems
- Network management systems
- Public Key Infrastructure (PKI)
- Routers and switches
- Field-programmable gate arrays (FPGA)
- Internet connected toys
- Personal wearable products
- …

Class 2

- Hypervisors and container systems
- Firewalls, intrusion detection and prevention systems
- Tamper-resistant microprocessors
- Tamper-resistant microcontrollers

Annex III



Digital Services Act (DSA)

- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

NIS2
CSA
CRA
DSA
AI Act
CER

- Ziel
  - besserer Schutz vor Verbreitung illegaler Inhalte im Internet
  - Etablieren von Meldeverfahren und Sperrungen
  - Geldbußen von bis zu 6 Prozent des weltweiten Umsatzes

- Teil eines Gesetzespakets
  - gemeinsam mit Digital Markets Act (DMA)
- Querbezüge auch zur »Chatkontrolle«
  - »Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern« (Prevent and Combat Child Sexual Abuse) aus 2022

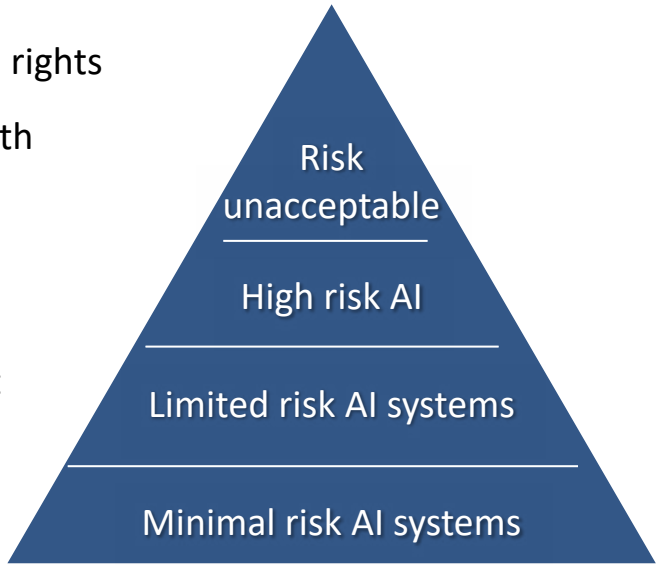
AI Act

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

NIS2
CSA
CRA
DSA
AI Act
CER

- Risikobasierte Klassifikation von KI-Systemen
  - Prohibited AI systems: contradict Union values, fundamental rights
  - High risk AI systems: Permitted but subject to compliance with specific product requirements and operator obligations
  - Limited risk AI systems: Permitted but subject to specific transparency and disclosure obligations
  - Minimal risk AI systems: Permitted, with no additional AI Act requirements. It is important to emphasize the importance of the GDPR in this context.

+ General Purpose AI (GPAI) models



Prohibited AI practices – Unacceptable Risk

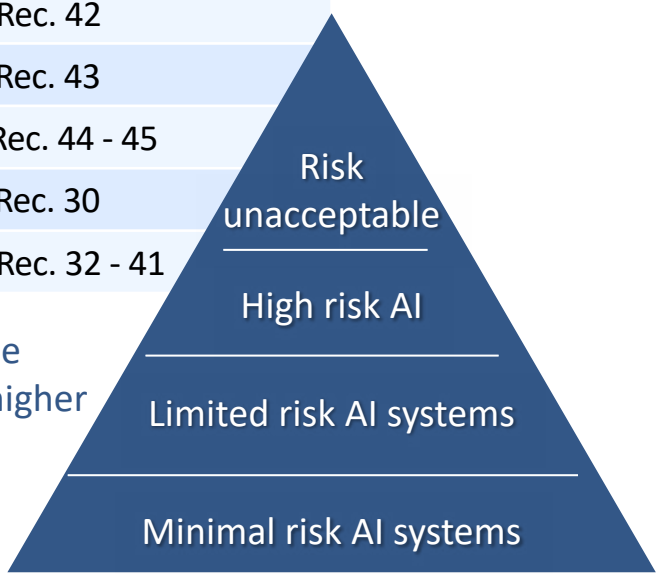
prohibitions will take effect on February 2, 2025

- Art. 5 identifies eight AI practices that are prohibited due to their unacceptable risk

