Fraunhofer IESE

Fraunhofer-Institut für Experimentelles Software Engineering IESE

NIS-2 Webinar

Grundlagen der neuen Cybersecurity Richtlinie der EU und erste Schritte zur Compliance

NIS-2 (EU) 2022/2555

Patrick Dzubba, Michael Ochs

Die NIS-2 Richtlinie

Webinarübersicht

1. **Einführung**
2. **Betroffenheit**
3. **Maßnahmen und Pflichten**
4. **Erste Schritte zur Umsetzung**
5. **Austausch mit Experten**

Kapitel 01

Einführung: Warum NIS-2?

Cybercrime nimmt weiter zu

Motivation

Im Gegensatz zur Inlands-PKS sind die erfassten Cybercrime-Delikte bei Auslandstaten im Jahr 2023 um ca. 28% angestiegen. Dabei handelt es sich um Sachverhalte, bei denen zwar Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters im Ausland liegt oder unbekannt ist.[2] Seit Beginn der separaten Erfassung dieser Auslandstaten zeigt sich hier ein fortlaufender Anstieg.

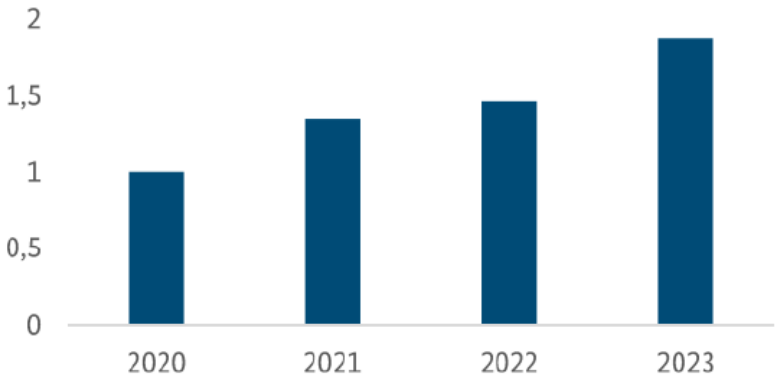


Abbildung 4: Erfasste Auslandstaten Cybercrime. (Anm.: Der Indexwert zeigt die Veränderung der erfassten Auslandstaten, dabei wird das Jahr 2020 als Basiswert auf 1 festgelegt. Die Werte der Folgejahre stehen in Relation zu diesem Basiswert und zeigen damit den Trend der steigenden Auslandstaten.)

Über 800 Unternehmen und Institutionen haben Ransomware-Angriffe zur Anzeige gebracht.

Die weltweiten Ransomware-Zahlungen steigen auf über 1 Mrd. US-Dollar.

Die vom Bitkom e.V. bezifferten Schäden in Deutschland belaufen sich auf 205,9 Mrd. Euro - 72% davon entstanden direkt durch Cyberangriffe.

Quelle: Bundeslagebild Cybercrime 2023, Bundeskriminalamt

Die Folgen sind katastrophal!

Cybercrime Vorfälle in Deutschland

Ransomware-Angriff auf Südwestfalen-IT GmbH

- Angriff auf den Kommunalen IT-Dienstleister im Oktober 2023
- Ursache: fehlende Sicherheitsmaßnahmen und Updateprozesse
- Erhebliche Auswirkungen auf Kommunen (72), Bürger (1.7Mio) und Webservices (160)
- Notfallzustand und eingeschränkte Dienste für 11 Monate bis September 2024
- Gesamtaufwand zur Behebung: über 43.000 Arbeitsstunden durch über 170 Personen, über 2.8M-EUR Zusatzkosten bis 09/2024

»In der NIS-2-Richtlinie verpasst der Gesetzgeber nach aktuellem Stand die Gelegenheit, eine verbindliche Gesetzesgrundlage für kommunale IT-Dienstleister zu schaffen. Die Regeln müssen klarer gefasst werden, und wir würden es begrüßen, dass auch kommunale IT-Dienstleister Gegenstand der NIS-2 werden.«

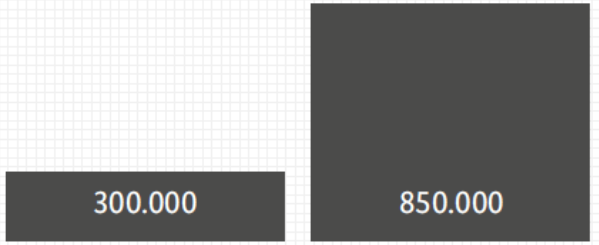
- Mirco Pinske, Geschäftsführer der SIT

Quellen:
https://kommunaler-notbetrieb.de/2023/10/30/zweckverband-suedwestfalen-it/
https://www.sit.nrw/detailansicht/ein-jahr-nach-dem-hackerangriff-suedwestfalen-it-zieht-bilanz

