EUROPÄISCHE UNION

NIS2-RICHTLINIE

(Richtlinie EU 2022/2555)

Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union

Deutsche Zusammenfassung für CISOs und Compliance-Verantwortliche

Dokumentreferenz

Feld	Wert
Offizieller Name	Richtlinie (EU) 2022/2555
Annahmedatum	14. Dezember 2022
Veröffentlichungsdatum	27. Dezember 2022 (ABl. L 333/80)
Inkrafttreten	16. Januar 2023
Umsetzungsfrist der Mitgliedstaaten	17. Oktober 2024
Aufgehobenes Instrument	Richtlinie (EU) 2016/1148 (NIS1)

> Dieses Dokument ist eine inoffizielle Zusammenfassung der EU-NIS2-Richtlinie vom 14. Dezember 2022; es ist keine verbindliche Übersetzung. Für eine verbindliche Auslegung ist der offizielle Text im ABl. L 333/80, 27.12.2022 heranzuziehen.

Inhaltsverzeichnis

1. Zusammenfassung
2. Zweck und Rechtsgrundlage
3. Von NIS1 zu NIS2: Warum eine neue Regelung?
4. Anwendungsbereich und ausgenommene Bereiche
5. Wesentliche Definitionen
6. Einrichtungskategorien: Wesentliche und wichtige Einrichtungen
7. Erfasste Sektoren (Anhang I und Anhang II)
8. Pflichten der Mitgliedstaaten
9. Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Artikel 21)
10. Meldepflichten bei Sicherheitsvorfällen (Artikel 23)
11. Sicherheit der Lieferkette
12. Verantwortung des Leitungsorgans
13. Kooperationsstrukturen auf EU-Ebene
14. Aufsicht und Durchsetzung
15. Verwaltungsgeldbußen
16. Umsetzungszeitplan und Übergangsbestimmungen
17. Auswirkungen auf Unternehmen außerhalb der EU
18. Praktischer Compliance-Fahrplan (10 Schritte)
19. Fazit und Bewertung

1. Zusammenfassung

Die **NIS2-Richtlinie** (Richtlinie EU 2022/2555), am 14. Dezember 2022 vom Europäischen Parlament und dem Rat angenommen, ist die allgemeine Cybersicherheits-Basisrichtlinie der EU. Sie hebt die frühere NIS1-Richtlinie 2016/1148 mit Wirkung ab dem 18. Oktober 2024 auf und ersetzt sie.

Überprüfungen haben ergeben, dass NIS1 zwar dazu beigetragen hat, das Niveau der Cyberresilienz in der Union anzuheben, jedoch nicht ausreicht, um den heutigen und zukünftigen Cybersicherheitsbedrohungen zu begegnen. NIS2 erweitert den Anwendungsbereich erheblich, führt einheitliche Kriterien ein, stärkt die Risikomanagement- und Meldepflichten und sieht abschreckendere Durchsetzungsbestimmungen vor.

Die fünf Säulen der Richtlinie

1. **Erweiterter Anwendungsbereich**: mehr Sektoren und Unternehmen werden reguliert.
2. **Verschärftes Risikomanagement**: 10 technische und organisatorische Mindestmaßnahmen sind nach Artikel 21 verpflichtend.
3. **Schnelle und phasenweise Meldung von Sicherheitsvorfällen**: 24-Stunden-Frühwarnung, 72-Stunden-Meldung, Abschlussbericht nach einem Monat.
4. **Verantwortung des Leitungsorgans**: die Geschäftsführung kann persönlich haftbar gemacht werden.
5. **Abschreckende Sanktionen**: Verwaltungsgeldbußen bis zu 2 % des weltweiten Jahresumsatzes oder EUR 10 Millionen.

2. Zweck und Rechtsgrundlage

Die Rechtsgrundlage der Richtlinie ist **Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)**, der verstärkte Maßnahmen zur Angleichung der einzelstaatlichen Vorschriften vorsieht, die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.

Die wesentlichen Ziele der Richtlinie sind:

- Große Divergenzen zwischen den Mitgliedstaaten beseitigen und gemeinsame Mindest-Cybersicherheitsregeln festlegen;
- Wirksame Mechanismen für die grenzüberschreitende Zusammenarbeit und den Informationsaustausch einrichten;
- Die Liste der Sektoren und Tätigkeiten, die Cybersicherheitspflichten unterliegen, aktualisieren, um der heutigen Bedrohungslage Rechnung zu tragen;
- Durchsetzungs- und Abhilfemechanismen bereitstellen, die eine wirksame Umsetzung der Pflichten gewährleisten;
- Die Cyberresilienzkapazitäten von Betreibern kritischer Infrastrukturen und Anbietern digitaler Dienste stärken.

Die Richtlinie gilt unbeschadet des und im Einklang mit dem EU-Recht zum Schutz personenbezogener Daten (DSGVO, Verordnung EU 2016/679) und zur Privatsphäre bei der elektronischen Kommunikation (Richtlinie 2002/58/EG).

3. Von NIS1 zu NIS2: Warum eine neue Regelung?

NIS1, die 2016 in Kraft trat, war die erste horizontale Cybersicherheitsregulierung der EU. Der Überprüfungsprozess offenbarte erhebliche Umsetzungsunterschiede zwischen den Mitgliedstaaten; die Festlegung des Anwendungsbereichs wurde weitgehend dem Ermessen der Mitgliedstaaten überlassen, was den Binnenmarkt fragmentierte.

