NIS-2: Viel Wirbel um nichts?

Webinar

BDO Cyber Security GmbH

25.09.2024

Begrüßung und Einführung

Wir geben Ihnen einen umfassenden Blick auf die neue NIS-2 Regulierung

Zielsetzung für heute

Verständnis

Grundlegenden Inhalte, Ziele und Neuerungen verstehen

Relevanz

Betroffenheit der Unternehmen und Branchen erkennen

Anforderungen

Sicherheitsanforderungen und Meldepflichten kennenlernen

Umsetzung

Best Practices für die praktische Umsetzung in Unternehmen

Agenda

1. NIS-2: Viel Wirbel um nichts ?
2. NIS-2 im Überblick
3. Hintergrund und Kontext der NIS-2-Richtlinie
4. Betroffene Sektoren durch NIS-2
5. NIS-2 und KRITIS-DachG: Cybersicherheit auf nationaler Ebene
6. Pflichten von Betreibern und Einrichtungen
7. NIS-2 im Detail: Maßnahmen
8. NIS-2 vs. ISO 27001
9. NIS-2 im Gesundheitswesen
10. Umsetzung der NIS-2-Richtlinie
11. Interaktives Beispiel: Cyber Risikomanagement
12. Zusammenfassung und Fragerunde

Moderatoren

Regine Knipper
Partnerin
Regine.Knipper@bdosecurity.de

Liane Kiesewalter
Senior Consultant
Liane.Kiesewalter@bdosecurity.de

Stefan Zimmermann
Senior Consultant
Stefan.Zimmermann@bdosecurity.de

NIS-2: Viel Wirbel um nichts?

Die aktuelle Bedrohungslage (1/3)

Der wachsenden Bedrohung durch Cyberattacken sehen sowohl öffentliche als auch privatwirtschaftliche Unternehmen täglich gegenüber.
Damit steigt die Relevanz für effiziente Notfallbewältigung. Die EU reagiert mit der EU NIS-2-Richtlinie und macht Resilienzmaßnahmen verpflichtend.

250.000

Neue Schadprogramm-Varianten wurden durchschnittlich pro Tag im Berichtszeitraum gefunden

Durc als

Bedrohung so hoch wie nie zuvor!

66%

Aller Spam-Mail im Berichtszeitraum waren Cyberangriffe

370

Wur
jedem Tag des
Berichtszeitrau wegen
Schadprogramm en gesperrt.

000

Infizierte Systeme täglich im Berichtszeitraum vom BSI erkannt und weiter gemeldet.

84%

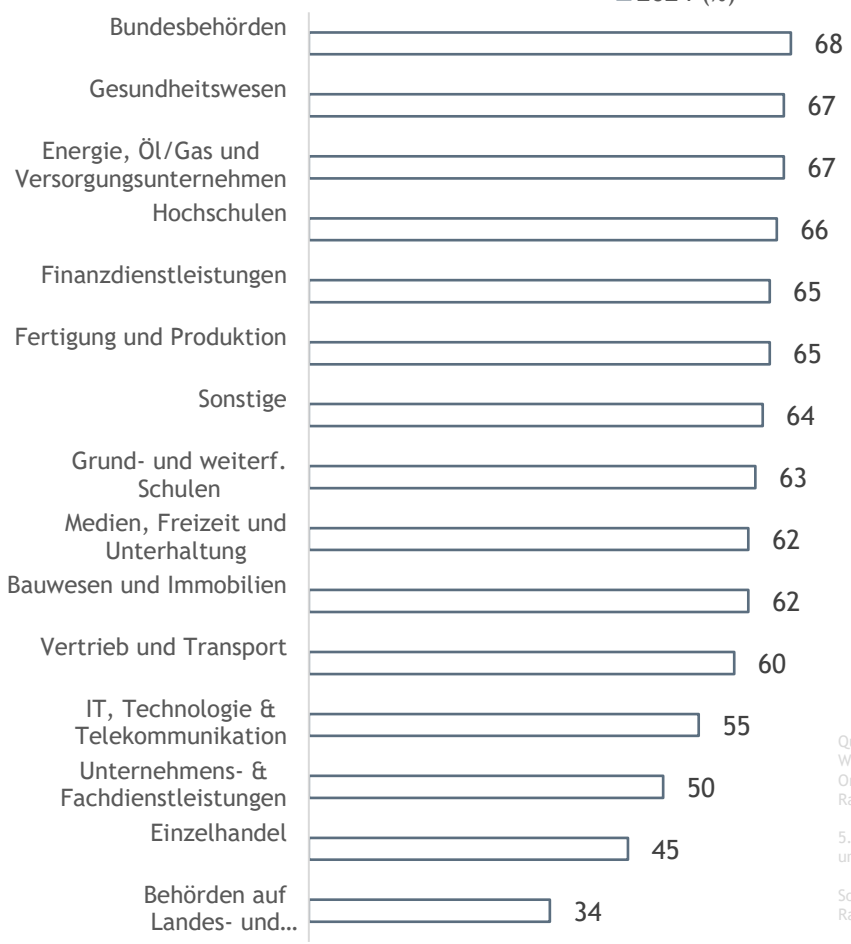
der Betrugsfälle per E-Mail wurden als Finanz-Phishing-Mails getarnt und angeblich von offiziellen Bankinstituten versendet.

