NIS-2-Richtlinie im Überblick

G DATA CyberDefense

Was die EU-Richtlinie und das deutsche Gesetz für Sie bedeuten

Mit der NIS-2-Richtlinie (EU) 2022/2555 und dem deutschen Umsetzungsgesetz gelten für viele Unternehmen und Organisationen verpflichtende Sicherheitsmaßnahmen und Meldepflichten. Bei Verstößen drohen hohe Geldstrafen.

Was ist die NIS-2-Richtlinie?

- NIS = Netz- und Informationssystemsicherheit
- Ziel: hohes gemeinsames Cybersicherheitsniveau in der EU

Wie hängen NIS-2 und BSI-Gesetz zusammen?

- NIS-2-Umsetzungsgesetz enthält selbst keine inhaltlichen Vorgaben
- Stattdessen fasst es in Art. 1 das BSI-Gesetz (2025) neu

Seit wann gilt NIS-2?

- Seit 2023 auf EU-Ebene in Kraft
- Als Richtlinie nicht direkt anwendbar, sondern erst in nationales Recht umzusetzen
- Das deutsche NIS-2-Umsetzungsgesetz ist am 06. Dezember 2025 in Kraft getreten
- Keine Übergangsfrist, d.h. Pflichten gelten sofort

Wen betrifft NIS-2?

- Öffentliche und private Einrichtungen in 14 Sektoren mit mindestens 50 Beschäftigten oder mindestens 10 Mio. EUR Jahresumsatz und Jahresbilanz
- ggf. viele weitere indirekt über die Lieferkette
- Einige unabhängig von ihrer Größe (z.B. Teile der digitalen Infrastruktur und öffentlichen Verwaltung, Anbieter öffentlicher Telekommunikationsdienste, Betreiber öffentlicher Telekommunikationsnetze, KRITIS)

Übersicht der 14 betroffenen Sektoren

Anlage I im BSI-Gesetz (2025)
= Sektoren mit hoher Kritikalität:

- Energie
- Transport und Verkehr (Luft, Schiene, Schiff, Straße)
- Finanzwesen
- Gesundheit
- Wasser
- Digitale Infrastruktur
- Weltraum

Anlage II im BSI-Gesetz (2025)
= Sonstige kritische Sektoren:

- Transport und Verkehr (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

§ 30 BSI-Gesetz (2025)

- 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

§ 38 BSI-Gesetz (2025)

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

Erhebliche Sicherheitsvorfälle melden

§ 32 BSI-Gesetz (2025)

- 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 Anlage 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 Anlage II** → > 249 Beschäftigte, oder → > 50 Mio. EUR Umsatz und > 43 Mio. EUR Bilanz **Mittlere Unternehmen aus Anlage I oder Anlage 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

§ 30 BSI-Gesetz (2025): Risikomanagementmaßnahmen

Vorgaben im Gesetz:	G DATA Lösungen
§ 30 (1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die in 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 zu 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 Schulungen und Sensibilisierungsmaßnahmen 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

§ 32 BSI-Gesetz (2025): Meldepflichten

Vorgaben im Gesetz:	G DATA Lösungen
§ 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

§ 38 BSI-Gesetz (2025): Schulungspflicht der Geschäftsleitung

Vorgaben im Gesetz:	G DATA Lösungen
§ 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.

NIS-2-Beratung

Haben Sie bereits ein NIS-2 Gap Assessment durchgeführt und stehen nun vor Herausforderungen in der Umsetzung? Oder brauchen Sie Rat, welcher Handlungsbedarf sich aus NIS-2 für Sie ergibt? Egal, wo Sie stehen: Unsere IT-Sicherheitsexperten begleiten Sie Schritt für Schritt auf dem Weg zur NIS-2-Compliance.

„Es gibt keine Übergangsfrist. Die Pflichten und Sanktionen gelten seit Inkrafttreten des deutschen Gesetzes am 06. Dezember 2025. Unternehmen müssen die Nachweise zur Umsetzung zwar normalerweise erst nach 3 Jahren einreichen. Aber wer auffällt oder besonders relevant ist, muss schon vorher damit rechnen, dass unabhängige Stellen die Umsetzung prüfen. Für Unternehmen wird es also höchste Zeit.“

Dr. Matthias Zuchowski, Regulatory Affairs & Compliance Manager, G DATA CyberDefense AG

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. G DATA ist nach ISO 27001:2022 zertifiziert, sodass Sie Ihre Pflichten einfacher nachweisen können.

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

G DATA CyberDefense