Subliminal, manipulative or deceptive techniques	Art. 5(1)(a), Rec. 28 & 29
Exploitation of vulnerabilities	Art. 5(1)(b), Rec. 28 & 29
Social scoring	Art. 5(1)(c), Rec. 31
Profiling for criminal risk assessment	Art. 5(1)(d), Rec. 42
Facial recognition database	Art. 5(1)(e), Rec. 43
Inference of emotions in working life and education	Art. 5(1)(f), Rec. 44 - 45
Biometric categorisation	Art. 5(1)(g), Rec. 30
Real-time remote biometric identification in public spaces	Art. 5(1)(h), Rec. 32 - 41

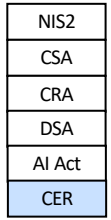
- Sanctioned by fines up to 35 million EUR or 7% of total worldwide annual turnover for the proceeding financial year, whichever is higher
- Most prohibitions have exceptions – requires individual analysis
- list will be re-assessed annually –not final

NIS2
CSA
CRA
DSA
AI Act
CER



CER-Richtlinie (Critical Entities Resilience) – Resilienz kritischer Einrichtungen

- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC



- Ziel
  - bessere Resilienz bei kritischen Infrastrukturen
  - recht strenge Meldepflichten (innerhalb von 24 Stunden) nach einem Vorfall

- Die CER-RL löst die European Critical Infrastructures Direktive von 2008 ab
  - Umsetzung in nationales Recht bis 17.10. 2024 gefordert – in KRITIS-Dachgesetz geplant
- Critical Entities (kritische Einrichtungen)
  - unter CER-RL regulierte Unternehmen als Critical Entities bezeichnet
    - mit Sektoren aus NIS-2-RL (Anhang I) fast deckungsgleich
    - vgl. auch KRITIS-Sektoren aus BSI-Gesetz (BSI-KritisV)
- Erstellung eines Resilienz-Plans: enge Bezüge zu ISO 27001/27002

Frist zur Ermittlung der kritischen Einrichtungen für die im Anhang festgelegten Sektoren und Teilsektoren: 17. Juli 2026

Sektoren nach Art. 2 Abs. 1 der NIS-2-RL und Vergleich mit der CER-RL

- **Anhang I Sektoren mit hoher Kritikalität**
  - Energie: Elektrizität, Fernwärme und -kälte, Erdöl, Erdgas, Wasserstoff
  - Verkehr: Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr
  - Bankwesen
  - Finanzmarktinfrastrukturen
  - Gesundheitswesen
  - Trinkwasser
  - Abwasser
  - Digitale Infrastruktur
  - Verwaltung von IKT-Diensten (Business-to-Business)
  - öffentliche Verwaltung
  - Weltraum

+ öffentlicher Verkehr (CER-RL)

nur NIS-2-RL

+ Produktion, Verarbeitung und Vertrieb von Lebensmitteln (CER-RL)

- **Anhang II Sonstige kritische Sektoren**
  - Post- und Kurierdienste
  - Abfallbewirtschaftung
  - Produktion, Herstellung und Handel mit chemischen Stoffen
  - Produktion, Verarbeitung und Vertrieb von Lebensmitteln
  - Verarbeitendes Gewerbe/Herstellung von Waren
  - Anbieter digitaler Dienste
  - Forschung

Anhang II nur NIS-2-RL

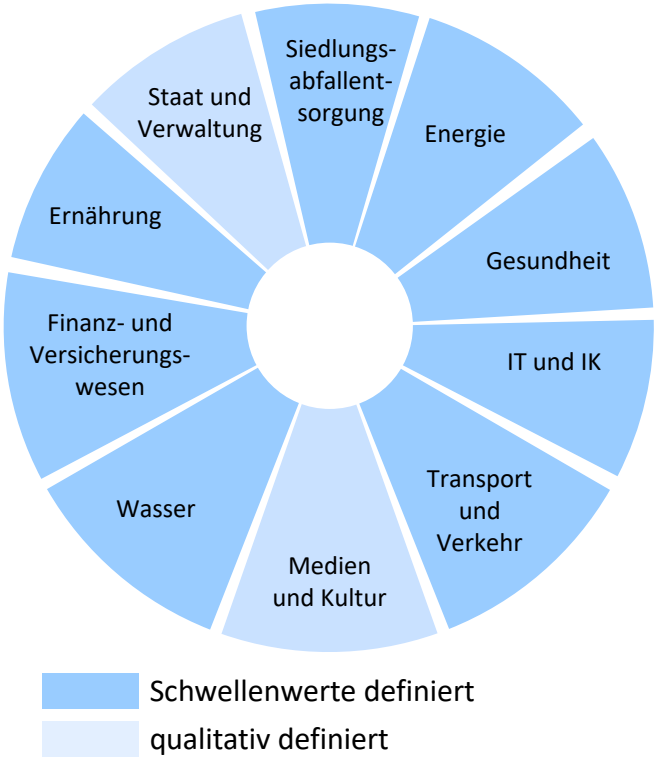
- Herstellung von Medizinprodukten und In-vitro-Diagnostika
- Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
- Herstellung von elektrischen Ausrüstungen
- Maschinenbau
- Herstellung von Kraftwagen und Kraftwagenteilen
- sonstiger Fahrzeugbau