Quelle: Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Berichtszeitraum: Juni 2022-Juni 2023.

NIS-2: Viel Wirbel um nichts?

Die aktuelle Bedrohungslage (2/3)

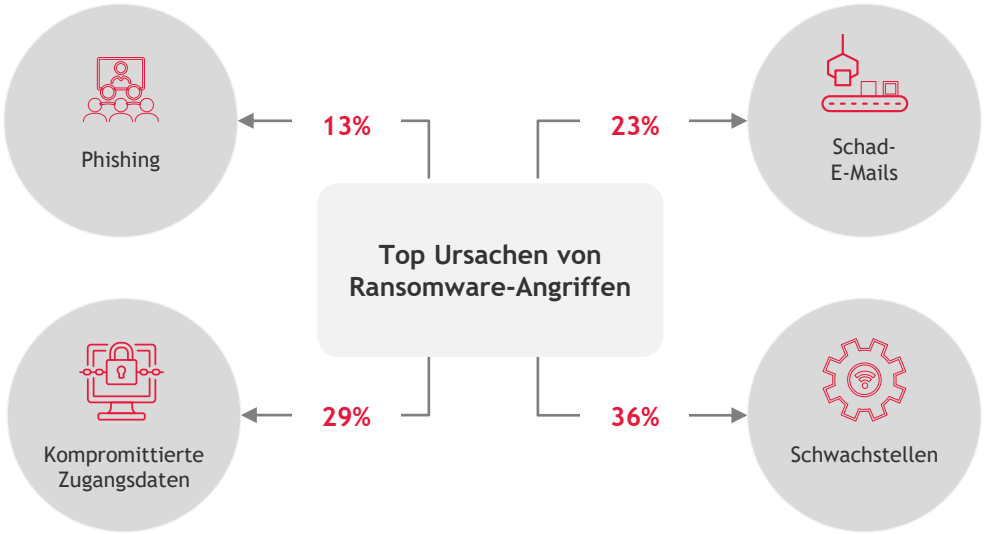
Häufigkeit von Ransomware-Vorfällen nach Branche



Quelle:
War Ihr Unternehmen/Ihre Organisation im letzten Jahr von Ransomware betroffen?

5.000 IT-Entscheider aus 14 Ländern und 15 Branchen

Sophos
Ransomware-Report 2024



Auswirkungen der Angriffe

- **Finanzielle Verluste:**
Durchschnittlicher Schaden pro Cyberangriff auf europäische Unternehmen liegt bei mehreren Millionen Euro

- **Reputationsschäden:**
Schädigung des Unternehmensimages durch Datenlecks oder Betriebsunterbrechungen

- **Betriebsunterbrechungen & Erhöhung der Mortalitätsrate:**
Längerer Stillstand von kritischen Systemen kann gravierende Folgen für die Bevölkerung haben, z.B. im Gesundheitswesen oder der Energieversorgung. Die Wahrscheinlichkeit als Patient in einem Krankenhaus zu sterben, erhöht sich um 20 bis 35 Prozent, wenn das Krankenhaus von einem Ransomware-Angriff betroffen ist.[1)]

1) Quelle: Heise. Ransomware-Angriffe auf Krankenhäuser gefährden Menschenleben (28.01.2024)

NIS-2: Viel Wirbel um nichts?

Die aktuelle Bedrohungslage (3/3)

- Die Universitätsklinik Düsseldorf ist Opfer eines Hackerattacke geworden Die Folge: Operationen waren nicht mehr möglich, die Notaufnahme musste schließen
- Unbekannte Täter hatten etwa 30 Server des Klinikums verschlüsselt hatten
- Dies hat dazu geführt, dass Notfallpatienten nicht aufgenommen und versorgt werden können
- Als Folge konnten keine Notarztwagen, Hubschrauber oder keine Krankenwagen koordiniert werden, alle Ambulanzen waren geschlossen
- Eine Notfall-Patientin musste in ein entfernteres Krankenhaus nach Wuppertal gebracht werden, wo sie später verstarb

Quelle: https://www.deutschlandfunk.de/notaufnahme-geschlossen-der-hackerangriff-auf-die-uniklinik-100.html ; dpa/Roland Weihrauch

- Wegen eines Cyberangriffs wurden in mehreren Londoner Kliniken Operationen verschoben worden, da u.a. Bluttransfusionen nicht mehr möglich waren
- 1.517 akute ambulante Termine und 136 elektive Eingriffe mussten wegen des Angriffs verschoben werden
- Dies bedeutet bisher 4.913 akute ambulante Termine und 1.391 elektive Eingriffe, die seit dem 3. Juni im King's College Hospital, im NHS Foundation Trust und im Guy's and St Thomas' NHS Foundation Trust verschoben wurden

Quelle: https://www.zm-online.de/news/detail/versorgung-in-london-wird-monate-beeintraechtigt-sein ; chrisdorney - stock.adobe.com