Festgestellte Schwächen von NIS1

Problembereich	NIS1-Lage	NIS2-Lösung
Bestimmung des Anwendungsbereichs	Im Ermessen der Mitgliedstaaten; erhebliche Unterschiede in der Praxis.	Einheitliche Größenschwellenregel in der gesamten EU (mittlere und große Unternehmen).
Sektorenliste	Begrenzte Anzahl von Sektoren; ein erheblicher Teil der digitalen Wirtschaft ausgeschlossen.	Deutlich breitere Sektorabdeckung; digitale Infrastruktur, öffentliche Verwaltung, Raumfahrt u. a. einbezogen.
Meldung von Sicherheitsvorfällen	Einstufig; Fristen und Inhalte variierten zwischen den Mitgliedstaaten.	Mehrphasige Meldung: 24-Stunden-Frühwarnung + 72-Stunden-Meldung + Abschlussbericht nach einem Monat.
Risikomanagement	Allgemeine Formulierungen; konkrete Mindestmaßnahmen unklar.	Artikel 21 listet 10 verpflichtende Mindestmaßnahmen-Kategorien auf.
Sanktionen	In den Mitgliedstaaten sehr unterschiedlich umgesetzt.	EU-weit harmonisierte Höchstbußen (EUR 10 Mio. / 2 % des Umsatzes).
Verantwortung der Geschäftsführung	Nicht klar geregelt.	Leitungsorgan persönlich haftbar für die Einhaltung; verpflichtende Schulungen.

NIS2 ist keine Aktualisierung von NIS1; sie ist ein Ersatz, der einen **einheitlichen, harmonisierten und durchsetzbaren Cybersicherheitsrahmen** in der gesamten Union schaffen soll.

4. Anwendungsbereich und ausgenommene Bereiche

Die Richtlinie erfasst in erster Linie Einrichtungen, die in der EU in Sektoren des **Anhangs I (mit hoher Kritikalität)** oder des **Anhangs II (sonstige kritische Sektoren)** tätig sind und die Definition eines mindestens mittleren Unternehmens erfüllen. Gemäß Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission ist ein mittleres Unternehmen eines mit weniger als 250 Beschäftigten und einem Jahresumsatz von höchstens EUR 50 Millionen (oder einer Bilanzsumme von höchstens EUR 43 Millionen). NIS2 erfasst Einrichtungen ab der Schwelle des mittleren Unternehmens; die praktische Untergrenze für in den Anwendungsbereich fallende Einrichtungen liegt bei 50 Beschäftigten oder EUR 10 Millionen Umsatz (die Obergrenze eines "Kleinunternehmens" nach derselben Empfehlung).

Unabhängig von der Größe erfasste Einrichtungen

- Anbieter öffentlicher elektronischer Kommunikationsnetze und öffentlich zugänglicher elektronischer Kommunikationsdienste;
- Vertrauensdiensteanbieter (gemäß eIDAS-Verordnung EU 910/2014);
- Namenregister für Domänen der obersten Stufe (TLD) und DNS-Diensteanbieter;
- Einrichtungen, die in einem Mitgliedstaat der einzige Anbieter eines Dienstes sind oder bei denen eine Dienstunterbrechung die öffentliche Sicherheit, Gesundheit oder Ordnung erheblich beeinträchtigen könnte;
- Alle Einrichtungen der zentralen öffentlichen Verwaltung (national durch die Mitgliedstaaten definiert).

Vom Anwendungsbereich ausgenommene Bereiche

Einrichtungen der öffentlichen Verwaltung, deren Tätigkeiten überwiegend in den Bereichen **nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung** (Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten) ausgeübt werden, sind vom Anwendungsbereich der Richtlinie ausgenommen. Diplomatische und konsularische Vertretungen der Mitgliedstaaten in Drittländern sowie Vertrauensdienste, die ausschließlich innerhalb geschlossener Systeme verwendet werden, sind ebenfalls ausgenommen.

5. Wesentliche Definitionen

Einige grundlegende Konzepte müssen für eine korrekte Auslegung der Richtlinie klar verstanden werden.

Begriff	Definition
Netz- und Informationssystem	Elektronische Kommunikationsnetze, alle Geräte oder Gerätegruppen, die digitale Daten verarbeiten, sowie alle digitalen Daten, die für Betrieb, Nutzung, Schutz und Wartung verarbeitet werden.
Cybersicherheit	Alle Maßnahmen, die zum Schutz von Netz- und Informationssystemen, ihrer Nutzer und anderer Personen vor Cyberbedrohungen erforderlich sind.
Sicherheitsvorfall	Ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der durch Netz- und Informationssysteme angebotenen oder darüber zugänglichen Dienste beeinträchtigt.
Erheblicher Sicherheitsvorfall	Ein Sicherheitsvorfall, der schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.
Cyberbedrohung	Jeder potenzielle Umstand, jedes potenzielle Ereignis oder jede potenzielle Aktion, die Netz- und Informationssysteme beschädigen, stören oder sonstige nachteilige Auswirkungen auf diese haben könnte.
Erhebliche Cyberbedrohung	Eine Cyberbedrohung, bei der aufgrund ihrer technischen Merkmale davon ausgegangen werden kann, dass sie das Potenzial hat, auf die Netz- und Informationssysteme einer Einrichtung, ihre Nutzer oder andere Personen erhebliche Auswirkungen durch erhebliche materielle oder immaterielle Schäden zu haben.
Schwachstelle	Eine Schwäche, Anfälligkeit oder ein Fehler von IKT-Produkten oder -Diensten, der von einer Cyberbedrohung ausgenutzt werden kann.
Beinahe-Vorfall	Ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die durch Netz- und Informationssysteme angeboten oder über diese zugänglich sind, hätte beeinträchtigen können, das jedoch erfolgreich verhindert wurde.
CSIRT	Computer Security Incident Response Team, das technische Team, das für die Bearbeitung von Sicherheitsvorfällen zuständig ist.
ENISA	Agentur der Europäischen Union für Cybersicherheit; übernimmt eine zentrale Beratungs- und Unterstützungsfunktion bei der Umsetzung der Richtlinie.