Exkurs: Sektoren kritischer Infrastrukturen nach BSI-KritisV

https://www.kritis.bund.de

- Energie
  - Elektrizität (≥420 MW), Gas, Kraftstoff und Heizöl, Fernwärme (≥2300 GWh/Jahr)
- Gesundheit
  - medizinische Versorgung/Krankenhäuser (≥30.000 vollstationäre Fälle/Jahr), verschreibungspflichtige Arzneimittel und Blut- und Plasmakonzentrate, Labordiagnostik (≥1,5 Mio. Aufträge/Jahr)
- Informationstechnik und Telekommunikation
  - Zugangs-, Übertragungsnetze (≥100.000 Anschlüsse), DNS-Resolver, Rechenzentren, Content Delivery Networks (≥75.000 TByte/Jahr), Certificate Authorities
- Siedlungsabfallentsorgung
  - neu seit 2021 mit Novellierung des IT-Sicherheitsgesetzes, Schwellenwerte für Restmüll, Bioabfall, Glas etc. in Mg/Jahr

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)



Exkurs: Sektoren kritischer Infrastrukturen nach BSI-KritisV

https://www.kritis.bund.de

- Transport und Verkehr
  - Personen- und Güterverkehr, Luftverkehr, Schienenverkehr, Binnen- und Seeschifffahrt, Straßenverkehr, öffentlicher Personennahverkehr (≥125 Mio. Fahrgäste/Jahr), Logistik
- Wasser
  - Trinkwasserversorgung, Abwasserbeseitigung
- Finanz- und Versicherungswesen
  - Bargeldversorgung (≥15 Mio. Transaktionen/Jahr), kartengestützter (≥21,5 Mio. Transaktionen/Jahr) und konventioneller Zahlungsverkehr, Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften, Versicherungsdienstleistungen
- Ernährung
  - Lebensmittelproduktion,-verarbeitung, -handel

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)

CER-Richtlinie (Critical Entities Resilience)

- Wesentliche Maßnahme: Erstellung eines sog. Resilienz-Plans
  - Risiko-Bewertung: Ausfallrisiken identifizieren und bewerten
  - Allgemeine Präventionsmaßnahmen gegen Sicherheitsvorfälle
  - Physische Sicherheitsmaßnahmen: Perimeterschutz, Zutrittskontrolle
  - Risiko- und Krisenmanagement
  - Business Continuity Management (BCM)
  - Personell Security
  - Awareness-Maßnahmen

NIS2
CSA
CRA
CER

- enge Bezüge zu ISO 27001/27002

Security Policy **2013**
Organization of Information Security
Human Resources Security
Asset Management
Access Control
Cryptography
Physical and Environmental Security
Operations security
Communications Security
Information Systems Acquisition, Development, Maintenance
Supplier Relationships
Information Security Incident Management
Information Security Aspects of Business Continuity
Compliance

Organizational controls (37 Maßnahmen) **2022**
People controls (8 Maßnahmen)
Physical controls (14 Maßnahmen)
Technological controls (34 Maßnahmen)

Kritik am NIS2UmsuCG-E in der Fassung vom 02.10.2024

Im Rahmen der Anhörung zum NIS2UmsuCG-E am 04.11.2024 im Innenausschuss des Deutschen Bundestages wurden einige wichtige Kritikpunkte am NIS2UmsuCG-E genannt.