- Das SickKids-Krankenhaus wurde Mitte Dezember Opfer eines Cyber-Angriffs. Um die betroffenen Systeme wieder online zu bringen, veranschlagte die Einrichtung zunächst mehrere Wochen
- Die SickKids-Klinik warnte zuvor vor längeren Wartezeiten und Verzögerungen bei Laboranalysen und Bildgebung aufgrund der bei dem Ransomware-Angriff lahmgelegten IT-Infrastruktur
- Die Cybergang Lockbit entschuldigt sich für einen Cyber-Angriff auf die größte kanadische Kinderklinik und gibt das Entschlüsselungstool kostenlos heraus

Quelle: https://www.heise.de/news/Cybergang-Lockbit-entschuldigt-sich-fuer-Angriff-auf-Kinderkrankenhaus-7445304.html ; Screenshot

NIS-2 Überblick

Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der EU

NIS2 Directive

Definition

- Richtlinie der EU für kritische Einrichtungen, die von EU-Staaten in nationales Recht überführt wird
- Die Richtlinie erweitert die NIS-1-Richtlinie von 2018
- Beinhaltet auch die Erweiterung des IT-Sicherheitsgesetz 2.0

Ziel

- Erweiterung des Geltungsbereichs auf mehr Sektoren
- Erhöhung der Cybersicherheitsstandards
- Sanktionen bei Nichteinhaltung
- Erhöhte Zusammenarbeit zwischen den EU-Mitgliedstaaten

Auswirkung

- Betroffenheit muss von Unternehmen selbst ermittelt werden
- Schätzung: etwa 30.000 Unternehmen allein in Deutschland betroffen
- Verschärfung der Meldepflichten und Sanktionsmaßnahmen

BSI-Meldepflicht

- Vorläufiger Bericht (24h)
- Vollständiger Bericht (72h)
- Abschlussbericht (1m)

Sanktionen

- Wesentliche Unternehmen:

bis zu 10 Mio. EUR oder 2% des Umsatzes

- Wichtige Unternehmen:

bis zu 7 Mio. EUR oder 1,4% des Umsatzes

Zielgruppe

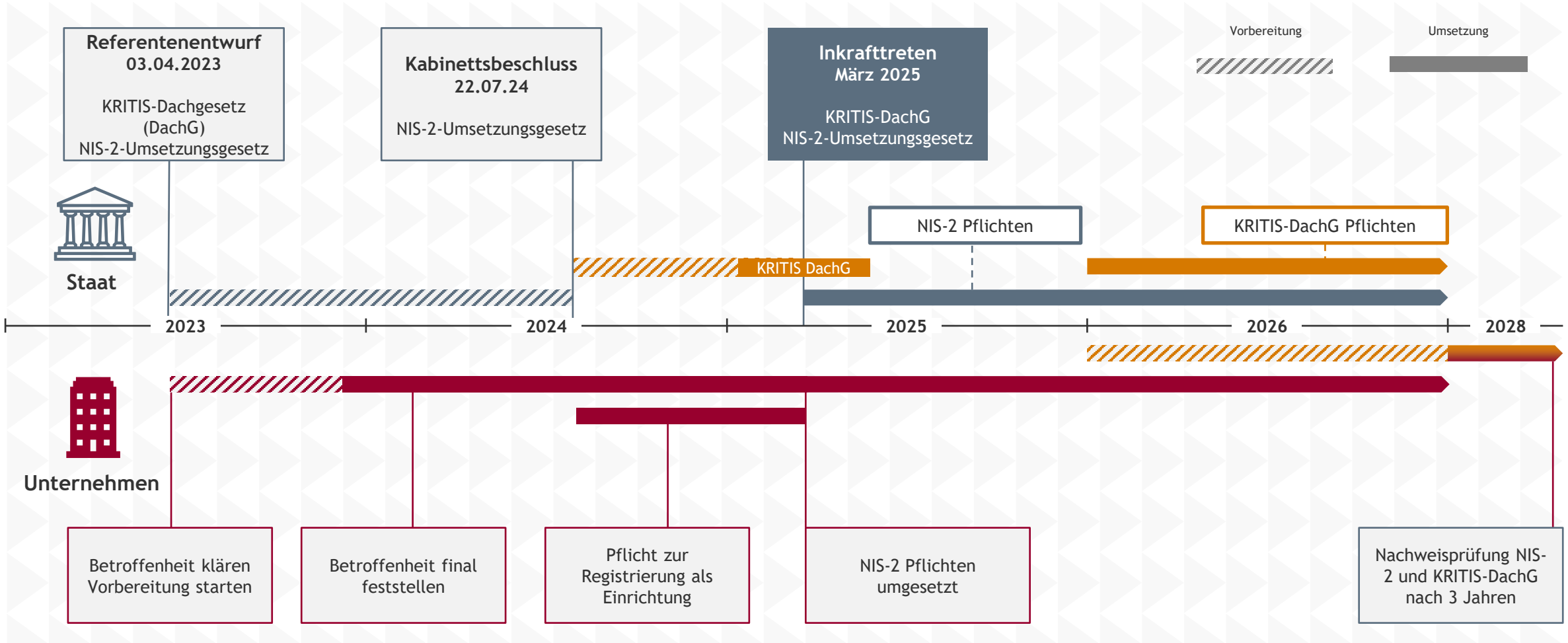
- Der Geltungsbereich geht weit über die bisher bekannten Schlüsselunternehmen der KRITIS hinaus
- Unterschieden wird anhand des Tätigkeitsbereichs
- Zusätzlich spielt die Unternehmensgröße und der Jahresumsatz eine bedeutende Rolle