6. Einrichtungskategorien: Wesentliche und wichtige Einrichtungen

Die Richtlinie unterteilt alle in den Anwendungsbereich fallenden Einrichtungen in zwei Hauptkategorien. Diese Unterscheidung bestimmt, wie die Pflichten und die Aufsichts-/Durchsetzungsregelung angewendet werden.

Kriterium	Wesentliche Einrichtungen	Wichtige Einrichtungen
Sektor	Anhang I, Sektoren mit hoher Kritikalität	Anhang II, sonstige kritische Sektoren (und mittlere Unternehmen aus Anhang I)
Größe	Große Unternehmen (250 oder mehr Beschäftigte oder Umsatz ab 50 Mio. EUR)	Mittlere Unternehmen (50 bis 249 Beschäftigte)
Aufsichtsregelung	Sowohl Ex-ante- als auch Ex-post-Aufsicht	Nur Ex-post bei Hinweisen oder Beschwerden
Höchste Verwaltungsgeldbuße	EUR 10 Millionen oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist)	EUR 7 Millionen oder 1,4 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist)
Sanktionen gegen die Geschäftsführung	Vorübergehendes Tätigkeitsverbot kann verhängt werden	Vorübergehendes Tätigkeitsverbot gilt nicht

Wichtiger Hinweis: Wurde eine Einrichtung nach NIS1 als "Betreiber wesentlicher Dienste" eingestuft, kann der Mitgliedstaat beschließen, dass diese Einrichtung unmittelbar eine wesentliche Einrichtung nach NIS2 ist. Darüber hinaus gelten alle Einrichtungen, die nach der Richtlinie 2022/2557 (CER) als "kritische Einrichtungen" eingestuft wurden, automatisch als wesentliche Einrichtungen im Sinne von NIS2.

7. Erfasste Sektoren (Anhang I und Anhang II)

Anhang I, Sektoren mit hoher Kritikalität

Große Unternehmen in diesen Sektoren sind wesentliche Einrichtungen; mittlere Unternehmen sind wichtige Einrichtungen.

Sektor	Teilsektor / Einrichtungstyp
Energie	Strom (Erzeugung, Übertragung, Verteilung, Lieferung); Fernwärme/-kälte; Öl (Pipeline, Erzeugung, Speicherung, Übertragung); Erdgas; Produktion, Speicherung und Übertragung von Wasserstoff
Verkehr	Luftfahrt (Fluggesellschaften, Flughäfen, Flugverkehrskontrolle); Schiene (Infrastrukturbetreiber, Eisenbahnunternehmen); Wasser (See-/Binnenschifffahrtsbetreiber); Straße (intelligente Verkehrssysteme, Straßenbetreiber)
Bankwesen	Kreditinstitute gemäß Verordnung (EU) Nr. 575/2013
Finanzmarktinfrastrukturen	Handelsplätze (Börsen) und zentrale Gegenparteien (CCP)
Gesundheit	Anbieter von Gesundheitsversorgung; EU-Referenzlaboratorien; Einrichtungen, die Forschung und Entwicklung von Arzneimitteln betreiben; Pharmahersteller; Hersteller von Medizinprodukten, die im Rahmen öffentlicher Gesundheitsnotfälle als kritisch eingestuft werden (gemäß Verordnung (EU) 2022/123)
Trinkwasser	Lieferanten und Verteiler von Wasser für den menschlichen Gebrauch
Abwasser	Einrichtungen, die städtisches Abwasser, häusliches Abwasser oder industrielles Abwasser sammeln, entsorgen oder behandeln
Digitale Infrastruktur	Internetknoten (IXP); DNS-Diensteanbieter (außer Root-DNS); TLD-Namenregister; Cloud-Computing-Dienstleister; Anbieter von Rechenzentrumsdiensten; Anbieter von Inhaltszustellnetzen (CDN); Vertrauensdiensteanbieter; Anbieter öffentlicher elektronischer Kommunikationsnetze/-dienste
IKT-Dienstverwaltung (B2B)	Anbieter verwalteter Dienste (MSP); Anbieter verwalteter Sicherheitsdienste (MSSP)
Öffentliche Verwaltung	Einrichtungen der zentralen und regionalen Verwaltung gemäß nationaler Definition der Mitgliedstaaten
Raumfahrt	Betreiber bodengestützter Infrastrukturen, die von einem Mitgliedstaat oder dem Privatsektor betrieben werden

