NIS-2-Richtlinie im Überblick

G DATA CyberDefense

Neue EU-Vorgaben für mehr Cybersicherheit

Mit der NIS-2-Richtlinie (EU) 2022/2555 gelten ab Oktober 2024 für viele Unternehmen und Organisationen in 18 Sektoren verpflichtende Sicherheitsmaßnahmen und Meldepflichten – auch für viele, die bisher nicht betroffen waren.

Was ist die NIS-2-Richtlinie?

- NIS = Netz- und Informationssystemsicherheit
- Ziel: hohes gemeinsames Cybersicherheitsniveau in der EU
- Gibt Mindeststandard vor, d.h. Länder dürfen strengere Vorschriften erlassen

Ab wann gilt NIS-2?

- Seit 2023 auf EU-Ebene in Kraft
- Bis 17. Oktober 2024 in nationales Recht umzusetzen
- Deutsches NIS2-Umsetzungsgesetz liegt als Referentenentwurf vor

Wen betrifft NIS-2?

Öffentliche und private Einrichtungen in 18 Sektoren mit mindestens 50 Beschäftigten oder mindestens 10 Mio. EUR Jahresumsatz und Jahresbilanz

Einige unabhängig von ihrer Größe (z.B. Teile der digitalen Infrastruktur und öffentlichen Verwaltung, alleinige Anbieter, KRITIS)

Übersicht der 18 betroffenen Sektoren

Anhang I der NIS-2 = Sektoren mit hoher Kritikalität:

- Energie
- Verkehr
- Bankwesen
- Finanzmarkt-infrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)
- öffentliche Verwaltung
- Weltraum

Anhang II der NIS-2 = 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

Was müssen betroffene Unternehmen und Organisationen tun?

Maßnahmen zum Risikomanagement für Cybersicherheit umsetzen

- Konzepte für Risikoanalyse und Sicherheit für Informationssysteme
- Prävention, Erkennung und Bewältigung von Sicherheitsvorfällen
- Business Continuity (z.B. Backup-Management) und Krisenmanagement
- Sicherheit in der Lieferkette
- Sicherheit bei Einkauf, Entwicklung und Wartung der IT-Systeme
- Bewertung der Wirksamkeit der Maßnahmen
- Cyberhygiene (z.B. Updates) und Schulungen in Cybersicherheit
- Kryptografie und ggf. Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Asset Management
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung
- Gesicherte Sprach-, Video- und Textkommunikation

ⓘ Entwurf deutsches Gesetz: nur zertifizierte IKT-Produkte und -Dienste dürfen genutzt werden.

Verantwortung der Geschäftsführung

- muss Umsetzung der Maßnahmen überwachen und haftet für Verstöße
- muss an Schulungen teilnehmen

Erhebliche Sicherheitsvorfälle melden

- innerhalb von 24 h ab Kenntnis Frühwarnung an die Behörde
- innerhalb von drei Tagen ein ausführlicher Bericht
- nach einem Monat ein Fortschritts-/Abschlussbericht

Wie sehen die behördliche Aufsicht und Geldstrafen aus?

	Wesentliche Einrichtungen	**Wichtige Einrichtungen**
Aufsicht durch Behörden	Proaktive Aufsicht (z.B. regelmäßige Sicherheitsprüfungen)	Reaktive Aufsicht nach Hinweisen auf Verstöße (z.B. gezielte Sicherheitsprüfungen)
Geldstrafen bei Verstößen	Höchstbetrag von mind. 10 Mio. EUR oder 2 % des weltweiten Umsatzes	Höchstbetrag von mind. 7 Mio. EUR oder 1,4 % des weltweiten Umsatzes
Wer zählt dazu?	**Große Unternehmen aus Anhang I** → > 249 Beschäftigte, oder → > 50 Mio. EUR Umsatz und > 43 Mio. EUR Bilanz **Größenunabhängige Sonderfälle:** z.B. DNS-Diensteanbieter, Zentralregierung, KRITIS, und Einrichtungen, die vom Staat als „wesentlich“ eingestuft werden	**Große Unternehmen aus Anhang II** → > 249 Beschäftigte, oder → > 50 Mio. EUR Umsatz und > 43 Mio. EUR Bilanz **Mittlere Unternehmen aus Anhang I oder Anhang II** → mind. 50 Beschäftigte, oder → > 10 Mio. EUR Umsatz und > 10 Mio. EUR Bilanz → kein großes Unternehmen **Größenunabhängige Sonderfälle:** Einrichtungen, die vom Staat als „wichtig“ eingestuft werden

Weitere Details zu NIS-2 erfahren Sie unter:
gdata.de/nis-2

G DATA CyberDefense