NIS-2-Richtlinie im Überblick

SentiGuard

NIS-2 Richtlinie

Einführung und Zielsetzung

Die Richtlinie zielt darauf ab, die Cybersicherheit und den Schutz von Netz- und Informationssystemen in der gesamten EU zu verbessern. Es stärkt die Anforderungen an Unternehmen, die kritische Dienstleistungen und digitale Infrastrukturen betreiben.

Wichtige Anforderungen und Pflichten

- **Sicherheitsmaßnahmen: Unternehmen müssen robuste Sicherheitsstrategien implementieren, die sowohl technische als auch organisatorische Maßnahmen beinhalten, um Cyber-Risiken zu minimieren.**
- **Vorfallsmanagement: Verpflichtung, Sicherheitsvorfälle umgehend zu melden, einschließlich konkreter Meldefristen und Inhalte.**
- **Risikoanalyse: Regelmäßige Durchführung von Risikoanalysen und Umsetzung geeigneter Maßnahmen zur Risikominderung.**
- **Dokumentation und Audits: Unternehmen müssen ihre Sicherheitsmaßnahmen regelmäßig dokumentieren und Audit-Prozessen unterziehen.**

BETROFFENE UNTERNEHMEN

Unternehmen müssen eigenständig prüfen, ob sie unter den Anwendungsbereich der NIS-2 fallen, da sie keine offizielle Benachrichtigung erhalten.

Kriterien für die Betroffenheit:

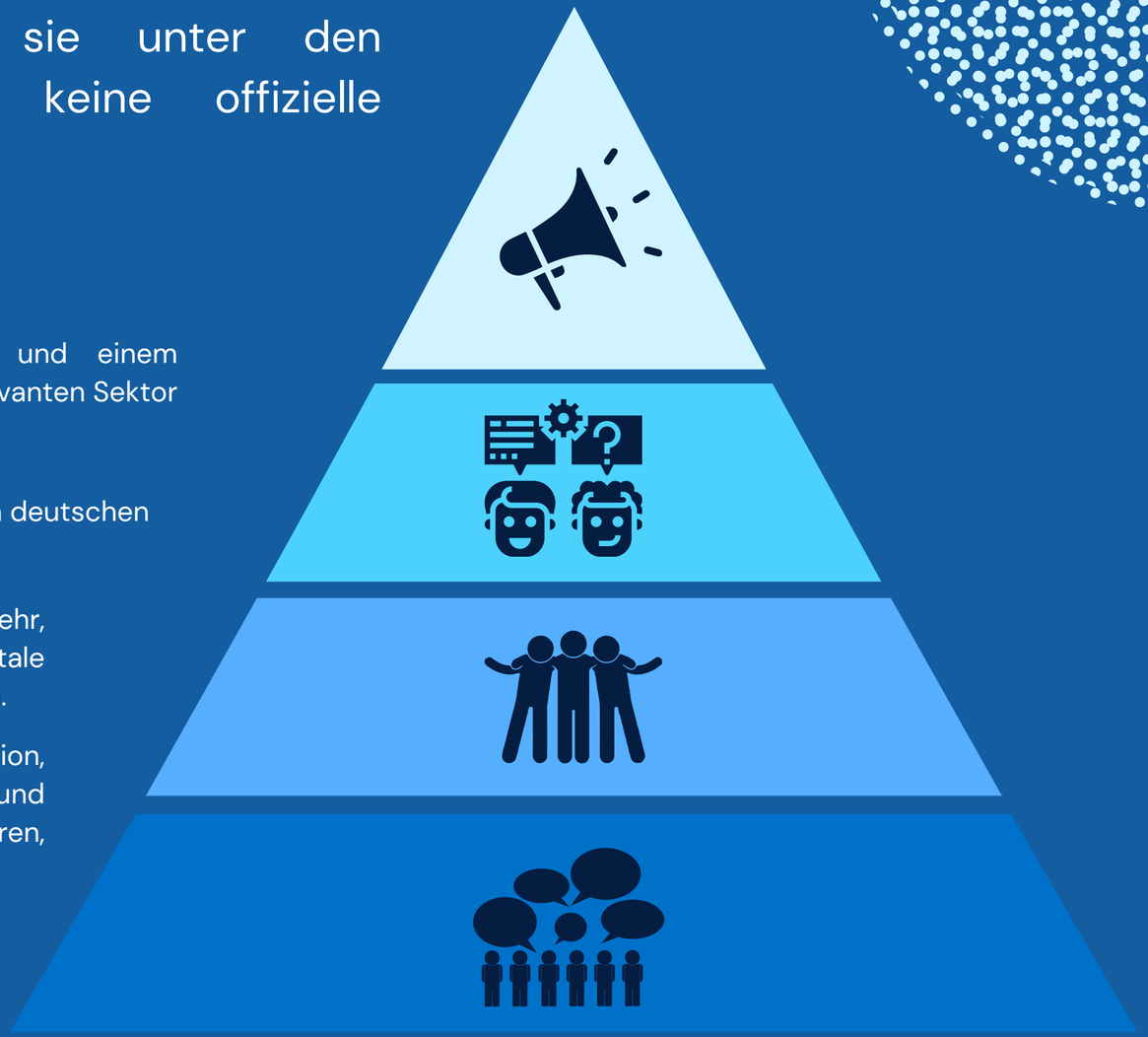
01 Unternehmensgröße: Unternehmen mit mehr als 50 Mitarbeitenden und einem Jahresumsatz von über 10 Millionen Euro sind betroffen, wenn sie in einem relevanten Sektor tätig sind.