Anhang II, Sonstige kritische Sektoren

Sektor	Teilsektor / Einrichtungstyp
Post- und Kurierdienste	Postdienstleister (einschließlich Kurierdienste)
Abfallbewirtschaftung	Einrichtungen, die Abfallsammlungs-, Recycling- und Entsorgungsdienstleistungen erbringen
Chemikalien	Einrichtungen, die an der Herstellung, Verarbeitung und dem Vertrieb von Chemikalien beteiligt sind
Lebensmittel	Große Unternehmen, die Lebensmittel erzeugen, verarbeiten und im Großhandel vertreiben
Verarbeitendes Gewerbe	Medizinprodukte/In-vitro-Diagnostika; Computer-, elektronische und optische Erzeugnisse; Elektrische Ausrüstungen; Sonstige Maschinen und Anlagen; Kraftwagen und Kraftwagenteile; Sonstiger Fahrzeugbau
Digitale Dienste	Online-Marktplätze; Online-Suchmaschinen; Plattformen für Dienste sozialer Netzwerke
Forschung	Forschungsorganisationen, die Forschung mit kommerziellem Ziel betreiben

8. Pflichten der Mitgliedstaaten

Die Richtlinie legt sowohl den Mitgliedstaaten als auch privatwirtschaftlichen Einrichtungen Pflichten auf. Jeder Mitgliedstaat muss folgende Schritte unternehmen:

Nationale Cybersicherheitsstrategie. Annahme einer nationalen Cybersicherheitsstrategie mit klaren strategischen Zielen, Prioritäten und einem Governance-Rahmen. Die Strategie behandelt Themen wie Lieferkettensicherheit, Ransomware, KMU-Unterstützung, Open Source und aktive Cyberabwehr.

Zuständige Behörde(n). Benennung oder Einrichtung einer oder mehrerer zuständiger Behörden zur Gewährleistung der Umsetzung und Aufsicht der Richtlinie.

Zentrale Anlaufstelle (SPOC). Benennung einer zentralen Anlaufstelle, die für die grenzüberschreitende Koordinierung auf EU-Ebene zuständig ist.

CSIRT. Einrichtung oder Benennung eines oder mehrerer CSIRTs, die für die Bearbeitung von Sicherheitsvorfällen, proaktives Monitoring, koordinierte Offenlegung von Schwachstellen sowie nationale und internationale Zusammenarbeit zuständig sind.

Einrichtungsliste. Pflege, regelmäßige Aktualisierung und Übermittlung einer Liste wesentlicher und wichtiger Einrichtungen sowie Einrichtungen, die Domänennamen-Registrierungsdienste anbieten, an die Kommission.

Koordinierte Offenlegung von Schwachstellen. Benennung eines CSIRT als Koordinator; Förderung der Rechtssicherheit für Schwachstellenforscher.

Gegenseitige Unterstützung. Gegenseitige Unterstützung anderer Mitgliedstaaten bei der grenzüberschreitenden Aufsicht und Durchsetzung.

KMU-Unterstützung. Bereitstellung von Leitlinien, kostenlosen Tools und einer nationalen/regionalen Anlaufstelle für kleine und Kleinstunternehmen.

9. Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Artikel 21)

Die wichtigste technische Bestimmung der Richtlinie ist Artikel 21. Er listet die technischen, operativen und organisatorischen Mindestmaßnahmen auf, die wesentliche und wichtige Einrichtungen umsetzen müssen. Der Ansatz beruht auf einem **gefahrenübergreifenden Ansatz**; nicht nur Cyberangriffe, sondern auch Bedrohungen wie physische Schäden, Naturkatastrophen, Geräteausfälle und menschliche Fehler sind abgedeckt.

Artikel 21, Zehn Mindestmaßnahmen

Nr.	Maßnahme	Beschreibung
1	Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme	Analyse aller Risiken und schriftliche Erstellung allgemeiner Informationssicherheitskonzepte.
2	Bewältigung von Sicherheitsvorfällen	Prozesse zur Prävention, Erkennung, Reaktion und Wiederherstellung bei Sicherheitsvorfällen.
3	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	Backup-Management, Notfallwiederherstellung und Krisenmanagement.
4	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	Einbeziehung der Sicherheitspraktiken von Lieferanten; Cybersicherheitsklauseln in Verträgen mit unmittelbaren Anbietern.
5	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen	Sicherheit über den gesamten Lebenszyklus, einschließlich Schwachstellenmanagement und -offenlegung.
6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	Regelmäßige Bewertung der Wirksamkeit der Risikomanagementmaßnahmen.
7	Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	Maßnahmen zur Cyberhygiene und Sensibilisierungsschulungen für Mitarbeiter.
8	Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung	Konzepte für den Einsatz von Verschlüsselung; Ende-zu-Ende-Verschlüsselung, wo angemessen.

10. Meldepflichten bei Sicherheitsvorfällen (Artikel 23)

Die wichtigste operative Neuerung der Richtlinie ist die mehrstufige Melderegelung für Sicherheitsvorfälle. Wesentliche und wichtige Einrichtungen müssen **erhebliche Sicherheitsvorfälle** -- definiert als solche, die schwerwiegende Betriebsstörungen, finanzielle Verluste oder erhebliche Auswirkungen auf andere Personen verursachen -- dem CSIRT oder der zuständigen Behörde innerhalb folgender Fristen melden.