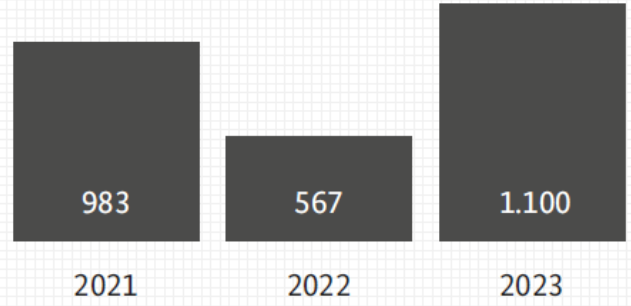
Schadwirkung/Impact

Ransomware

Lösegeld pro Fall (in US-Dollar, ca. Durchschnitt):



Von Ransomware-Gruppen erbeutete Lösegelder weltweit (in US-Dollar, Mio.):



KRITIS

Störungen bei KRITIS-Betreibern 490

Beispiele

Ransomware-Angriff auf kommunalen IT-Dienstleister im Oktober 2023

Betroffene Kommunen:	72
Betroffene Arbeitsplätze:	rund 20.000
Betroff. Einwohnerinnen und Einwohner:	rund 1,7 Mio.

Geschätzter Schaden durch Systemausfälle eines **fehlerhaftes Update** in der Software Crowdstrike Falcon:
> 8,5 Mio. Geräte > 5 Milliarden Dollar

VerbraucherInnen

Top-3-Schäden für Verbraucherinnen und Verbraucher bei IT-Sicherheitsvorfällen und Cybercrime (%)

Vertrauensverlust in den Onlinedienst	30
Finanzieller Schaden	26
Zeitlicher Schaden	24

- Exfiltrierte Daten wesentlich mehr wert als verschlüsselte → Fähigkeit zur Prävention muss gestärkt werden
- Schäden im Milliardenbereich, unvorhergesehene Ereignisse, menschliches Versagen → Fähigkeit zur Vorfallsbewältigung muss gestärkt werden

Quelle: BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024-Doppelseite.html?nn=129410

Die Gesetzeslage in Deutschland

Historie

2009 BSI-Gesetz
- BSI als zentrale Melde- und Zertifizierungsstelle für Cybersicherheit

2015 IT-Sicherheitsgesetz
- Änderung des BSI-Gesetzes
- Erweitert Aufgaben und Rechte des BSI
- Betreiber kritischer Infrastrukturen müssen Cybersicherheit dem BSI nachweisen und Sicherheitsvorfälle melden

2016 BSI-Kritis-Verordnung
- Definiert betroffene Sektoren und legt Schwellenwerte für betroffene Unternehmen fest

2016 EU-Richtlinie 2016/1148 aka NIS-1
- Anforderungen an die Cybersicherheit kritischer Infrastrukturen auf EU-Ebene
- Nach Vorbild des IT-SiG

2021 IT-Sicherheitsgesetz 2.0
- Erneute Erweiterung der Zuständigkeiten und Rechte des BSI
- Siedlungsabfallentsorgung als neuer KRITIS-Sektor
- Erweiterung der Überwachung auf Unternehmen im besonderen öffentlichen Interesse

2022 EU-Richtlinie 2022/2555 aka NIS-2
- Ablösung der NIS-1
- Reaktion auf sich ständig verändernde Bedrohungslage und zunehmende Systemvernetzung
- Vereinheitlichung der Maßnahmen auf EU-Ebene

