NIS2

Wie deutsche Unternehmen Cybersecurity neu denken müssen

“Cyberangriffe sind längst Alltag - mit NIS2 zieht die EU klare Konsequenzen.”

Jörg Deusinger

11.06.2025

Was ist NIS2?

Neue EU-Richtlinie zur Cybersicherheit vom 16.01.2023

EU NIS2

NIS2UMsuCG

- Umsetzung in nationales Recht bis 17.10.2024 (**NICHT EINGEHALTEN)**
- Ungefähr 30.000 Unternehmen in Deutschland betroffen

Aktueller Stand eingearbeitet: Referentenentwurf des BMI vom 26.05.2025

Warum sprechen wir über NIS2:

- NIS2 als **einheitliches Sicherheitsniveau gegen Cyberbedrohungen** in der EU
- **Cyberangriffe häufiger, gezielter, teurer:** Schäden stiegen 2024 laut einer Bitkom-Studie auf 266,6 Milliarden Euro

Nicht nur kritische Infrastruktur -> Jetzt auch Mittelstand und Bundesverwaltung betroffen

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

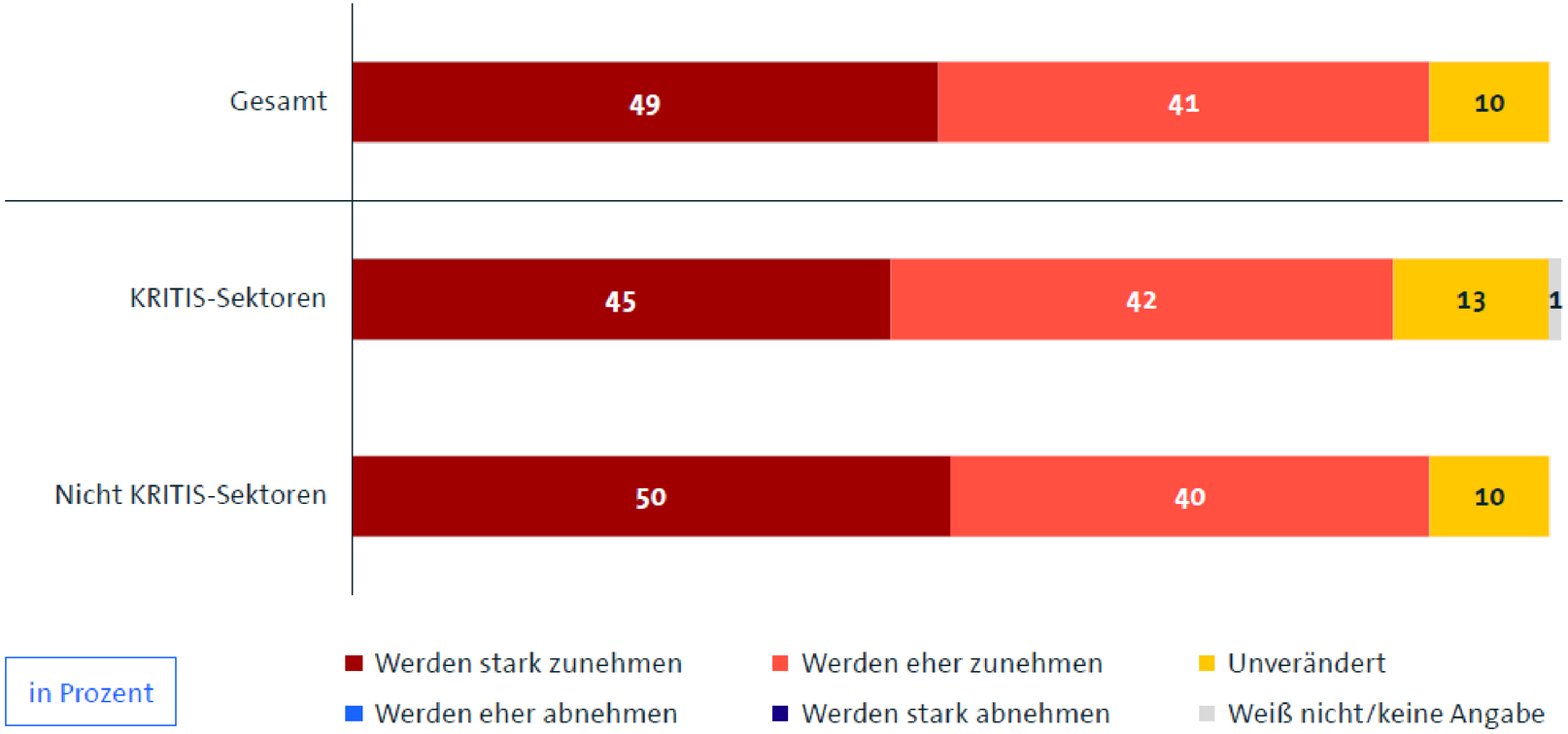
Schaden durch…	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4	18,3
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3	23,6
Patentrechtsverletzungen, auch vor Anmeldung	14,8	10,4	18,8
Erpressung mit gestohlenen Daten	13,4	16,1	10,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5	41,5
Geldabfluss durch Betrugsversuche	0,8	3,9	-
Sonstige Schäden	0	1,1	0,9
Gesamtschaden pro Jahr	**266,6**	**205,9**	**202,7**