Stufe	Frist	Inhalt
Frühwarnung	Unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls	Angabe, ob der Verdacht besteht, dass der Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist; mögliche grenzüberschreitende Auswirkungen; grundlegende Informationen, die dem CSIRT die Kenntnisnahme ermöglichen.
Meldung über den Sicherheitsvorfall	Unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des Sicherheitsvorfalls	Aktualisierung der Frühwarnung; Schweregrad, Auswirkungen und gegebenenfalls Kompromittierungsindikatoren (IoCs).
Zwischen-/Abschlussbericht	Spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls	Ausführliche Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen; Art der ausgenutzten Bedrohung; ergriffene und geplante Abhilfemaßnahmen; gegebenenfalls grenzüberschreitende Auswirkungen.
Fortschrittsbericht	Wenn der Sicherheitsvorfall zum Zeitpunkt der Fälligkeit des Abschlussberichts noch andauert	Fortschrittsbericht über den aktuellen Stand des Sicherheitsvorfalls; Abschlussbericht einen Monat nach Abschluss der Bearbeitung des Sicherheitsvorfalls.

Benachrichtigung der Dienstempfänger: Wenn eine erhebliche Cyberbedrohung wahrscheinlich eintreten wird, müssen Einrichtungen ihre Dienstempfänger unverzüglich und unentgeltlich über mögliche Abhilfemaßnahmen und gegebenenfalls über die Bedrohung selbst in klarer und verständlicher Sprache informieren.

Beinahe-Vorfälle und freiwillige Meldungen

Zusätzlich zu Sicherheitsvorfällen **können Einrichtungen Beinahe-Vorfälle und erhebliche Cyberbedrohungen freiwillig** dem CSIRT oder der zuständigen Behörde melden. Auch

11. Sicherheit der Lieferkette

Die meisten großen Cyberangriffe der letzten Jahre erreichten ihre Zielorganisationen über Lieferanten und Softwareanbieter und nicht durch direkte Angriffe auf die Organisation selbst. Die Richtlinie stellt daher das Lieferkettenrisiko in den Mittelpunkt der Risikomanagementpflichten.

- Einrichtungen müssen die **Qualität, Sicherheitspraktiken und sicheren Entwicklungsprozesse** der Produkte und Dienste ihrer Lieferanten und Diensteanbieter bewerten.
- **Cybersicherheitsanforderungen müssen in Verträge** mit unmittelbaren Anbietern aufgenommen werden.
- Bei der Auswahl von **Anbietern verwalteter Sicherheitsdienste (MSSP)** ist besondere Sorgfalt geboten; diese Anbieter sind attraktive Angriffsziele.
- Die Kooperationsgruppe führt gemeinsam mit der Kommission und ENISA **koordinierte Sicherheitsrisikobewertungen** für kritische Lieferketten durch (wie es für 5G-Netze erfolgt ist).
- **Nichttechnische Risikofaktoren** liegen ebenfalls im Bewertungsbereich, einschließlich des potenziellen übermäßigen Einflusses von Drittländern auf Lieferanten, versteckter Schwachstellen/Backdoors und Anbieterabhängigkeiten.

12. Verantwortung des Leitungsorgans

Die Richtlinie stellt sicher, dass Cybersicherheit nicht länger ein Thema ist, das auf technische Abteilungen beschränkt ist, sondern in den **direkten Verantwortungsbereich der Geschäftsführung** übergeht. Gemäß Artikel 20 sind die Leitungsorgane wesentlicher und wichtiger Einrichtungen:

- Verantwortlich für die **Genehmigung der Risikomanagementmaßnahmen** nach Artikel 21 und die Überwachung ihrer Umsetzung;
- Können für Verstöße gegen diese Pflichten **persönlich haftbar gemacht werden**;
- Müssen regelmäßig Cybersicherheitsschulungen absolvieren, um ausreichende Kenntnisse und Fähigkeiten zu erlangen;
- Sollten ähnliche Schulungen für ihre Mitarbeiter fördern.

> **Wichtig:** Bei wesentlichen Einrichtungen kann die zuständige Behörde beantragen, dass **vorübergehende Tätigkeitsverbote** gegen die Geschäftsführung (Personen auf Geschäftsführer- oder gesetzlicher Vertreterebene) verhängt werden. Dies ist eine Maßnahme des letzten Mittels, die erst angewendet werden kann, wenn alle anderen Durchsetzungsmöglichkeiten ausgeschöpft wurden.

13. Kooperationsstrukturen auf EU-Ebene

Die Richtlinie regelt oder stärkt verschiedene Strukturen, die eine wirksame Zusammenarbeit zwischen den Mitgliedstaaten gewährleisten:

Struktur	Funktion
Kooperationsgruppe	Unterstützt die Zusammenarbeit auf strategischer Ebene; erstellt zweijährige Arbeitsprogramme; veröffentlicht Leitlinien; führt koordinierte Risikobewertungen für kritische Lieferketten durch.
CSIRT-Netzwerk	Zusammenarbeit auf operativer Ebene; Austausch von Informationen zu Sicherheitsvorfällen; gegenseitige Unterstützung; gemeinsame Reaktion.
EU-CyCLONe	Europäisches Cyber-Krisenverbindungsorganisationsnetzwerk; Brücke zwischen technischer und politischer Ebene bei großangelegten Sicherheitsvorfällen und Krisen; erstellt Folgenanalysen.
ENISA	Einrichtung und Pflege der europäischen Schwachstellendatenbank; technische Unterstützung; Entwicklung von Leitlinien; Überwachung der Cyberhygienepolitik der Mitgliedstaaten.
IPCR-Regelungen	EU-Regelungen für eine integrierte politische Krisenreaktion (Durchführungsbeschluss des Rates 2018/1993), Krisenmanagement auf Unionsebene für großangelegte Krisen.
EU-CSIRTs-CVD-Koordinator	Ein CSIRT in jedem Mitgliedstaat wird als Koordinator für die grenzüberschreitende koordinierte Offenlegung von Schwachstellen benannt.