02 Sektor: Die NIS-2 definiert 18 Unternehmenssektoren. Die genaue Zuordnung im deutschen Recht wird den Vorgaben der EU-Richtlinie folgen.

2A Anhang I = Sektoren mit hoher Kritikalität: Energie, Bankwesen, Verkehr, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung Weltraum.

2B Anhang II = Sonstige kritische Sektoren: AbfallbewirtschaftunG, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Verarbeitendes Gewerbe/Herstellung von Waren, Anbieter digitaler Dienste, Post- und Kurierdienste, Forschung.

03 Unabhängig von der Größe: Einige Organisationen können auch betroffen sein, wenn ein Ausfall systemische Risiken verursacht. (z.B. Teile der digitalen Infrastruktur und öffentlichen Verwaltung, alleinige Anbieter, KRITIS)



Maßnahmen zum Risikomanagement

01 Sicherheit bei Einkauf, Entwicklung, Verkauf und Wartung der IT-Systeme in der Lieferkette

02 Konzepte für Risikoanalyse und Sicherheit für Informationssysteme; Prävention, Erkennung und Bewältigung von Sicherheitsvorfällen

03 Cyberhygiene und Schulungen in Cybersicherheit, Kryptografie und ggf. Verschlüsselung, Personalsicherheit, Zugriffskontrolle und Asset Management, Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, Gesicherte Sprach-, Video- und Textkommunikation

04 Business Continuity und Bewertung der Wirksamkeit der Maßnahmen

05 Verantwortung der Geschäftsführung:

- Überwachung der Umsetzung der Maßnahmen und Haftung für Verstöße
- Teilnahme an Schulungen

06 Meldung der Sicherheitsvorfälle:

- innerhalb von **24 Stunden** ab Kenntnis Frühwarnung an die Behörde
- innerhalb von **3 Tagen** ein ausführlicher Bericht
- nach **1 Monat** ein Fortschritts-/Abschlussbericht

Bundeseinrichtungen

Im Rahmen der NIS2-Umsetzung unterliegt der öffentliche Sektor der Regulierung für Einrichtungen der Bundesverwaltung. Diese Einrichtungen übernehmen nicht nur die Pflichten besonders wichtiger Stellen, sondern haben auch zusätzliche Verantwortungen. Reguliert werden in der Bundesverwaltung, sofern keine ausdrücklichen Ausnahmen bestehen, gemäß §29 folgende Einrichtungen:

- Bundesbehörden
- Öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung
- Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, sofern dies durch das BSI angeordnet wurde

Es bestehen verschiedene Ausnahmen und Abgrenzungen für Einrichtungen der Bundesverwaltung:

- Der Geschäftsbereich des Bundesministeriums der Verteidigung
- Der Geschäftsbereich des Auswärtigen Amts
- Nachrichtendienste (BND und BfV)

Länder und Kommunen

Die deutschen Bundesländer und Kommunen sind in der Umsetzung der NIS2-Richtlinie nicht unmittelbar reguliert. Der Gesetzgeber auf Bundesebene verweist auf die Zuständigkeit der Länder und deren eigene Gesetzgebung.

Aus der Definition der regulären Einrichtungen sind ausdrücklich öffentliche IT-Dienstleister ausgeschlossen, die sich zu 100 Prozent im Besitz der Länder oder Kommunen befinden, keine Dienstleistungen für den Bund erbringen und durch Landesgesetze reguliert werden.

Anforderungen

An Bundeseinrichtungen werden damit folgende Anforderungen an Cybersicherheit gestellt:

- Meldepflichten für Sicherheitsvorfälle gemäß §31
- Umsetzungs- und Überwachungspflichten gemäß §38

Bundeseinrichtungen müssen zusätzlich erfüllen:

- Informationssicherheitsmanagement unter Berücksichtigung von IT-Grundschutz bzw. Mindeststandards für die Sicherheit der Informationstechnik des Bundes.

Forchungseinrichtungen

Im Forschungssektor stellen Einrichtungen der Allgemeinheit eine essenzielle Dienstleistung zur Verfügung – die Forschung für kommerzielle Zwecke. Diese Dienstleistung muss gemäß den Cybersecurity-Vorgaben der NIS2-Richtlinie geschützt werden.

Ab 2024 wird der Sektor durch die NIS2-Richtlinie umfassend reguliert. Unternehmen, die diese Dienstleistungen anderen anbieten und dabei die von NIS2 festgelegten Unternehmensgrößen überschreiten, gelten als wichtige Einrichtungen."

Forschung

	Unternehmen	Geltungsbereich
	Wichtige Einrichtung	Unternehmen (NIS2) • ≥50 Mitarbeiter oder • >10 Mio. EUR Umsatz und >10 Mio. EUR

NIS2-Sektordefinition Forschung:
- Forschungseinrichtungen, angewandt oder experimentell für kommerzielle Zwecke

Behördliche Aufsicht und Sanktionen

Wichtige Einrichtungen

Reaktive Aufsicht nach Hinweisen auf Verstöße
(z.B. gezielte Sicherheitsprüfungen)

Höchstbetrag von mind. 7 Mio. EUR
oder 1,4 % des weltweiten Umsatzes

Große Unternehmen aus Anhang II
- x > 249 Beschäftigte, oder
- x > 50 Mio. EUR Umsatz und > 43 Mio. EUR Bilanz

Mittlere Unternehmen aus Anhang I oder Anhang II
- mind. 50 Beschäftigte, oder
- x > 10 Mio. EUR Umsatz und > 10 Mio. EUR Bilanz
- kein großes Unternehmen

Größenunabhängige Sonderfälle: Einrichtungen, die vom Staat als „wichtig“ eingestuft werden

Wesentliche Einrichtungen

Proaktive Aufsicht
(z.B. regelmäßige Sicherheitsprüfungen)

Höchstbetrag von mind. 10 Mio. EUR
oder 2 % des weltweiten Umsatzes

Große Unternehmen aus Anhang I
- x > 249 Beschäftigte, oder
- x > 50 Mio. EUR Umsatz und > 43 Mio. EUR Bilanz

Größenunabhängige Sonderfälle:
DNS-Diensteanbieter, Zentralregierung, KRITIS, und Einrichtungen, die vom Staat als „wesentlich“ eingestuft werden