NIS-2-Richtlinie im Überblick

G DATA CyberDefense

Neue EU-Vorgaben für mehr Cybersicherheit

Mit der NIS-2-Richtlinie (EU) 2022/2555 sind bereits seit Oktober 2024 für viele Unternehmen und Organisationen in 18 Sektoren verpflichtende Sicherheitsmaßnahmen und Meldepflichten vorgesehen – auch für viele, die bisher nicht betroffen waren. Sie muss allerdings jeweils in nationales Recht umgesetzt werden. 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; ist in vielen Staaten aber noch offen
- Deutsches NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz (NIS2UmsuCG) lag als Regierungsentwurf vor, wird aber vsl. überarbeitet
- Nach Expertenvermutung tritt ein NIS2UmsuCG nicht vor Herbst 2025 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
- Möglicherweise sehr viele weitere Unternehmen indirekt über die Lieferkette

- Einige unabhängig von ihrer Größe (z.B. Teile der digitalenInfrastruktur 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
- Abwasser
- Verkehr
- Digitale Infrastruktur
- Bankwesen
- Verwaltung von IKT-Diensten (B2B)
- Finanzmarkt-infrastrukturen
- öffentliche Verwaltung
- Gesundheitswesen
- Weltraum
- Trinkwasser

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

Art. 1 § 30: Risikomanagementmaßnahmen

Vorgaben im NIS2UmsuCG-Entwurf:	G DATA Lösungen
Art. 1 § 30 (1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die durch Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten (…). (2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen: 1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik	**IT-Security Assessment** Erhalten Sie eine objektive Risikoeinschätzung und Beurteilung Ihres Cybersecurity Levels.
	Penetration Test Finden Sie Ihre Sicherheitslücken, bevor Cyberkriminelle es tun.
(2) 2. Bewältigung von Sicherheitsvorfällen [d.h. Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon];	**Managed Extended Detection and Response** Ihr 24/7-Expertenschutz: Wir erkennen und stoppen Cyberangriffe für Sie.
	Incident Response Vertrauen Sie auf Sofort-Hilfe bei Sicherheitsvorfällen durch unser erfahrenes Notfallteam.
	Incident Response Rahmenvertrag Ihre optimale Kombination aus Prävention und Sofort-Hilfe.
(2) 4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	**ISO 27001** G DATA ist nach ISO 27001:2022 zertifiziert, sodass Sie Ihre Pflichten einfacher nachweisen können. Zudem können wir eine Komfortlösung für vertragliche Fragen mit uns anbieten.
(2) 6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik	**IT-Security Assessment** Erhalten Sie eine objektive Risikoeinschätzung und Beurteilung Ihres Cybersecurity Levels.
(2) 7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik	**Security Awareness Trainings** Mit spannenden Online-Kursen schulen Sie Ihre Geschäftsführung und Mitarbeitenden in IT-Sicherheit.

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

Art. 1 § 32: Meldepflichten

Vorgaben im NIS2UmsuCG-Entwurf:	G DATA Lösungen
Art. 1 § 32 (1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, folgende Informationen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden: 1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte	**Managed Extended Detection and Response** Dank gemanagter Angriffserkennung und -abwehr in Ihrer IT-Umgebung können Sie kurze Meldefristen im Ernstfall einhalten.
(1) 2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über diesen Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden. 3. auf Ersuchen des Bundesamtes eine Zwischenmeldung über relevante Statusaktualisierungen	**Managed Extended Detection and Response** Dank gemanagter Angriffserkennung und -abwehr in Ihrer IT-Umgebung können Sie kurze Meldefristen im Ernstfall einhalten.
(1) 4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält: a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls Die Verpflichtung nach Satz 1 gilt frühestens ab Einrichtung des Meldewegs.	**Incident Response** Die Hilfe unseres Notfallteams ermöglicht Ihnen, die Pflicht zum Abschlussbericht (Ursachenanalyse etc.) einzuhalten. **Incident Response Rahmenvertrag** Ihre optimale Kombination aus Prävention und Sofort-Hilfe im Notfall – zur Einhaltung des Abschlussberichts.

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

Art. 1 § 38: Schulungspflicht der Geschäftsleitung

Vorgaben im NIS2UmsuCG-Entwurf:	G DATA Lösungen
Art. 1 § 38 (3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.	**Security Awareness Trainings** Mit spannenden E-Learning-Angeboten schulen Sie Ihre Geschäftsführung und Mitarbeitenden in IT-Sicherheit. **Incident Readiness Trainings** Bereiten Sie sich optimal auf Cyberangriffe vor – um im Ernstfall Zeit und Kosten zu sparen.

„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 NIS-2-konform zu sein.
Mehr Details: gdata.de/nis-2

G DATA CyberDefense