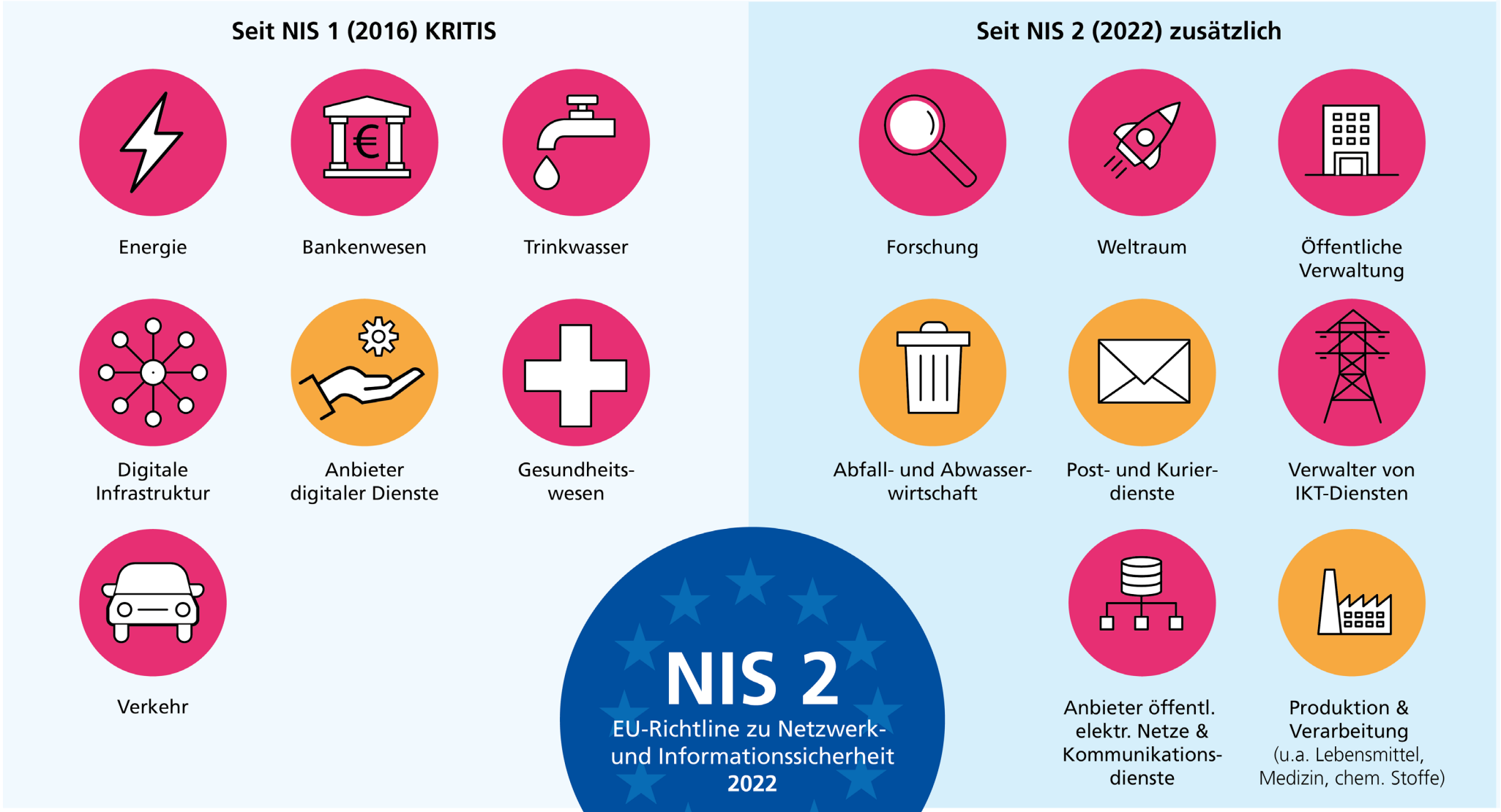
~~17.10.2024~~
März 2025?
NIS2UmsuCG
- Nationale Umsetzung der NIS-2 in Deutschland

Kapitel 02

Betroffenheit: Sektoren und Kriterien

Sektoren der NIS-2

Hoch-kritische und kritische Sektoren



Rückblick: Entwicklung der Sektoren

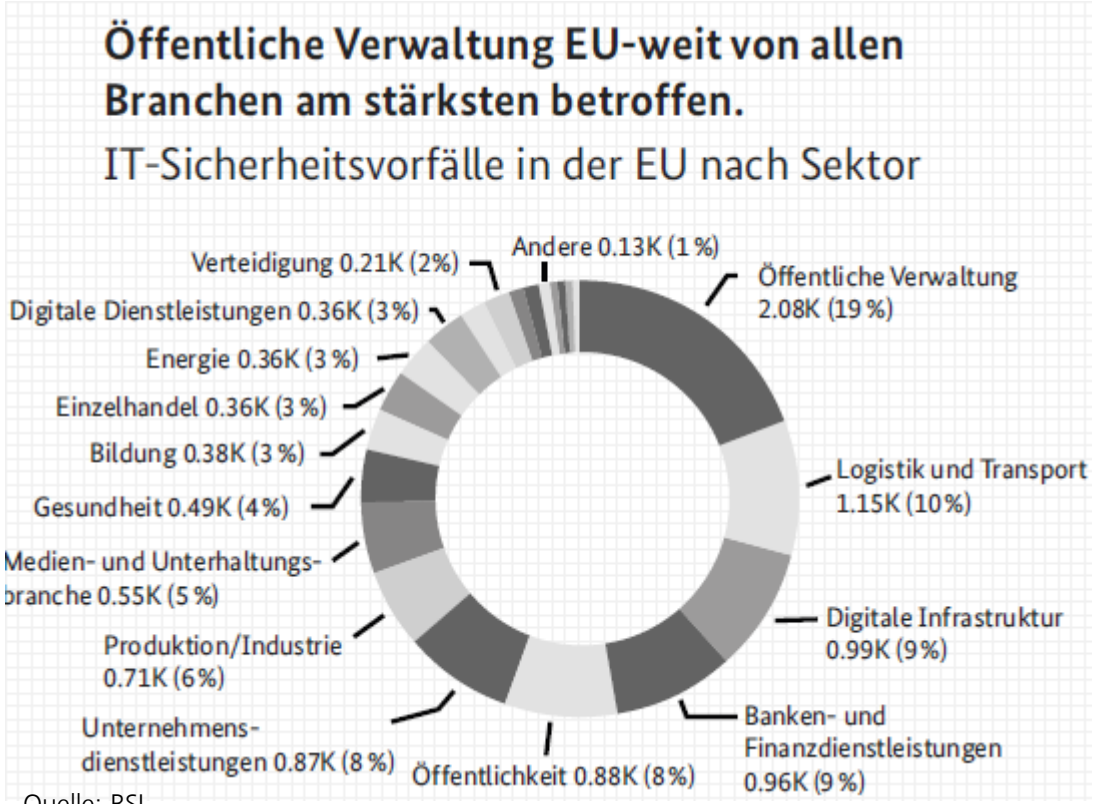
KRITIS nach nat. KRITIS-Strategie	KRITIS gemäß §2 (10) BSIG	NIS-2-Richtlinie	CER-Richtlinie
Energie	Energie	Energie	Energie
Transport und Verkehr	Transport und Verkehr	Verkehr	Verkehr
Finanz- und Versicherungswesen	Finanz- und Versicherungswesen	Bankwesen und Finanzmarktinfrastrukturen	Bankwesen und Finanzmarktinfrastrukturen
Gesundheit	Gesundheit	Gesundheit	Gesundheit
Wasser	Wasser	Wasser	Wasser
Informationstechnik und Telekommunikation	Informationstechnik und Telekommunikation	Digitale Infrastruktur, Verwaltung von IKT-Diensten	Digitale Infrastruktur
Ernährung	Ernährung	–	Ernährung
Siedlungsabfallentsorgung	Siedlungsabfallentsorgung	–	–
Medien und Kultur	–	–	–
–	–	Weltraum	Weltraum
Staat und Verwaltung	–	Öffentliche Verwaltung	Öffentliche Verwaltung