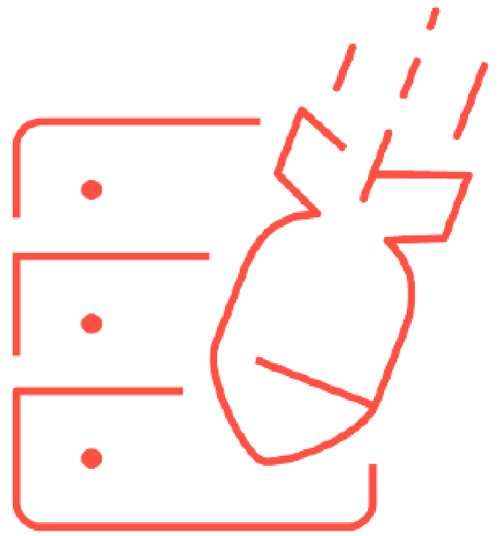
Basis: Alle Unternehmen (n=1.003) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2024

bitkom

Massive Zunahme von Cyberattacken befürchtet

Wie wird sich die Anzahl der Cyberattacken auf Ihr Unternehmen in den nächsten 12 Monaten im Vergleich zu den letzten 12 Monaten voraussichtlich entwickeln?





Basis: Alle Unternehmen (n=1.003) | Abweichungen von 100 Prozent sind rundungsbedingt | Quelle: Bitkom Research 2024

bitkom

Betroffenheit durch NIS2

Welche Einrichtungen betrachtet das NIS2UmsuCG:

Betreiber kritischer Anlagen (BSI-KritisV)

Besonders wichtige Einrichtungen (NIS2; Anlage 1)