	Wichtig	Besonders wichtig
Größe	Große Unternehmen > 250 > 50 Mio. Umsatz	Mittlere Unternehmen ≥ 50 – 250 10 - 50 Mio. Umsatz
Sektor*	Bsp.: Transport- und Finanzunternehmen	Bsp.: Herstellungs- und Chemieunternehmen

*keine vollumfängliche Darstellung

Hintergrund und Kontext der NIS-2-Richtlinie

Die nächsten Meilensteine im Überblick



Stand 25.09.2024

NIS-2 und KRITIS-DachG: Cybersicherheit auf nationaler Ebene

Schutz kritischer Infrastruktur in der EU

KRITIS

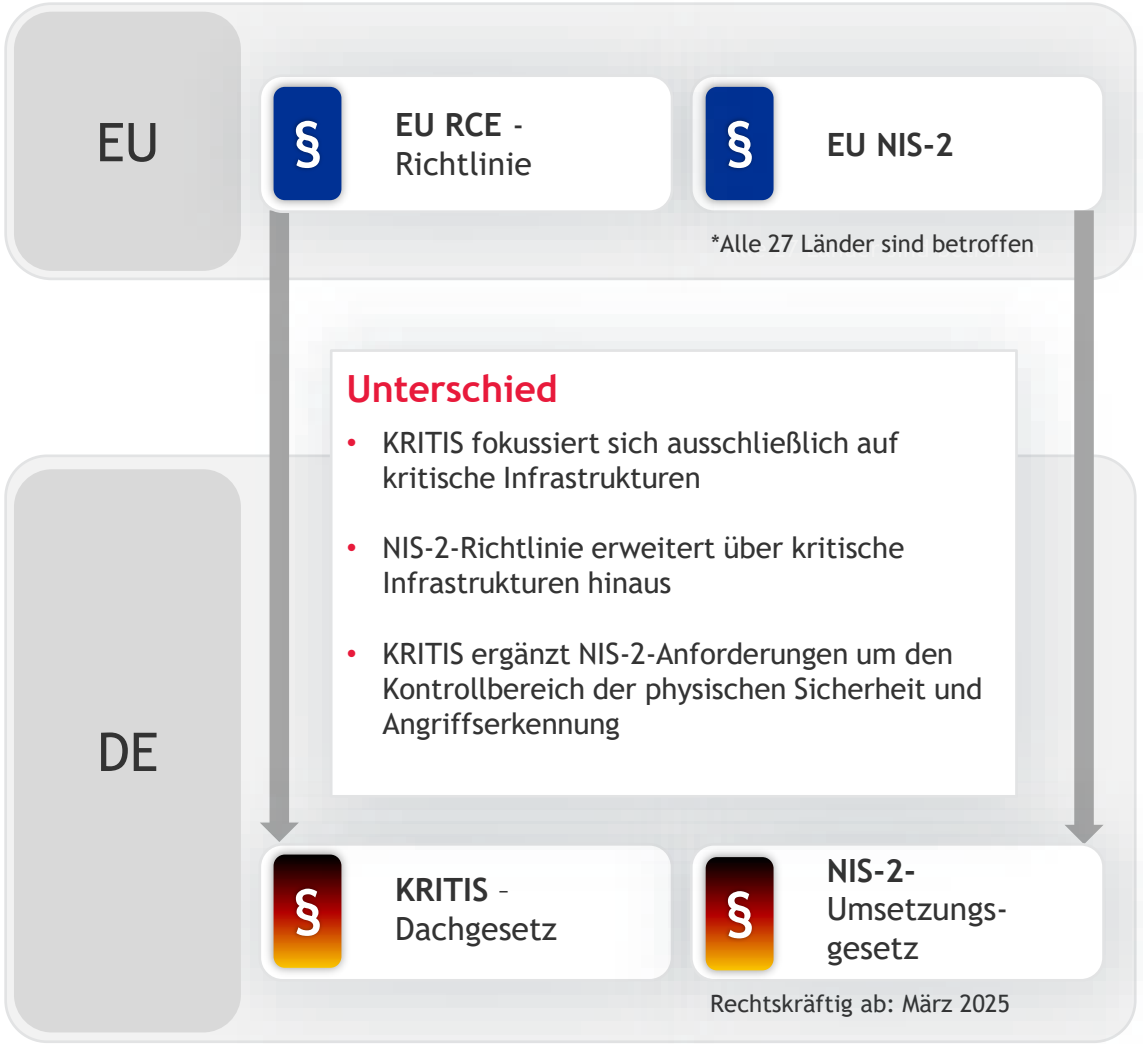
- Das KRITIS-Dachgesetz reguliert ab 2024 die Resilienz und physische Sicherheit kritischer Infrastrukturen
- Das Gesetz setzt die EU-Direktive EU RCE in Deutschland durch zusätzliche Pflichten für Betreiber kritischer Anlagen um
- Konkrete Vorgaben für Betreiber wie Meldepflichten, Krisen- und Risikomanagement, BCM, Personalsicherheit, physische Sicherheit
- Umsetzung in nationales Recht bis zum 18.10.2024