Tabelle 2: KRITIS-Sektoren nach der nationalen KRITIS-Strategie, dem BSI-Gesetz und den aktuellen EU-Richtlinien
Quelle: BSI

Bankwesen: gemäß EG28 NIS-2 unter DORA-VO

CER-RL (EU) 2022/2557: Resilience of Critical Entities

DORA-VO (EU) 2022/2554: Digital Operational Resilience Act Regulation

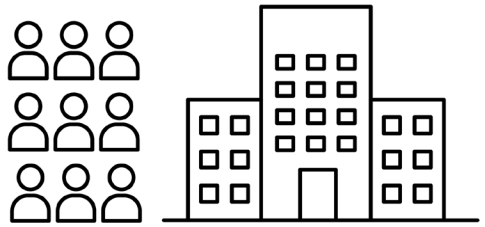


Quelle: BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024-Doppelseite.html?nn=129410

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410

Sektoren der NIS-2

Hoch-kritische und kritische Sektoren



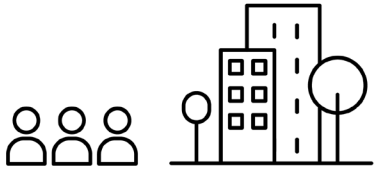
Große Unternehmen
(≥250 MAB, >50 MEUR Umsatz)

Wesentliche Einrichtung

- Zugehörig zu **Sektor hoher Kritikalität**
- Erfüllung der 10 Risikomaßnahmen
- **Regelmäßige Sicherheitsprüfungen**
- Erstmeldung von Cybersicherheits-vorfällen innerhalb 24h, Update nach 3 Tagen und 30 Tagen
- **Unternehmensleitung haftet** für Verstöße

Wichtige Einrichtung

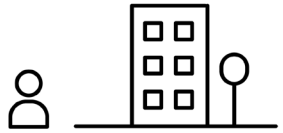
- Zugehörig zu **kritischem Sektor**
- Erfüllung der 10 Risikomaßnahmen
- Behördliche Überprüfung **bei Verdacht**
- Erstmeldung von Cybersicherheits-vorfällen innerhalb 24h, Update nach 3 Tagen und 30 Tagen
- **Unternehmensleitung haftet** für Verstöße



Mittlere Unternehmen
(<250 MAB, ≤50 MEUR Umsatz)

Wichtige Einrichtung

- Zugehörig zu **NIS2-relevantem Sektor**
- Erfüllung der 10 Risikomaßnahmen
- Behördliche Überprüfung **bei Verdacht**
- Erstmeldung von Cybersicherheits-vorfällen innerhalb 24h, Update nach 3 Tagen und 30 Tagen
- **Unternehmensleitung haftet** für Verstöße



Kleine Unternehmen
(≤50 MAB, ≤10 MEUR Umsatz)

Nicht betroffen

Sonstige Sektoren

- Gegebenenfalls werden durch von NIS 2 betroffene Unternehmen Sicherheitsmaßnahmen in der Lieferkette gefordert (Maßnahme d aus Artikel 21)

Betroffenheit: Besonderheiten

Die NIS-2 kann auch relevant für Unternehmen werden, die nicht die Kriterien zu Größe, Umsatz und Sektor erfüllen. Hier kann der Aspekt „Sicherheit in der Lieferkette“ in der NIS-2 zum Tragen kommen.