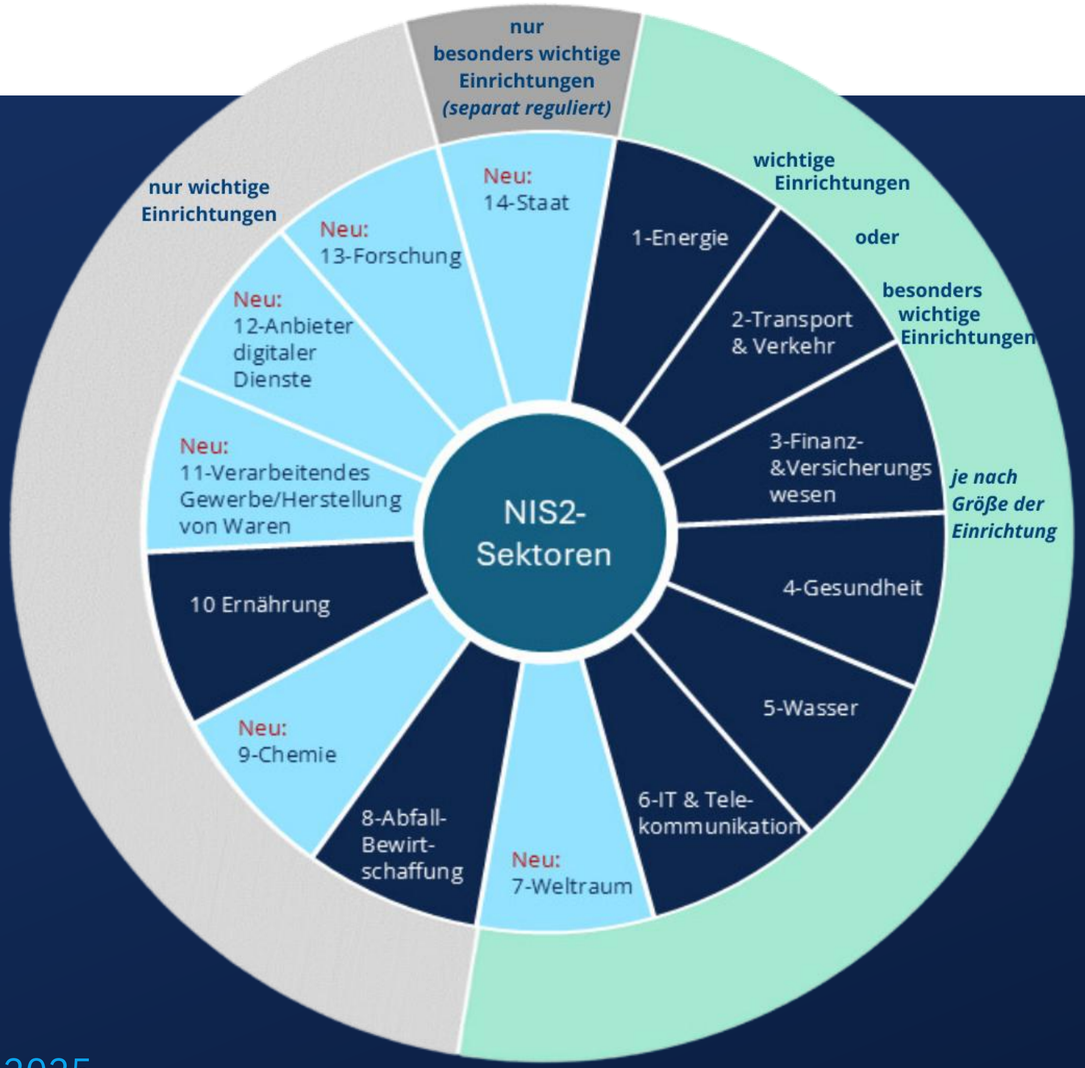
- **Schwellenwerte:** ≥ 250 Beschäftigte ***oder*** ≥ 25 Mio. € Umsatz ***und*** ≥ 43 Mio. € Bilanz

Wichtige Einrichtungen (NIS2; Anlage 1 u. 2)

- **Schwellenwerte:** ≥ 50 Beschäftigte ***oder*** ≥ 10 Mio. € Umsatz ***und*** ≥ 10 Mio. € Bilanz

Einrichtungen der Bundesverwaltung (separate Regelungen in NIS2 / nicht betrachtet)

Übersicht der Sektoren



Legende

neue NIS2-Sektoren

bereits bekannte KRITIS-Sektoren (BSI-KritisV)

NIS2UmsuCG
KRITIS-Sektoren

KRITIS-Sektoren (BSI-KritisV)	**Branchen** (Überschreitung der KRITIS-Schwellenwerte)
1 - Energie	Stromversorgung, Gasversorgung, Kraftstoff-/Heizölversorgung, Fernwärmeversorgung
2 - Transport und Verkehr	Luftverkehr, Schienenverkehr, Binnen/Seeschifffahrt, Straßenverkehr, ÖPNV, Logistik, Übergreifend: Wetter und Satellitennavigation
3 - Finanz- und Versicherungswesen	Bargeldversorgung, Kartengestützter Zahlungsverkehr, Konventioneller Zahlungsverkehr, Wertpapier- und Derivatgeschäfte, Versicherungsdienstleistungen, Sozialversicherung, Grundsicherung
4 - Gesundheitswesen	Stationäre medizinische Versorgung, Versorgung mit lebenserhaltenden Medizinprodukten, Versorgung mit Arzneien und Blut/Plasma, Laboratoriums Diagnostik
5 - Wasser und Abwasser	Trinkwasserversorgung, Abwasserbeseitigung
6 - Informationstechnik und Telekommunikation	Sprach- und Datenübertragung, Datenspeicherung und -verarbeitung
7 - Weltraum	Betrieb von Bodeninfrastrukturen
10 - Ernährung	**Lebensmittelversorgung:** Herstellung, Behandlung, Distribution, Handel, zentrale Steuerung
8 - Siedlungsabfallentsorgung	**Entsorgung von Siedlungsabfällen:** Sammlung und Beförderung, Verwertung und Beseitigung