Kernelemente

- Einrichtung eines betrieblichen Risiko- und Krisenmanagements
- Erstellung von Resilienzplänen
- Umsetzung geeigneter Maßnahmen (technisch, personell, organisatorisch)

Zielgruppe

- Betroffen sind Betreiber kritischer Anlagen (KRITIS) in bisherigen KRITIS-Sektoren
- Betreiber kritischer Anlagen, wenn diese (in der Regel) über 500 Tsd. Personen versorgen

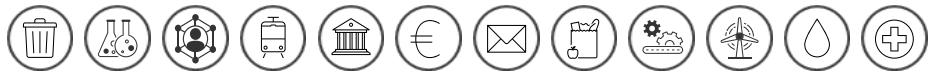


Betroffene Sektoren durch NIS-2

Übersicht der entscheidenden Betroffenheitskriterien

Prüfung der Sektoren und Schwellenwerte für KRITIS-Relevanz 1

RCE / **KRITIS-DachG** Betroffene



Qualifizierte Vertrauensdienste, TLD-Registries, DNS-Dienste

Prüfung des Sektors nach Anlage 1 & 2 2

Große Unternehmen

Sektoren:
Energie, Transport/Verkehr, Finanzwesen, Gesundheit, Wasser/Abwasser, Digitale Infrastruktur, Weltraum

Besonders Wichtig

≥ 250 Mitarbeiter

≥ 50 Mio Umsatz

Große und Mittlere Unternehmen

Sektoren:
Post/Kurier, Siedlungsabfallentsorgung, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Digitale Dienste, Forschung

Anlage 2

Mittlere Unternehmen

Sektoren:
Energie, Transport/Verkehr, Finanzwesen, Gesundheit, Wasser/Abwasser, Digitale Infrastruktur, Weltraum

Anlage 1

Wichtig

≥ 50 Mitarbeiter

> 10 Mio. Umsatz

3 Prüfung der Sektoren und Schwellenwerte nach NIS-2UmsuCG

4 Registrierung bei BSI & BBK

Spätestens 3 Monate nach Betroffenheit

Name der Einrichtung
Handelsregisternummer

Anschrift
Kontaktdaten, mindestens:
E-Mail
Telefonnummer

IP-Adressbereich(e)
Zutreffend(r) Sektor(en) & Teilsektor(en)
Liste der EU-Mitgliedsstaaten in denen die Tätigkeit(en) erfolgen.

Pflichten von Betreibern und Einrichtungen

Nachweise und Prüfungen

Maßnahmen und Pflichten	KRITIS-Betreiber	Besonders wichtig	Wichtig
Maßnahmen Risikomanagement (ISMS) und Business Continuity Management (BCMS)	✓	✓	✓
Höhere Maßstäbe für KRITIS	✓		
Besondere Maßnahmen SzA (Systeme zur Angriffserkennung)	✓		
Registrierung Selbständig bei der Kontaktstelle (BSI)	✓	✓	✓
Meldepflichten Meldung von Sicherheitsvorfällen innerhalb von 24 Std. Zwischenmeldungen, Fortschrittsmeldungen, Abschlussmeldung	✓	✓	✓
Nachweise/ Prüfungen	✓ Stichproben BBK	✓ Stichproben BSI	✓ bei Anlass
Informationsaustausch Teilnahme am Informationsaustausch	✓	✓	
Unterrichtungspflichten	✓	✓	✓
Governance Leitungsorgane	✓	✓	✓

Meldepflichten

- Erstmeldung bei erheblichen Sicherheitsvorfällen unverzüglich, spätestens innerhalb von 24h
- Folgemeldung über einen erheblichen Sicherheitsvorfall innerhalb von 72h mit Bewertung der Erstmeldung (Schwere, Auswirkungen, Kompromittierung)
- Zwischenmeldungen auf Nachfrage des BSI

Prüfung der Maßnahmenumsetzung

	Betreiber kritischer Anlagen		Einrichtungen	
			Besonders wichtig	Wichtig
Gesetz	NIS-2UmsuCG	DachG	NIS-2UmsuCG	NIS-2UmsuCG
Prüfungen	Alle drei Jahre	Teil von Audits	Stichproben durch BSI	Stichproben durch BSI
Inhalt	IT-Sicherheit Meldepflicht SzA	Resilienz	IT-Sicherheit Meldepflicht	IT-Sicherheit Meldepflicht
Stichproben	Tiefenprüfung	Nachweisqualität	Risikobasiert	Bei Anlass

NIS-2 im Detail: Maßnahmen

Übersicht der technischen und prozessualen Maßnahmen

Technische Maßnahmen

Management & Policies

- Asset Management
- Risikoanalyse und Sicherheit für Informationssysteme
- Bewertung der Cybersicherheit und Risiko-Management

Personal Security

- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Schulungen Cybersicherheit und Cyberhygiene

Physical Security

Supply Chain

- Sicherheit der Lieferkette und Dienstleistern

IT Security & Networks

- Multi-Faktor und kontinuierliche Authentisierung
- Management von Schwachstellen
- Kryptografie und Verschlüsselung
- Sichere Entwicklung, Beschaffung und Wartung

Business Continuity

- Sichere Notfallkommunikation
- Wiederherstellung, Backup Management, Krisen Management