Quellen und weitere Infos unter https://www.bundestag.de/dokumente/textarchiv/2024/kw45-pa-inneres-cyber-1026336

- Allgemeine Kritik an den EU-Richtlinien und deren Umsetzung:
  - Chance für EU-weite Harmonisierung der IT-Sicherheitsregulierung wurde verpasst
  - Forderung nach besserer Verzahnung des NIS2UmsuCG mit dem KRITIS-Dachgesetz
    - vermutlich bestenfalls halbherzige Berücksichtigung bei nächstem Entwurf des NIS2UmsuCG
- Begriffliche Abweichung von der NIS-2-Richtlinie
  - NIS-2-RL: Wesentliche und wichtige Einrichtungen (Art. 3 NIS-2-RL)
  - NIS2UmsuCG-E: Besonders wichtige Einrichtungen und wichtige Einrichtungen (§ 28 BSIG)
  - zusätzlich noch im NIS2UmsuCG-E: Betreiber kritischer Anlagen: »die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt« (§ 28 Absatz 7 BSIG)
    - vermutlich keine Berücksichtigung bei nächstem Entwurf des NIS2UmsuCG

Im Rahmen der Anhörung zum NIS2UmsuCG-E am 04.11.2024 im Innenausschuss des Deutschen Bundestages wurden einige wichtige Kritikpunkte am NIS2UmsuCG-E genannt.

Quellen und weitere Infos unter https://www.bundestag.de/dokumente/textarchiv/2024/kw45-pa-inneres-cyber-1026336

- erhebliche und nennenswerte Schwächen aus Datenschutzsicht
  - Meldung nur »offensichtlicher« Datenschutzverletzungen (§ 7 Absatz 8, § 61 Absatz 11 BSIG)
  - Regelung wurde auch kritisiert vom Deutschen Bundesrat
  - Regelungen bleiben hier auch hinter denen der DSGVO zurück
    - vermutlich Berücksichtigung bei nächstem Entwurf des NIS2UmsuCG
- mangelnde Unabhängigkeit des BSI als nationale Cybersicherheitsbehörde
  - Zielkonflikt: Sicherheitslücken zum Schutz der Bürger/innen und der Wirtschaft schnellstens schließen vs. Sicherheitslücken durch Sicherheits- und Ermittlungsbehörden heimlich ausnutzen
  - Funktion des CISO Bund im Gesetzentwurf konkretisieren
    - vermutlich halbherzige Berücksichtigung bei nächstem Entwurf des NIS2UmsuCG

Im Rahmen der Anhörung zum NIS2UmsuCG-E am 04.11.2024 im Innenausschuss des Deutschen Bundestages wurden einige wichtige Kritikpunkte am NIS2UmsuCG-E genannt.

Quellen und weitere Infos unter https://www.bundestag.de/dokumente/textarchiv/2024/kw45-pa-inneres-cyber-1026336

- Zahlreiche Ausnahmen für Bundesbehörden
  - fehlende Vorbildwirkung des Staates; »wenn wir selber nicht bereit sind zu tun, was wir von der Wirtschaft erwarten« (BSI-Präsidentin Claudia Plattner)
  - Unterscheidung der Bedrohungslage für staatliche und nichtstaatliche Akteure ist weltfremd bzw. konträr zur realen Faktenlage
    - vermutlich keine Berücksichtigung bei nächstem Entwurf des NIS2UmsuCG