NIS2UmsuCG
Anlage 1

Sektoren (Anlage 1) - *(besonders) wichtige Einrichtungen*	**Branchen** (keine Überschreitung der KRITIS-Schwellenwerte)
1 - Energie	Stromversorgung, Fernwärme/-kälte, Kraftstoff/Heizöl, Gasversorgung
2 - Transport und Verkehr	Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr
3 - Finanzwesen	Bankwesen (Kreditinstitute), Finanzmarktinfrastrukturen (Handelsplätze, zentrale Gegenparteien)
4 - Gesundheit	Gesundheitsdienstleistungen, EU-Referenzlaboratorien, F&E Arzneimittel, Herstellung Pharmazeutika sowie Medizinprodukten
5 - Wasser	Trinkwasserversorgung (Wasserversorgungsanlagen), Abwasserbeseitigung (Abwasser sammeln, entsorgen, behandeln)
6 - Digitale Infrastruktur (IT und Telekommunikation)	IXP, DNS, TLD, Cloud, RZ, CDNs, Vertrauensdienstanbieter, Betreiber öffentlicher Telekommunikationsnetze, Anbieter öffentlich zugänglicher Telekommunikationsdienste, Managed Services (MSP, MSSP)
7 - Weltraum	Bodeninfrastrukturen zur Unterstützung weltraumgestützter Dienste

NIS2UmsuCG
Anlage 2

Sektoren (Anlage 2) – *nur wichtige Einrichtungen*	**Branchen**
2 - Transport und Verkehr	Post und Kurierdienste
9 - Chemie (Produktion, Herstellung und Handel mit chemischen Stoffen)	Hersteller und Importeure
13 - Forschung	Forschungseinrichtungen
11 - Verarbeitendes Gewerbe/ Herstellung von Waren	Herstellung Medizinprodukte und In-vitro-Diagnostika Herstellung von DV-Geräte, Elektronik und Optik (NACE 26 und 27) Herstellung von elektrischen Ausrüstungen Maschinenbau (NACE 28) Herstellung von Kraftwagen und Teilen (NACE 29) Sonstiger Fahrzeugbau (NACE 30: Schiffe, Schienen, Luft/Raumfahrt, Fahrräder)
12 - Anbieter Digitaler Dienste	Anbieter von Online-Marktplätzen, Anbieter von Online-Suchmaschinen, Anbieter von Plattformen für Dienste sozialer Netzwerke
10 - Ernährung (Produktion, Verarbeitung und Vertrieb von Lebensmitteln)	Lebensmittelunternehmen (Produktion, Verarbeitung und Vertrieb)
8 - Abfallbewirtschaftung	Unternehmen der Abfallbewirtschaftung

NIS2UmsuCG
Pflichten der Betroffenen

Pflicht	Betreiber kritischer Anlagen (BSI-KritisV)	Besonders wichtige Einrichtung	Wichtige Einrichtung
Geltungsbereich	*Kritische Anlage(n)*	*Unternehmen*	*Unternehmen*
Maßnahmen Risikomanagement §30	✓	✓	✓
Höhere Maßstäbe für KRITIS §31 • Lageberichte des BSI • Schutzziel Verfügbarkeit	✓		
Besondere Maßnahmen SzA §31	✓		
Registrierung §33 §34	✓	✓	✓
Meldepflichten §32	✓	✓	✓
Nachweise §39 • KRITIS-Prüfungen/ Audits • Stichproben durch BSI	✓	Kontrolle durch (regelmäßige) **Stichproben**	**Keine Kontrollen**, bei begründetem Verdacht (Anlassbezogen)
Informationsaustausch §6 • Cybersicherheitswarnungen	✓	✓	✓
Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen §38	✓	✓	✓

Was verlangt NIS2 konkret?