Incident Management

- Bewältigung von Sicherheitsvorfällen

Prozessuale Maßnahmen

NIS-2 im Detail

Technische Maßnahmen

Angemessenheit der Maßnahmen

Besonders wichtige und wichtige Einrichtungen

müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen,

um die IT und Prozesse ihrer erbrachten Dienste zu schützen, Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu vermeiden und Auswirkungen von Sicherheitsvorfällen gering zu halten. §30 (1)

Zur Erfüllung der Anforderungen

können die branchenspezifischen BSI B3S Standards verwendet werden:

- Geben den neusten Stand der Technik wieder
- Gelten rechtskräftig
- Dienen zur Orientierung

Management von Schwachstellen

- Überwachung von Schwachstellenquellen (CSIRTs, Behörden), Durchführung von Scans und Behebung von Schwachstellen
- Schwachstellenmanagement, inklusive Dokumentation von Ausnahmen und regelmäßiger Überprüfung der Informationskanäle

Zugriffskontrolle & Anlagen-Management

- Verwendung von separaten, speziell gesicherten Systemen für die Systemadministration
- Zugriffskontrollrichtlinie für logischen und physischen Zugang
- Sicherheitsvorkehrungen für Administratorensysteme

Sichere Notfallkommunikation

- Meldeverfahren für Vorfälle mit Schulungen und Kommunikation für Mitarbeiter, Lieferanten und Kunden
- Kommunikation mit CSIRTs und Stakeholdern, sowie Protokollierung

Kryptografie und Verschlüsselung

- Proprietäre Festplattenverschlüsselung und Verschlüsselung von Laufwerken,
- Kryptographierichtlinien mit Maßnahmen zu Protokollen, Algorithmen, Schlüssellängen und Schlüsselmanagement

Asset Management

- Zuordnung von Schutzklassen (C/I/A/A)
- Vollständigkeit und Genauigkeit des Asset-Inventars
- Sicherstellung der Rückgabe von physischen Geräten (z. B. Laptops).
- Sichere Löschung von digitalen Informationen (z. B. durch Datenvernichtungstools)

Multi-Faktor und kontinuierliche Authentisierung

- Multi-Faktor Authentifizierung oder kontinuierlichen Authentifizierung,
- Gesicherte Sprach-, Video- und Textkommunikation sowie
- gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

NIS-2 im Detail

Prozessuale Maßnahmen

Geschäftsleitung ist persönlich für die Umsetzung der Maßnahmen haftbar

Bei **Verstoß** gegen die Vorgaben des Gesetzes sind **Bußgelder** zu zahlen:

- **Wichtige Einrichtungen:**
  von 100.000 EUR bis 7 Mio. EUR oder 1,4 % vom Umsatz
- **Besonders wichtige Einrichtungen:**
  100.000 EUR bis 10 Mio. EUR oder 2 % vom Umsatz

Sektor-Regelungen

Bestimmte Sektoren werden durch sektorspezifische Regulierungen konkretisiert oder umgesetzt.

1. **IT-Dienstleister und Sektoren** – NIS2 IT Implementing Act
2. **Betreiber öffentlicher TK-Netze und TK-Dienste** – Telekommunikationsgesetz und Bundesnetzagentur-Katalog
3. **Betreiber von Energieversorgungsnetzen und Energieanlagen** – Energiewirtschaftsgesetz und Bundesnetzagentur-Katalog
4. **Finanzeinrichtungen werden nach Digital Operational Resilience Act reguliert**

Bewertung der Cybersicherheit und Risiko-Management

- Penetrationstests
- KPIs
- Bewertung der Umsetzung und Wirksamkeit von Richtlinien
- Regelmäßige Überprüfung und Anpassung von Bewertungsrichtlinien und -prozessen

Personalsicherheit und Cyberhygiene

- Regelmäßige Schulungen und Programme zur Steigerung des Sicherheitsbewusstseins
- Durchführung von Hintergrundüberprüfungen
- Sicherstellung der Sicherheitsverantwortung durch Mitarbeiter und Dritte

Sichere Entwicklung, Beschaffung und Wartung

- Sicherheit von Lieferketten in ausgelagerte Entwicklungsprojekte
- Management und Dokumentation von Änderungen
- Sicherheitstests und Patchmanagement

Wiederherstellung, Backup Management, Krisen Management

- Rahmenwerk zur Kontinuitätsplanung
- Redundanz für Systeme und Kommunikation
- Festgelegte Rollen, Verantwortlichkeiten und Kommunikationsprozesse im Krisenmanagement

Bewältigung von Sicherheitsvorfällen

- Notfallhandbuch mit Checklisten
- Vollständigkeit und Genauigkeit der Log-Dokumentation
- Vorfallmanagement mit Reaktionsprozeduren, Nachbearbeitungen und Verbesserung der Sicherheit nach Vorfällen

NIS-2 vs. ISO 27001

Viele Gemeinsamkeiten, aber auch Unterschiede

Zertifizierung nach ISO 27001 ist ein erster Schritt zur NIS-2-Compliance

Gemeinsamkeiten 70%

Unternehmen können ihr ISO 27001-basiertes ISMS (Informationssicherheitsmanagementsystem) als Grundlage für den Nachweis der NIS-2-Anforderungen nutzen