- Beispiel: Ein Softwarehersteller, der sein Produkt in Lizenz verkauft oder als Teil eines Produkts seiner Abnehmer einbringt
  - Dieser Hersteller muss ebenfalls – in Abstimmung mit seinem/seinen Kunden – Maßnahmen aus der NIS-2 umsetzen
  - Bekanntes Beispiel: Solarwinds-Hack (2020) – über ein kompromittiertes Update der Plattform Orion des US-Software-Herstellers SolarWinds konnte bei bis zu 18.000 Unternehmen eine Hintertür in deren IT-Sicherheitssystem geschaffen und genutzt werden.
  - Näheres z.B. unter https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187

Sonderfall: Einzelanbieter einer kritischen Infrastruktur-Dienstleistung, der nicht ersetzbar ist, z.B. im Sektor Energie

- Beispiel: Ein regionaler Fernwärmeanbieter, mit weniger als 10 MEUR Umsatz und weniger als 50 MAB
  - Dieser Anbieter muss ebenfalls die NIS-2 Anforderungen aufgrund seiner Alleinstellung in der versorgten Region erfüllen

Betroffenheit: Besonderheiten

Sonderfall Banken (und Versicherungen)

- Für Banken und Versicherungen gilt im Bereich IKT-Risiken/Cybersicherheit die NIS-2 nicht umfassend. Stattdessen gilt die EU-Verordnung „Digital Operational Resilience Act“ (DORA, (EU) 2022/2554) ab 17.01.2025 (DORA als lex specialis zur NIS-2)
- Da Bankwesen auch in der NIS-2 als Sektor von hoher Kritikalität ausgewiesen wird besteht eine
  - Registrierungspflicht für Banken und (über BSI-KRITIS-VO) für Finanzwesen allgemein beim BSI
  - Pflicht zur Umsetzung von Cybersicherheitsrisikomaßnahmen (z.B. in DORA Kapitel II – IKT Risikomanagement zu finden)
  - Pflicht zur Meldung von erheblichen Sicherheitsvorfällen
- Das Finanzwesen muss durch DORA in Summe erheblich mehr Anforderungen erfüllen, als die NIS-2 fordert

Möglichkeit der kostenlosen Betroffenheitsprüfung beim BSI

- Das BSI bietet auf seiner Webseite eine kostenlose NIS-2-Betroffenheitsprüfung an, die bereits das noch nicht verabschiedete NIS2UmsuCG implementiert

- Online-Prüfung des BSI
- NIS-2-Entscheidungsbaum (nach NIS2UmsuCG)

Kapitel 03

Maßnahmen und Pflichten

NIS-2 Sicherheitsansatz und grundlegende Ziele

Ein Blick auf Artikel 21 der NIS-2

NIS-2 Art. 21 definiert *zehn* Maßnahmen für Netzwerk- und Informationssicherheit

Fokus I

Risikomanagement

- **Bewusstsein** für eigene **Angriffsfläche**
- Systematische **Analyse** der **Bedrohungen** und **Folgen**
- **Verhältnismäßige** und angebrachte **Maßnahmen**

Fokus II

Resilienz

- **Bewusstsein** für die **Unerreichbarkeit** von **Sicherheit**
- **Abhängigkeiten** zwischen Systemen, **systemübergreifende Folgen**
- **Kontinuierliche** Anpassung und **Verbesserung**

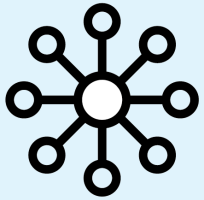
NIS-2 Maßnahmen im Überblick

Maßnahmen aus NIS 2 Artikel 21 für Risikomanagement und Resilienz

Vorbereitung auf Cybersicherheitsvorfälle

- **Risikoanalyse** und Sicherheit von Informationssystemen
- **Bewältigung** von Sicherheitsvorfällen
- **Aufrechterhaltung** des Betriebs

Geschäftsbeziehungen



- Sicherheit der **Lieferkette** (unmittelbare Anbieter und Dienstanbieter)
- Sicherheitsmaßnahmen bei **Erwerb und Wartung** von Netz- und Informationssystemen, einschließlich Management und Offenlegung von **Schwachstellen**

Kontrolle und Awareness

- Konzepte und Verfahren zur **Bewertung der Wirksamkeit** der Risikomanagementmaßnahmen
- Grundlegende Verfahren im Bereich **Cyberhygiene, Schulungen** im Bereich der Cybersicherheit

Technische Umsetzung

- Konzepte und Verfahren für den Einsatz von **Kryptografie** und Verschlüsselung
- Sicherheit des Personals, Konzepte für **Zugriffskontrolle** und Management von Anlagen
- Verwendung von **Multi-Faktoren-Authentifizierung** oder kontinuierlicher Authentifizierung, **gesicherte Kommunikation** und ggfs. gesicherte interne Notfallkommunikation