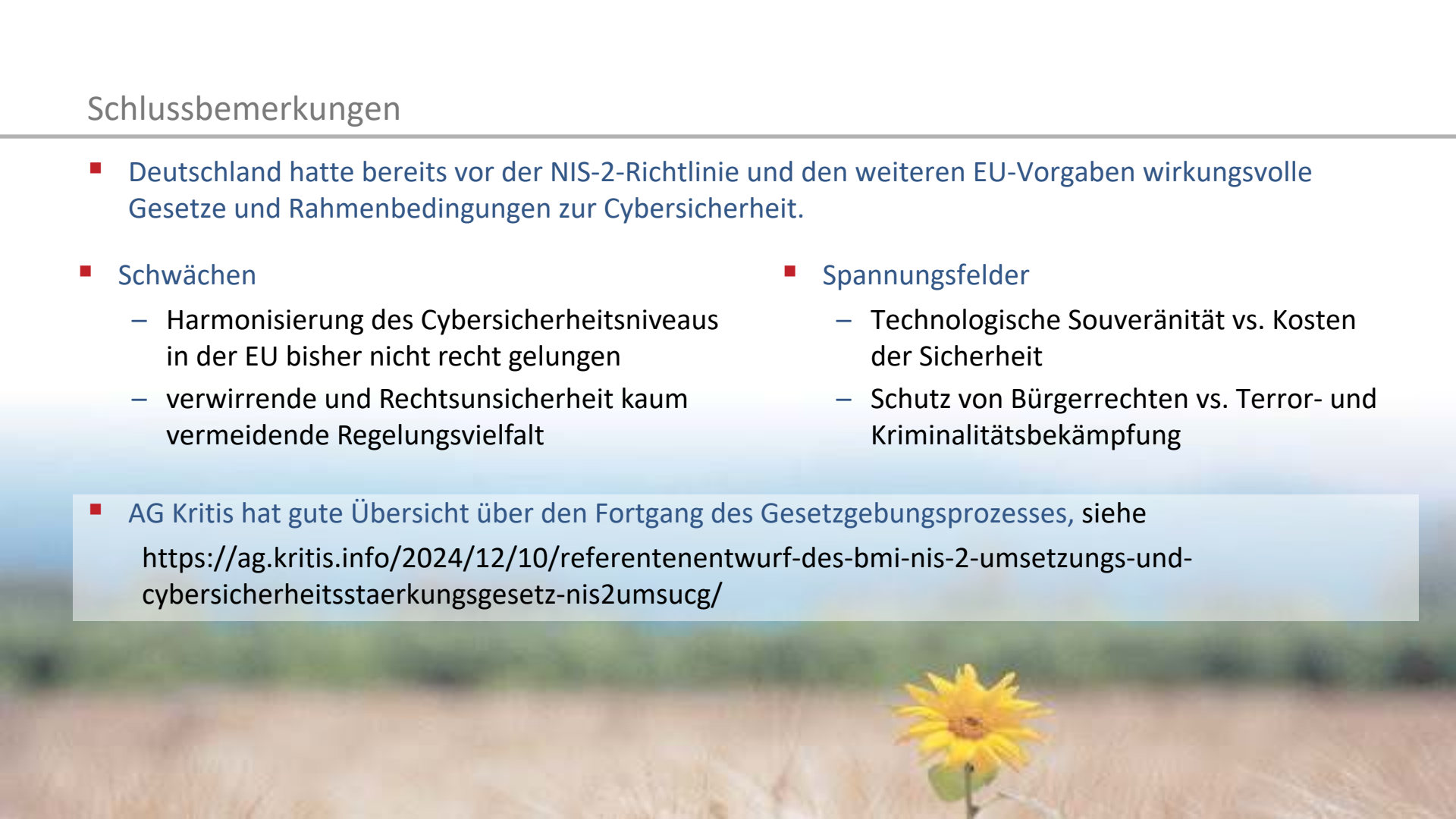
Schlussbemerkungen

- Deutschland hatte bereits vor der NIS-2-Richtlinie und den weiteren EU-Vorgaben wirkungsvolle Gesetze und Rahmenbedingungen zur Cybersicherheit.

- Schwächen
  - Harmonisierung des Cybersicherheitsniveaus in der EU bisher nicht recht gelungen
  - verwirrende und Rechtsunsicherheit kaum vermeidende Regelungsvielfalt

- Spannungsfelder
  - Technologische Souveränität vs. Kosten der Sicherheit
  - Schutz von Bürgerrechten vs. Terror- und Kriminalitätsbekämpfung

- AG Kritis hat gute Übersicht über den Fortgang des Gesetzgebungsprozesses, siehe
  https://ag.kritis.info/2024/12/10/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/



inf.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DEPARTMENT OF INFORMATICS
SECURITY AND PRIVACY

HOME COURSES THESES RESEARCH PEOPLE SERVICE

UHH → MIN-Fakultät → Fachbereich Informatik → Einrichtungen → Arbeitsbereiche → Security and Privacy → Home

WORKING GROUP ON «SECURITY AND PRIVACY»

Security and Privacy

Information systems become more and more important in critical infrastructures, while the Internet has evolved to a critical infrastructure itself. The secure operation of these infrastructures is vital and their failure can have severe impacts up to the loss of human lives.
Security refers to the fact that protection goals are achieved in the presence of malicious attacks and system failures. Typical security goals can be confidentiality, integrity, accountability, and availability. Security and privacy in information systems addresses both technical and organizational aspects, such as building and establishing security concepts and security infrastructures as well as risk analysis and risk management.
Privacy can be a conflicting goal to security, but they can also benefit from each other. Hence, it is necessary to balance both when developing secure information systems.

Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

Telefon +49 40 42883 2358

hannes.federrath@uni-hamburg.de

https://svs.informatik.uni-hamburg.de