Artikel der NIS2-Richtlinie

- EU-NIS-2 (2022/2555) in Artikel 20 (Governance)
- Artikel 21 (Maßnahmen)
- EU-RCE (2022/2557) Artikel 12 (Einschätzung des Risikos)
- Artikel 13 (Maßnahmen)

Gleiche Themen in ISO 27001 und NIS-2

- Risikobewertung & Management
- Datenklassifizierung
- Dokumentation
- Awareness Training
- Policies/Templates
- Supply Chain
- Reporting im Notfall (NIS-2 < 24 Stunden)
- Incident Response
- Management Approval Process
- Asset Management
- Backup Management

Differenzen 30%

Unterschiedliche Themen

- Netzwerksegmentierung – ISO
- Physische Sicherheit - ISO
- Meldepflichten – NIS-2

Überprüfung und Zertifizierung:

- NIS-2 ermöglicht Prüfung auf nationaler Ebene
- ISO 27001 setzt auf unabhängige Zertifizierungsstellen

Meldung von Sicherheitsvorfällen:

NIS-2 legt strengere Anforderungen an Meldepflichten und Umgang mit Vorfällen fest (z. B. Meldefristen, Meldestellen).

Umsetzungsbewusstere Anforderungen in der ISO 27001 im Vergleich zu NIS-2

- ISO gibt bestimmte Umsetzungsziele voraus während NIS2 an die Angemessenheit der Maßnahmenumsetzung adressiert ist

NIS-2 vs. ISO 22301

Viele Gemeinsamkeiten, aber auch Unterschiede

Zertifizierung nach ISO 22301 ist ein erster Schritt zur NIS-2-Compliance

Gemeinsamkeiten 70%

Unternehmen können ihr ISO 22301-basiertes BCMS (Business Continuity Managementsystem) als Grundlage für den Nachweis der NIS-2-Anforderungen nutzen

Artikel der NIS2-Richtlinie

- EU-NIS-2 (2022/2555) in Artikel 4 (Netz- und Informationssysteme)
- Artikel 8 (Sicherheitsmaßnahmen)
- Artikel 9 (Reaktions- und Wiederherstellungsmaßnahmen)
- Artikel 10 (Berichterstattung und Sicherheitsvorfälle)

Gleiche Themen in ISO 22301 und NIS-2

- Risikobewertung & Management
- Prävention
- Reaktionspläne
- Awareness Training, Notfallübungen
- Policies/Templates
- Kontinuitätsmanagement
- Dokumentation
- Berichterstattung

Differenzen 30%

Unterschiedliche Themen

- Business Impact Analyse – ISO
- Meldepflichten – NIS-2

Überprüfung und Zertifizierung:

- NIS-2 ermöglicht Prüfung auf nationaler Ebene
- ISO 22301 setzt auf unabhängige Zertifizierungsstellen

Business Impact Analyse:

NIS-2 erfordert keine Business Impact Analyse (BIA) für die Bewertung kritischer Geschäftsprozesse.

Umsetzungsbewusstere Anforderungen in der ISO 22301 im Vergleich zu NIS-2

- ISO gibt bestimmte Umsetzungsziele voraus während NIS2 an die Angemessenheit der Maßnahmenumsetzung adressiert ist

NIS-2 im Gesundheitswesen

Unsere derzeitige Einschätzung

Direkte Betroffenheit:

- Krankenhäuser (stationäre medizinische Versorgung)
- Produktion, Herstellung, Abgabe von lebenserhaltenden Med.-Produkten, sowie Arzneien und Blut-/Plasma
- Labore und Analytik

Indirekte Betroffenheit:

- Ambulante und (teil-)stationäre Pflegeeinrichtungen (Seniorenheime, Diakonie/Caritas, Pflegeheime, etc.)

Grundsätzlich **fallen Pflegeeinrichtungen indirekt unter NIS-2**, da

KRITIS-Studie des BSI:

- Einrichtungen sind kritisch, wenn sie intensivmedizinische Versorgung anbieten und eng mit Krankenhäusern kooperieren
- Einrichtungen für Menschen mit Behinderung gelten nicht primär als kritisch, außer bei spezialisierter Versorgung schwerwiegender Behinderungen

Umkehrschluss:

- Einrichtungen der medizinischen Intensivpflege außerhalb von Krankenhäusern fallen in den Scope von NIS-2 (Hospizdienste ausgenommen)

(Richtlinie 2011/24/EU):
Dienstleistungen zur Förderung „routinemäßiger Verrichtungen“ und „selbstbestimmten Lebens“ sind ausgenommen (Langzeitpflege, ambulante Pflegedienste, betreutes Wohnen)

Juristische Komplexität

Einzelfallbetrachtung notwendig

Stand 25.09.2024

Umsetzung der NIS-2-Richtlinie

Unsere Vorgehensweise zur NIS-2 Readiness

Modul 1

NIS-2 Betroffenheits-analyse

- Vorbereitung und Informations-beschaffung
- Betroffenheits-analyse
- Validierung & Dokumentation des Projektscopes & Status Quo

Modul 2

Soll-Ist-Abgleich

- Gap-Analyse
- Entwicklung und Priorisierung von Maßnahmen
- Ausarbeitung einer Roadmap zur Erreichung von NIS-2 Compliance