Vorbereitung auf den Ernstfall

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

- Nachweisen können, dass Risiken analysiert und bewertet wurden
- Systematisches Vorgehen und Bewusstsein für die eigene Lage

b) Bewältigung von Sicherheitsvorfällen

- Vorfälle lassen sich nie vollständig verhindern
- Im Ernstfall muss klar sein, was zu tun ist

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall und Krisenmanagement

- Anforderungsanalyse und Identifikation der Kernprozesse
- Vollständige Ausfälle und Verluste vermeiden

Sicherheit in Geschäftsbeziehungen

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern

- Moderne Angriffe beginnen in der Lieferkette (z.B. SolarWinds)
- Ausbreitung der Anforderungen auf weitere Unternehmen

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen

- Betrifft sowohl Hersteller als auch Nutzer → Doppelte Absicherung
- Offener Austausch und Transparenz

Kontrolle und Awareness

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

- Kontinuierliche Verbesserung und Lernen aus Vorfällen
- Gelebte Prozesse statt Dokumentation als Alibi

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit

- Sicherheitsfaktor Mensch und Sicherheitskultur im Unternehmen
- Korrekter Umgang mit technischen Maßnahmen

Technische Umsetzung

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung

- Datenschutz
- Informationssicherheit
- Schutz der Vertraulichkeit und Integrität

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

- Schutz vor Schadsoftware
- Verwaltung der IT-Infrastruktur
- Moderne Sicherheitsarchitekturen (Tiering-Modelle)

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

- Moderne, sichere Authentifizierung
- Moderne Sicherheitsarchitekturen (Zero-Trust)

Vieles in der NIS-2 ist bereits bekannt

Mapping Anforderungen NIS2UmsuCG und NIS-2 auf BSI-KRITIS-Maßnahmen und ISO 27001 2022

Auszug!

NIS2UmsuCG	Anforderung		KRITIS	ISO 27001 2022	NIS2 Artikel
§30 (1) Satz 1	Maßnahmen basierend auf Risiko-Exposition und gesellschaftlichen und wirtschaftlichen Auswirkungen		BSI-3, 15	4.3, 6.1, 8.2, 8.3, A.5.4, A.5.29, A.5.30	21 (1)
§30 (1) Satz 3	Dokumentation der (NIS2) Risiko-Management Maßnahmen		BSI-16	6.1.3, 8.3, A.5.31	32 (2) e, g
§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	Vorbereitung auf Cybersicherheitsvorfälle	BSI-13, 14, 16, 85, 86, 87, 88, 89	6.1, 8.2, 8.3, 10.1, A.5.31, A.5.36, A.8.34	21 (2) a
§30 (2) Nr. 2	Bewältigung von Sicherheitsvorfällen	Vorbereitung auf Cybersicherheitsvorfälle	BSI-77, 78, 79, 80, 90, 92, 93, SzA	A.5.2, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.5.30, A.6.8, A.8.9, A.8.15, A.8.16	21 (2) b
§30 (2) Nr. 3	Aufrechterhaltung Betrieb (BCM)	Vorbereitung auf Cybersicherheitsvorfälle	BSI-15, 17, 18	A.5.29, A.5.30, A.5.31, A.8.14	21 (2) c
§30 (2) Nr. 4	Sicherheit der Lieferkette	Geschäfts-beziehungen	/	A.5.19, A.5.20, A.5.21 A.5.22, A.5.23	21 (2) d

Quelle: https://www.openkritis.de/massnahmen/nis2-mapping-standards-implementing.html (letzte Spalte angepasst auf NIS2)

Berichts- und Meldepflichten

Zeithorizonte für Meldungen von Cybersicherheitsvorfällen

- **Verpflichtung wesentlicher und wichtiger Einrichtungen** ihrem CSIRT bzw. der zuständigen Behörde **unverzüglich über jeden erheblichen Sicherheitsvorfall zu unterrichten**
- Zuständige Behörden leiten umgehend an das CSIRT weiter
- Im Falle von rechtswidrigem oder böswilligem Handeln muss Strafanzeige erstattet werden
- Grenzüberschreitende Vorfälle sind als solche in der Frühwarnung zu kennzeichnen

- Ein **Sicherheitsvorfall** gilt als **erheblich**, wenn
  - er **schwerwiegende Betriebsstörungen der Dienste** oder **finanzielle Verluste** für die betreffende Einrichtung verursacht hat oder verursachen kann
  - er **andere natürliche oder juristische** Personen durch **erhebliche materielle oder immaterielle Schäden** beeinträchtigt hat oder beeinträchtigen kann