- **Registrierungspflicht**
- **Risikomanagement** für IT & OT
- **Meldepflichten** bei Cybervorfällen
- **Schulungs- und Umsetzungspflicht** der Geschäftsleitung & Governance
- Weitergabe der Sicherheitsvorgaben an **Dienstleister & Lieferkette**
- **Nachweispflichten**

Registrierungspflicht

Registrierung innerhalb von 3 Monaten

- Name, Rechtsform, Kontaktdaten, Benennung Kontaktstelle, öffentliche IP-Adressbereiche, Sektor (Anlage 1 oder 2), EU-Staaten mit Geschäftsaktivitäten, Zuständige Aufsichtsbehörden des Bundes und der Länder
- **Für Betreiber kritischer Anlagen zusätzlich:** kritische Dienstleistung, öffentliche IP-Adressbereiche der von ihnen betriebenen Anlagen, ermittelte Anlagenkategorie, ermittelte Versorgungskennzahlen, Standort der Anlagen, Kontaktstelle (jederzeit erreichbar)

Benennung einer jederzeit erreichbaren Kontaktstelle

- daraus folgt: **Bereitschaft 24/7** um Informationen und Cybersicherheitswarnungen unverzüglich zu sichten und zu bewerten

Risikomanagement für IT & OT

1. Konzepte für Risikoanalyse und Sicherheit für IT-Systeme
2. Bewältigung von Sicherheitsvorfällen
3. Backup-Management und Wiederherstellung nach einem Notfall und Krisenmanagement
4. Sicherheit der Lieferkette
5. Sicherheitsmaßnahmen bei IT-Systemen, Komponenten und Prozessen

Risikomanagement für IT & OT

6. Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
7. Schulungen und Sensibilisierungen im Bereich der IT-Sicherheit
8. Konzepte und Prozesse für den Einsatz von kryptografischen Verfahren
9. Konzepte für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen
10. Verwendung von Multi-Faktor-Authentifizierung, gesicherte Notfallkommunikation

Meldepflichten bei erheblichen Cybervorfällen

- **Schritt 1: Erstmeldung** (unverzüglich, spätestens innerhalb 24h)
- **Schritt 2: Bewertung der Erstmeldung** (unverzüglich, spätestens innerhalb 72h)
- **Schritt 3: Zwischenmeldungen** (auf Nachfrage des BSI)
- **Schritt 4: Abschlussbericht** (innerhalb von 1 Monat)

Schulungs- und Umsetzungspflicht der Geschäftsleitung

Umsetzungspflicht der Geschäftsleitung:

- Geschäftsleitungen sind verspflichtet, die zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.

Schulungspflicht der Geschäftsleitung:

- Die **Geschäftsleitungen müssen regelmäßig (persönlich) an Schulungen teilnehmen**, um ausreichende Kenntnisse von Risikomanagementpraktiken zu erlangen und die Auswirkungen von Risiken beurteilen zu können.

Sicherheitsvorgaben an Dienstleister & Lieferkette

Um die **„Sicherheit der Lieferkette“** zu gewährleisten, müssen Anforderungen der NIS2 an die Lieferanten und Dienstleister weitergegeben werden

Beispiele für Vereinbarungen mit Lieferanten und Dienstleistern:

- Risikomanagementmaßnahmen,
- Bewältigung von Cybersicherheitsvorfällen,
- Meldepflichten,
- Patchmanagement, etc.

Daraus folgen auch gegebenenfalls **Anpassungen an Verträgen / Neuverhandlungen**

Nachweispflichten

- Die Nachweiserbringung durch **regelmäßige Prüfungen** gilt für **Betreiber kritischer Anlagen**

- Für **besonders wichtige und wichtige Einrichtungen** besteht **keine direkte Nachweispflicht,** das BSI kann jedoch einzelne Einrichtungen direkt oder anlassbezogen zu Prüfungen verpflichten oder Nachweise bei Sicherheitsvorfällen einfordern

Konsequenzen bei Nichteinhaltung

Bußgelder

- bis zu **10 Mio. € oder 2%** des globalen **Umsatzes**

Haftung des Managements

- deutlich höherer Druck als bisher

Reputationsschäden

- BSI veröffentlicht Informationen bei Sicherheitsvorfällen oder Nichteinhaltung von Maßnahmen

Erste Schritte für Unternehmen
Was sollten Betroffene zeitnah tun?

- Betroffenheit prüfen
- Gap-Analysen (wo stehen wir?)
- Partner und Lieferanten einbeziehen
- ISMS, BCMS implementieren
- Mitarbeiterschulungen starten
- Cybersecurity als Chef-Sache etablieren

Jörg Deusinger
Gründer und Geschäftsführer

de-bit Computer-Service GmbH
Seestraße 11
63571 Gelnhausen

Tel.:
Info: +49 6051 91675-0
Sec: +49 6051 91675-1800

Online:
info@de-bit.de
www.de-bit.de