Zusammenarbeit mit Drittländern: Die EU kann gemäß Artikel 218 AEUV internationale Übereinkünfte mit Drittländern oder internationalen Organisationen schließen. Solche Übereinkünfte können unter Wahrung der Interessen der Union und des Datenschutzes diesen Parteien die Beteiligung an Tätigkeiten der Kooperationsgruppe, des CSIRT-Netzwerks oder EU-CyCLONe ermöglichen.

14. Aufsicht und Durchsetzung

Die Richtlinie sieht für die beiden Einrichtungskategorien unterschiedliche Aufsichtsregelungen vor. **Wesentliche Einrichtungen** unterliegen sowohl der Ex-ante- als auch der Ex-post-Aufsicht, während **wichtige Einrichtungen** nur ex-post, bei Hinweisen oder Beschwerden, beaufsichtigt werden.

Aufsichtsbefugnisse der zuständigen Behörden

- Durchführung von Vor-Ort-Inspektionen und Fernaufsicht;
- Anforderung gezielter Sicherheitsprüfungen (wobei die Kosten möglicherweise von der Einrichtung getragen werden);
- Anordnung von Sicherheitsscans;
- Anforderung von Nachweisen über die Einhaltung der Risikomanagementmaßnahmen;
- Anforderung von Informationen über mutmaßliche Verstöße gegen die Richtlinie;
- Anforderung von Informationen, die den Zugang zu personenbezogenen Daten und Verkehrsdaten erfordern, soweit erforderlich.

Anwendbare Durchsetzungsmaßnahmen

- Erteilung von Warnungen und verbindlichen Anweisungen;
- Anordnung bestimmter Maßnahmen oder Behebung von Schwachstellen innerhalb einer bestimmten Frist;
- Anordnung einer unabhängigen Prüfung zur Überprüfung der Risikomanagementmaßnahmen;
- Anordnung an Einrichtungen, Dienstempfänger über die Art des Verstoßes zu informieren;
- Abgabe öffentlicher Erklärungen (mit Offenlegung des Namens der Einrichtung und der Art des Verstoßes);
- Bei wesentlichen Einrichtungen (als letztes Mittel): vorübergehende Aussetzung von Zertifizierungen oder Genehmigungen und vorübergehende Tätigkeitsverbote gegen die Geschäftsführung;
- Verhängung oder Beantragung der Verhängung von Verwaltungsgeldbußen.

15. Verwaltungsgeldbußen

Die Richtlinie legt **EU-weit harmonisierte Höchstschwellen** für Verwaltungsgeldbußen fest, die von den Mitgliedstaaten verhängt werden. Diese Schwellen sind -- ähnlich wie bei der DSGVO -- am weltweiten Umsatz der Einrichtung ausgerichtet.

Einrichtungstyp	Höchstbetrag (es gilt jeweils der höhere Betrag)
Wesentliche Einrichtungen	EUR 10.000.000 oder 2 % des weltweiten Jahresumsatzes
Wichtige Einrichtungen	EUR 7.000.000 oder 1,4 % des weltweiten Jahresumsatzes

Faktoren bei der Bemessung von Geldbußen

- Art, Schwere und Dauer des Verstoßes;
- Verursachte materielle oder immaterielle Schäden;
- Ob der Verstoß vorsätzlich oder fahrlässig begangen wurde;
- Ergriffene Maßnahmen zur Verhütung oder Schadensbegrenzung;
- Grad der Verantwortung und frühere Verstöße;
- Grad der Zusammenarbeit mit der zuständigen Behörde;
- Sonstige erschwerenden oder mildernden Umstände.

Geldbußen müssen **verhältnismäßig** sein, und Grundrechte wie das Recht auf Verteidigung, die Unschuldsvermutung und das Recht auf wirksamen Rechtsschutz müssen bei ihrer Anwendung gewahrt werden. Die Mitgliedstaaten können auch strafrechtliche Sanktionen für Verstöße gegen nationales Recht vorsehen; jedoch darf keine Person für dieselbe Handlung zweimal bestraft werden, was den **"ne bis in idem"**-Grundsatz verletzt.

16. Umsetzungszeitplan und Übergangsbestimmungen

Datum	Ereignis
14. Dezember 2022	Annahme der Richtlinie durch das Europäische Parlament und den Rat
27. Dezember 2022	Veröffentlichung im Amtsblatt der EU (ABl. L 333/80)
16. Januar 2023	Inkrafttreten der Richtlinie (20 Tage nach Veröffentlichung)
17. Oktober 2024	Frist für die Mitgliedstaaten zur Umsetzung der Richtlinie in nationales Recht
18. Oktober 2024	Beginn der Anwendung der Richtlinie
18. Oktober 2024	Aufhebung der Richtlinie (EU) 2016/1148 (NIS1)
17. April 2025	Frist für die Mitgliedstaaten zur Übermittlung der Liste wesentlicher und wichtiger Einrichtungen an die Kommission
Ab 17. Oktober 2027	Regelmäßige Überprüfung der Umsetzung der Richtlinie durch die Kommission (alle 36 Monate)

Wichtig: NIS2 ist eine Richtlinie; sie gilt nicht unmittelbar. Jeder Mitgliedstaat muss die Richtlinie in sein nationales Recht umsetzen. Die für eine Einrichtung geltenden konkreten Pflichten und Sanktionen hängen daher vom nationalen Umsetzungsgesetz des Mitgliedstaats ab, in dem sie tätig ist.