Berichtsschema und Zeitschiene

- **Frühwarnung:** Erstmeldung über einen erheblichen Sicherheitsvorfall innerhalb von **24 Stunden** nach Bekanntwerden — **24h**
- **Aktualisierung:** Innerhalb von **72 Stunden (3 Tage)** nach Bekanntwerden mit Aktualisierung der Informationen aus der Frühwarnung und erste Bewertung, einschließlich Schweregrad, Auswirkungen und ggfs. Kompromittierungsindikatoren (digitale Spuren der Angreifer) zum erheblichen Sicherheitsvorfall — **72h**
- **Zwischenbericht:** Auf Ersuchen eines CSIRT oder zuständigen Behörde hinsichtlich relevanter Statusaktualisierungen
- **Abschlussbericht:** Spätestens 30 Tage nach Bekanntwerden des erheblichen Sicherheitsvorfalls — **30d**
  - Ausführliche Beschreibung, inkl. Schweregrad und Auswirkungen
  - Angaben zur Art der Bedrohung (Ursache)
  - Angaben zu getroffenen und laufenden Abhilfemaßnahmen
  - Gegebenenfalls grenzüberschreitende Auswirkungen

NIS2-bezogene Geldbußen

Fälligkeit von Geldbußen

- Verstoß gegen die Umsetzung und Durchführung der 10 Risikomaßnahmen aus Artikel 21 NIS-2
- Verstoß gegen die Berichtspflichten (unterlassene Meldungen von erheblichen Sicherheitsvorfällen) aus Artikel 23 NIS-2
- Besonders schwere Vorfälle
  - Nichtbehebung von Mängeln, z.B. nach verbindlicher Anweisung der zuständigen Behörde
  - Behinderung von Prüfungen oder Überwachungstätigkeiten
  - Übermittlung von falschen oder grob verfälschten Informationen in Bezug auf Risikomanagementmaßnahmen im Bereich Cybersicherheit oder Berichtspflichten
  - Wiederholte Verstöße gegen Auflagen oder Regeln

Höhe von Geldbußen für wichtige Einrichtungen

- Höchstbetrag min. 7 MEUR bis 1.4% weltweiter Jahresumsatz
  - Verstoß gegen Artikel 21 (Risikomaßnahmen)
  - Verstoß gegen Artikel 23 (Berichtspflichten)

Höhe von Geldbußen für wesentliche Einrichtungen

- Höchstbetrag min. 10 MEUR bis 2% weltweiter Jahresumsatz
  - Verstoß gegen Artikel 21 (Risikomaßnahmen)
  - Verstoß gegen Artikel 23 (Berichtspflichten)

NIS-2-Verstöße mit Verletzungen des Schutzes personenbezogener Daten (DSGVO)

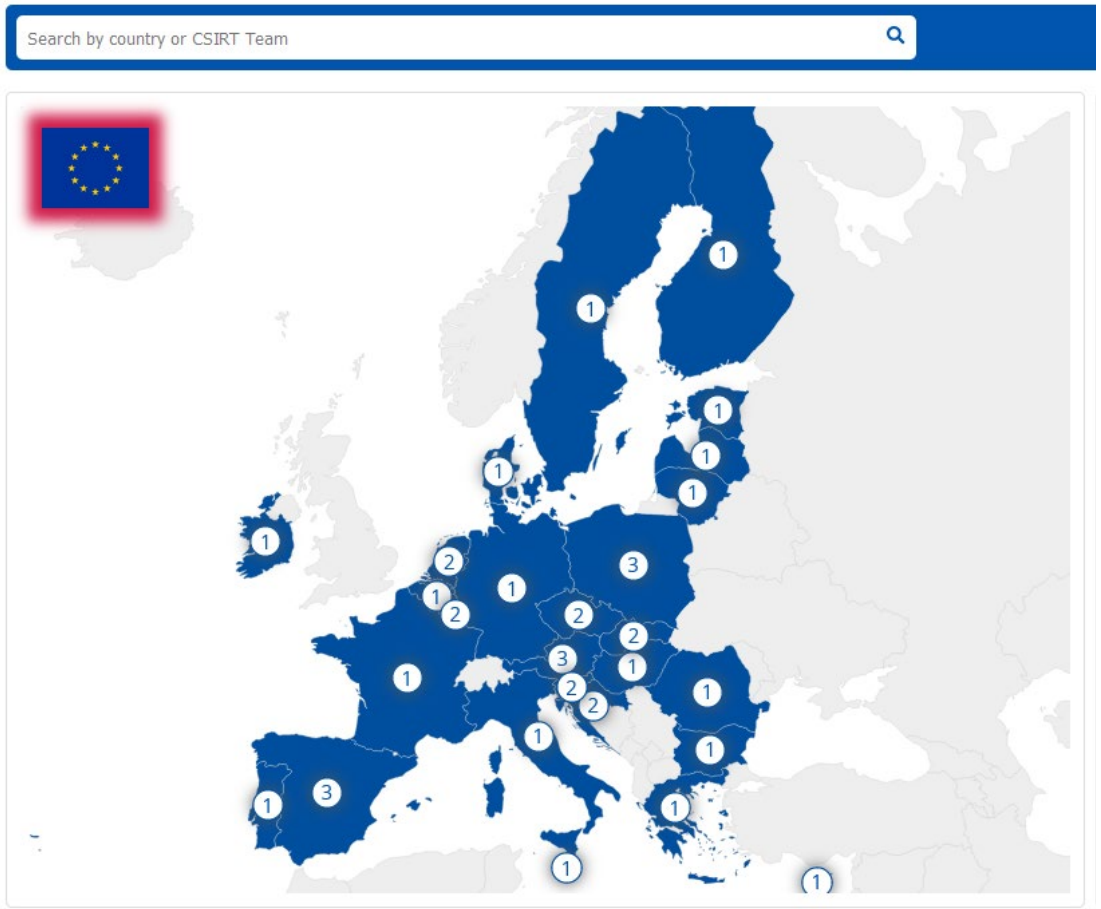
- Bußgelder werden nach DSGVO (EU) 2016/679 verhängt
- Höchstbetrag min. 10 MEUR bis 2% weltweiter Jahresumsatz (normaler Verstoß)
- Höchstbetrag min. 20 MEUR bis 4% weltweiter Jahresumsatz (Grundsatzverstoß)