Modul 3

Programm Setup & PMO

Programmdefinition sowie Initiierung und Steuerung des Projekt Management Offices

Modul 4

Implementierung

Planung und Umsetzung der einzelnen Projekte auf Basis der verabschiedeten Roadmap

Modul 4a

Konzeption

Entwicklung benötigter Strategien und Konzepte für die Projektumsetzung in den NIS-2 Anforderungsbereichen

Modul 4b

Operationalisierung

Operative Umsetzung der Projekte gemeinsam mit internen und externen Stakeholdern

Prozessuale Maßnahmen

§ 30 Absatz 2 NIS-2UmsuCG

- Risikoanalyse
- Incident Management
- Business Continuity Management
- Sicherheit der Lieferketten
- Sicherheit: Erwerb, Entwicklung und Wartung
- Bewertung der Wirksamkeit
- Cyberhygiene und Schulungen

Technische Maßnahmen

- Kryptografie/ Verschlüsselung
- Zugriffskontrollen
- Asset Management
- Kontinuierliche- /ZF-Authentifizierung
- gesicherte (Notfall-) Kommunikation

Interaktives Beispiel: Cyber Risikomanagement

NIS-2-Compliance Vorbereitung

Exemplarische Darstellung am Beispiel Cyber Risikomanagement!

Bestandsaufnahme
zur Bearbeitung identifizierter Gaps.

Risikobewertung und Priorisierung
basierend auf der Gap Analyse

Maßnahmenplan und Umsetzung
zur NIS-2 Compliance

Überwachung und Dokumentation
für die Nachweisbarkeit

Modul 4

Implementierung

- Aufwände für Konzeption abhängig von der jeweiligen Feststellung und von weiteren Faktoren, z.B.:
- Unternehmensgröße (z.B. Anzahl Gesellschaften im Scope, Anzahl Mitarbeiter)
- Anzahl der Assets
- Anzahl involvierter Stakeholder pro Prozess

Modul 4a

Konzeption

- Prozess für Cyber Risikomanagement definieren und dokumentieren
- Rollen definieren (z.B. Risk Owner, Risiko Manager)
- Richtlinien und Vorgabedokumente erstellen
- Schulung der Mitarbeiter

Modul 4b

Operationalisierung

Beispiel: Cyber Risikomanagement

- ca. 50 IT-Assets mit erhöhten Schutzbedarf bzw. Teil der kritischen Einrichtung

➔ 50 Risikoanalysen

Zusammenfassung und Fragerunde

EU setzt neue Standards zur Stärkung der Cybersicherheit in kritischen Infrastrukturen

NIS2 Directive

Gibt es noch offene Fragen ?

Definition

- Richtlinie der EU für kritische Einrichtungen, die von EU-Staaten in nationales Recht überführt wird
- Die Richtlinie erweitert die NIS-1-Richtlinie von 2018
- Beinhaltet auch die Erweiterung des IT-Sicherheitsgesetz 2.0

Ziel

- Erweiterung des Geltungsbereichs auf mehr Sektoren
- Erhöhung der Cybersicherheitsstandards
- Sanktionen bei Nichteinhaltung
- Erhöhte Zusammenarbeit zwischen den EU-Mitgliedstaaten

Wesentliches

Prüfungen

- Nachweispflicht für Betreiber kritischer Anlagen alle 3 Jahre
- Dokumentationspflicht und Stichproben durch Behörden

BSI-Meldepflicht

- Vorläufiger Bericht (24h)
- Vollständiger Bericht (72h)
- Abschlussbericht (1m)

Sektorgesetze

TKG und EnWG, um Anforderungen von NIS2 für dortige Betreiber abzubilden. Für Finanzunternehmen wird DORA

Sanktionen

- Wesentliche Unternehmen:

bis zu 10 Mio. EUR oder 2% des Umsatzes

- Wichtige Unternehmen:

bis zu 7 Mio. EUR oder 1,4% des Umsatzes

Organisationen werden unterteilt nach:

- besonders wichtige
- oder wichtige Einrichtungen

Mindestens **30.000 Unternehmen** in Deutschland fallen unter NIS-2

Zielgruppe

Große Unternehmen

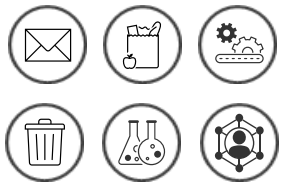
> 250

> 50 Mio. Umsatz

Mittlere Unternehmen

≥ 50 - 250

10 - 50 Mio. Umsatz



EU-Beschluss 2022 — **Referentenentwürfe** 2023 — **Gesetzgebung 07/24** — **Inkrafttreten 03/25** 2024

Ihre Ansprechpartner

Untertitel

Regine Knipper

Partnerin
Strategy & Governance
Tel.: +49 152 213 07589

Regine.Knipper@
bdosecurity.de

Liane Kiesewalter

Senior Consultant
BCM & ITSCM
Tel.: +49 351 866 91171

Liane.Kiesewalter@
bdosecurity.de

Stefan Zimmermann

Senior Consultant
BCM & ITSCM
Tel.: +49 351 866 91172

Stefan.Zimmermann@
bdosecurity.de

Vielen Dank für Ihre Aufmerksamkeit!

Wir unterstützen Sie gerne auf Ihrem Weg zur NIS-2-Compliance.