17. Auswirkungen auf Unternehmen außerhalb der EU

Obwohl NIS2 eine EU-Richtlinie ist, hat sie erhebliche Auswirkungen auf Unternehmen außerhalb der EU, insbesondere auf solche, die den EU-Markt bedienen oder in der EU ansässige kritische Einrichtungen beliefern:

Unmittelbar betroffene Unternehmen außerhalb der EU

- Nicht-EU-**DNS-Anbieter, Cloud-Dienstleister, Rechenzentrumsbetreiber, CDN-Anbieter, Anbieter verwalteter Dienste und verwalteter Sicherheitsdienste, Online-Marktplätze, Suchmaschinen und soziale Netzwerkplattformen**, die in der EU Dienste anbieten, müssen einen EU-Vertreter benennen und die Pflichten der Richtlinie einhalten;
- Nicht-EU-Unternehmen mit EU-Tochtergesellschaften oder -Niederlassungen können über diese Einheiten der Richtlinie unterliegen;
- Nicht-EU-Lieferanten, die Produkte oder Dienstleistungen an wesentliche oder wichtige Einrichtungen der EU liefern, unterliegen den **vertraglichen Anforderungen an die Lieferkettensicherheit**, die ihre Kunden auferlegen (Artikel 21(2)(d));
- Nicht-EU-MSPs/MSSPs, die EU-Digitalinfrastruktur oder Finanzeinrichtungen betreuen, können unmittelbar in den Anwendungsbereich fallen.

Mittelbare Auswirkungen

- Lieferketten-Risikobewertungen durch EU-Kunden zwingen Nicht-EU-Lieferanten, ihre Cybersicherheitsstandards anzuheben;
- Von der Richtlinie eingeführte Standards (ISO/IEC 27001, ENISA-Leitlinien usw.) werden zu **faktischen Referenzpunkten** auf dem globalen Markt;
- Nicht-EU-Rechtsordnungen nutzen NIS2 zunehmend als Referenz bei der Entwicklung eigener Cybersicherheitsgesetze.

18. Praktischer Compliance-Fahrplan (10 Schritte)

Der folgende 10-Schritte-Fahrplan dient als praktischer Leitfaden sowohl für Unternehmen, die innerhalb der EU tätig sind, als auch für solche, die sich freiwillig an den NIS2-Standards ausrichten möchten.

Schritt	Aktivität
1. Feststellung des Anwendungsbereichs	Prüfen, ob das Unternehmen in Sektoren des Anhangs I oder Anhangs II tätig ist, ob es die Größenkriterien erfüllt, und Identifizierung der Kategorie (wesentlich/wichtig).
2. Gap-Analyse	Bewertung des bestehenden Informationssicherheitsmanagementsystems anhand der 10 Maßnahmenkategorien des Artikels 21; Lücken kartieren.
3. Governance-Struktur	Zuständigkeiten, Berichtslinien und Genehmigungsverfahren auf Vorstands-/Geschäftsführungsebene festlegen; regelmäßiges Schulungsprogramm einrichten.
4. Richtlinien und Dokumentation	Informationssicherheitsrichtlinie, Risikomanagementrichtlinie, Incident-Response-Richtlinie, Nutzungsrichtlinie und weitere Dokumente erstellen oder aktualisieren.
5. Risikobewertung	Anlagenbestandsaufnahme, Bedrohungsanalyse und Risikobewertung mit gefahrenübergreifendem Ansatz durchführen; Risikoakzeptanzkriterien festlegen.
6. Umsetzung technischer Kontrollen	MFA, Verschlüsselung, Netzwerksegmentierung, Zero-Trust-Architektur, Log-Management, SIEM, EDR/XDR, Backup und Disaster-Recovery-Lösungen implementieren.
7. Incident-Response-Fähigkeit	Incident-Response-Plan dokumentieren; Rollen und Zuständigkeiten zuweisen; 24-Stunden-Frühwarn-Kommunikationsablauf einrichten; Tischübungen durchführen.
8. Lieferkettenmanagement	Lieferanten inventarisieren; nach Risikoniveau klassifizieren; Cybersicherheitsklauseln in Vertragsvorlagen aufnehmen; regelmäßige Audits durchführen.
9. Schulung und Sensibilisierung	Jährliche Cyberhygieneschulungen für alle Mitarbeiter durchführen; Fachschulungen für das Leitungsorgan anbieten; Phishing-Simulationen durchführen.
10. Kontinuierliche Verbesserung	Interne und externe Audits durchführen; KPIs verfolgen; aus jedem Sicherheitsvorfall lernen; Risikobewertung jährlich aktualisieren; Zertifizierung anstreben (ISO/IEC 27001, EU-Cybersicherheitszertifizierung).

19. Fazit und Bewertung

Die NIS2-Richtlinie hebt das Cybersicherheits-Grundniveau der Europäischen Union erheblich an. Sie stellt nicht nur technische Anforderungen, sondern macht Cybersicherheit auch zu einem **integralen Bestandteil der Governance-Struktur und des Geschäftsbetriebs von Unternehmen**.