Umsetzung: NIS-2 Gesamtrahmen national und EU

CSIRTs und Austausch über Cybersicherheitsvorfälle – ein echter Mehrwert

Computer Security Incident Response Teams (CSIRTs)

- Jeder EU-Mitgliedsstaat benennt und richtet ein oder mehrere CSIRTs ein (ein CSIRT ist Koordinator)
- Kooperation der CSIRTs mit wesentlichen und wichtigen Einrichtungen und Austausch von Informationen mit dem Ziel
  - Verhindern, Aufdecken von und Reaktion auf Sicherheitsvorfälle
  - Mitigation und Eindämmung der Folgen von Sicherheitsvorfällen
  - Steigerung Cybersicherheitsniveau durch Informationsaustausch
  - Aufklärungsarbeit über Cyberbedrohungen
  - Offenlegung und Beseitigung von Schwachstellen
  - Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen
- CSIRTs arbeiten EU-weit unter Koordination der ENISA zusammen



Kapitel 04

Erste Schritte zur Umsetzung

Erste Schritte zur Umsetzung

Roadmap für Unternehmen

1

Betroffenheit und Registrierungspflicht prüfen

- Sonderfälle beachten (DORA, Ausnahmeregelungen)
- indirekte Betroffenheit durch Geschäftsbeziehungen beachten
- Registrierungspflicht prüfen und rechtzeitig durchführen

2

Bestandsaufnahme und Gap-Analyse

- Geschäftsprozesse, Abhängigkeiten und Geschäftsbeziehungen analysieren
- Bereits umgesetzte Maßnahmen mit den Anforderungen der NIS-2 vergleichen
- Bestehende oder mögliche zusätzliche Zertifizierungen beachten

3

Priorisierung und Planung der Umsetzung

- Risiko- und Bedrohungsanalyse durchführen
- Quick-Wins und Abhängigkeiten identifizieren
- Priorisierte Maßnahmen definieren, z.B. auch Möglichkeiten zur Abgabe von Verantwortung (Dienstleister, Cloud) bewerten

4

Umsetzung der Maßnahmen

- Maßnahmen durchführen
- Prozesse dokumentieren
- Nachweise sichern
- Synergien nutzen

5

Kontinuierliche Überprüfung und Verbesserung

- Technische Maßnahmen auf aktuellem Stand halten
- Regelmäßige Kontrolle der Effektivität der Maßnahmen, z.B. durch interne oder externe Audits, Penetrationstests, BCM Übung
- Kontinuierliche Verbesserung der Prozesse (organisatorischer Teil)

Kapitel 05

Austausch mit Experten

Es gibt verschiedene europäische Rechtsvorschriften, die für die Cybersicherheit von Bedeutung sind. Diese effizient umzusetzen und eine Fragmentierung zu vermeiden, ist eine zentrale Herausforderung, der wir uns gemeinsam stellen. Die internationale Zusammenarbeit ist für das BSI ein essentieller Erfolgsfaktor zur Verbesserung der Cybersicherheit in Deutschland und Europa. Cybersicherheit muss ganz oben auf der Agenda aller Verantwortlichen in Staat, Regierung und Privatwirtschaft stehen. Daran arbeiten wir europaweit im engen Schulterschluss.«

Claudia Plattner,
BSI-Präsidentin

Fraunhofer IESE

Fraunhofer-Institut für Experimentelles Software Engineering IESE

Vielen Dank für Eure Aufmerksamkeit!

Kontakt

Patrick Dzubba
Michael Ochs

patrick.dzubba@iese.fraunhofer.de
michael.ochs@iese.fraunhofer.de

Fraunhofer IESE
Fraunhofer-Platz 1
67663 Kaiserslautern
https://www.iese.fraunhofer.de

Fraunhofer IESE

Fraunhofer-Institut für Experimentelles Software Engineering IESE