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. Die Informationen in diesem Merkblatt basieren auf der NIS-2 der EU sowie dem aktuellen deutschen Gesetzesentwurf.

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 17.10.2024 in nationales Recht umzusetzen
- Deutsches NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz (NIS2UmsuCG) liegt als Regierungsentwurf vor
- Nach Expertenvermutung tritt das NIS2UmsuCG nicht fristgerecht zum 17.10.2024 in Kraft
- Dennoch sollten Unternehmen die Vorgaben so schnell wie möglich umsetzen

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, Anbieter öffentlicher Telekommunikationsdienste, Betreiber öffentlicher Telekommunikationsnetze, 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 (Art. 1 § 30 im NIS2UmsuCG-Entwurf)

- 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

Verantwortung der Geschäftsführung (Art. 1 § 38 im NIS2UmsuCG-Entwurf)

- muss die Maßnahmen umsetzen und die Umsetzung überwachen
- haftet für Verstöße nach den Regeln des jeweiligen Gesellschaftsrechts
- muss an Schulungen teilnehmen

Erhebliche Sicherheitsvorfälle melden (Art. 1 § 32 im NIS2UmsuCG-Entwurf)

- 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?

	Besonders wichtige Einrichtungen (= „wesentliche Einrichtungen“ in der NIS-2)	**Wichtige Einrichtungen (= „wichtige Einrichtungen“ in der NIS-2)**
Aufsicht durch Behörden	Proaktive Aufsicht ohne vorige Hinweise auf Verstöße (z.B. Sicherheitsprüfungen nach Ermessen des BSI)	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. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter, KRITIS und teils Zentralregierung	**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:** z.B. Vertrauensdiensteanbieter **Hinweis:** Die Einstufung als „besonders wichtig“ geht immer vor.

Wie G DATA Lösungen Ihnen helfen, die NIS-2 zu erfüllen

Managed Extended Detection and Response

Vorgaben im NIS2UmsuCG-Entwurf:	So hilft Managed Extended Detection and Response
Art. 1 § 30 (2) 2): Bewältigung von Sicherheitsvorfällen (d.h. Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon) gemäß Stand der Technik	Unsere Analysten überwachen mit unserer eigens entwickelten Technologie Ihre IT-Systeme und reagieren für Sie auf Angriffe – rund um die Uhr. Detection-and-Response-Technologien entsprechen laut Bundesverband IT-Sicherheit e.V. (TeleTrusT) dem Stand der Technik.
Art. 1 § 32 (1): Meldung erheblicher Sicherheitsvorfälle an die Behörden mit kurzen Fristen	Dank gemanagter Angriffserkennung und -abwehr auf Ihren IT-Systemen können Sie kurze Meldefristen im Ernstfall einhalten.

Security Awareness Trainings

Vorgaben im NIS2UmsuCG-Entwurf:	So helfen die Security Awareness Trainings
Art. 1 § 38 (3) / § 30 (2) 7): Schulungen im Bereich der Cybersicherheit für Geschäftsführung und Mitarbeitende	Mit spannenden Online-Kursen schulen Sie Ihre Geschäftsführung und Mitarbeitenden in IT-Sicherheit. Dank langfristigem Lernkonzept erfüllen Sie spielend leicht die NIS-2-Pflicht zu regelmäßigen Schulungen.

„Als Unternehmen im besonderen öffentlichen Interesse (kurz: UBI) müssen wir genau prüfen, wo wir uns in der neuen NIS2-Richtlinie der EU wiederfinden und was auf uns zukommt. Beruhigend ist, dass wir einige Punkte mit den Awareness Trainings und MXDR von G DATA schon gut abgedeckt haben.“

Heiko Streichert, IT-Administrator, etna GmbH

Warum G DATA?

NIS-2-pflichtige Unternehmen müssen die IT-Sicherheit ihrer Zulieferer und Dienstleister berücksichtigen. Als deutsches Unternehmen fällt G DATA selbst unter die NIS-2 – und steht Ihnen mit IT Security „Made in Germany“ als vertrauenswürdiger Dienstleister zur Seite.

Beginnen Sie jetzt, um ab Oktober 2024 NIS-2-konform zu sein. Mehr Details:
gdata.de/nis-2

G DATA CyberDefense