Stärken der Richtlinie

- **Breite Reichweite**: ca. 18 Sektoren und über 100.000 Einrichtungen in der EU-27 im Anwendungsbereich;
- **Harmonisierung**: Einheitliche Ausgangsbedingungen im Binnenmarkt durch einheitliche Kriterien und Durchsetzungsregelung in der gesamten EU;
- **Governance-Fokus**: Durch die Verantwortlichkeit der Geschäftsführung wird sichergestellt, dass Cybersicherheit alle Unternehmensebenen durchdringt;
- **Lieferkettenbetonung**: Reagiert auf die Realität, dass die Mehrzahl moderner Angriffe über die Lieferkette erfolgt;
- **Kooperationsstrukturen**: Mehrschichtige EU-Koordination durch Kooperationsgruppe, CSIRT-Netzwerk und EU-CyCLONe.

Kritikpunkte und Herausforderungen

- Verzögerungen und Abweichungen bei der Umsetzung durch die Mitgliedstaaten; in der Praxis ist eine einheitliche Umsetzung in der EU-27 lückenhaft;
- Insbesondere für mittlere Unternehmen stellen Compliance-Kosten und die Schließung technischer Kompetenzlücken eine ernsthafte Herausforderung dar;
- Die Umsetzung der 24-Stunden-Frühwarnfrist vor Erreichen ausreichender Reife kann zu oberflächlichen oder fehlerhaften Meldeprozessen führen;
- Überschneidungsbereiche mit sektoralen Regelungen (DORA, Finanzwesen; eIDAS, Vertrauensdienste; sektorale Luftfahrtregelungen usw.) können für Einrichtungen zu Komplexität führen.

Gesamtbewertung

NIS2 rahmt Cybersicherheit neu -- von einem technischen Anliegen zu einer Frage der **Betriebskontinuität, der Corporate Governance und des Kundenvertrauens.** Für Einrichtungen, die in der EU tätig sind oder mit ihr interagieren, ist die Einhaltung sowohl eine rechtliche Verpflichtung als auch ein Mittel zur Stärkung der operationellen Resilienz.

Für Unternehmen außerhalb der EU etabliert NIS2 einen neuen **faktischen Standard** für den Zugang zum EU-Markt und erhöht die Cybersicherheitserwartungen weltweit. Eine frühzeitige Compliance erleichtert die Erfüllung vertraglicher Verpflichtungen und verbessert die allgemeine Cyberresilienz.

> **Abschließender Hinweis:** Dieses Dokument fasst die wesentlichen Bestimmungen der Richtlinie für deutschsprachige Leser zusammen. Für die für Ihre Organisation spezifischen Compliance-Anforderungen sollten Sie den offiziellen Text (ABl. L 333/80, 27.12.2022), das nationale Umsetzungsgesetz Ihres Mitgliedstaats und sektorspezifische Regelungen prüfen sowie rechtliche und Cybersicherheitsberatung in Anspruch nehmen.

Quellen

- Richtlinie (EU) 2022/2555, EUR-Lex-CELEX-Nummer 32022L2555
- Amtsblatt der EU L 333/80, 27. Dezember 2022
- ENISA, Agentur der Europäischen Union für Cybersicherheit (www.enisa.europa.eu)
- Portal der Europäischen Kommission für die digitale Strategie (digital-strategy.ec.europa.eu)

Mehr zu NIS2 von Rediacc

Diese Zusammenfassung bildet die Struktur und die Pflichten der Richtlinie ab. Die Begleitleitfäden auf rediacc.com übersetzen diese Pflichten in konkrete operative und beschaffungsbezogene Entscheidungen.

Drei Begleitleitfäden

- **Artikel 21(2)(d) und Self-Hosting.** Warum das Drittanbieter-IKT-Register kleiner wird, wenn die Datenebene Ihre Tenancy nie verlässt. Für CISOs und Beschaffungsverantwortliche, die DPAs im Jahr 2026 neu verhandeln.
- **Kontinuierliche Wirksamkeit ohne Theater.** Artikel 21(2)(e), (f) und 23 zusammen gelesen. Der Fork mit konstanter Zeitkomplexität, der wöchentliche Übungen realistisch macht, und der Meldeplan nach Artikel 23, den Sie ohne forensisch-taugliche Artefakte nicht einhalten können. Für SRE- und Ops-Verantwortliche.
- **Die strukturellen Kosten der NIS2-Compliance.** Der Fünf-Tools-Stack, den mittelgroße wesentliche Einrichtungen im Stillen zusammenstellen, was eine selbst gehostete Control Plane konsolidiert, und die Kostenpositionen, die in jedem Fall bei Ihnen bleiben. Für CFOs und Einkäufer vor einem Vertragsverlängerungszyklus.

Wo Sie diese finden

Alle drei Leitfäden sowie diese Zusammenfassung als herunterladbares PDF finden Sie unter:

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ ist eine estnisch eingetragene selbst gehostete Infrastrukturplattform (Registernummer 17363830, USt-IdNr. EE102920091). Das Produkt ist kein Ersatz für ein Sicherheitsprogramm; es ist eine Tooling-Schicht, die das Datenebenen-Anbieterrisiko beseitigt, das herkömmliche Backup-, DR- und Testdaten-Tools nicht beseitigen können. Kostenloser Community-Tarif und kostenpflichtige Tarife ab 349 $/Monat.

> Dieses Dokument und seine Begleitleitfäden sind Bildungsmaterial. Compliance-Entscheidungen, die spezifisch für Ihre Organisation sind, erfordern rechtliche Beratung und den Verweis auf das nationale Umsetzungsgesetz in Ihrer Rechtsordnung.