mondoo

VERSTÄNDNIS UND AUSWIRKUNGEN

# DIE NIS2-CYBERSICHER-HEITSRICHTLINIE DER EU

# EINLEITUNG

In einer zunehmend vernetzten und digitalen Welt ist der Schutz kritischer Infrastrukturen und wesentlicher Dienste vor Cyberbedrohungen zu einem zentralen Anliegen für Regierungen, Unternehmen und Einzelpersonen geworden. In Anerkennung der dringenden Notwendigkeit, die Cybersicherheitsfähigkeiten in der gesamten Europäischen Union (EU) zu stärken, hat die Europäische Kommission die NIS2-Cybersicherheitsrichtlinie eingeführt.

Die NIS2-Richtlinie, die Richtlinie über die Sicherheit von Netz- und Informationssystemen, stellt einen umfassenden und zukunftsorientierten Rahmen dar, der die Widerstandsfähigkeit der EU gegenüber Cybervorfällen stärken soll. Aufbauend auf den Erfolgen und Erkenntnissen der ursprünglichen, 2016 verabschiedeten NIS-Richtlinie zielt NIS2 darauf ab, neue Herausforderungen im Bereich der Cybersicherheit zu bewältigen, sich an technologische Entwicklungen anzupassen und eine engere Zusammenarbeit zwischen öffentlichen und privaten Einrichtungen zu fördern.

Das Hauptziel der NIS2-Cybersicherheitsrichtlinie besteht darin, eine harmonisierte und robuste Cybersicherheits-Governance in allen EU-Mitgliedstaaten zu etablieren und so den Schutz kritischer Infrastruktursektoren und digitaler Diensteanbieter sicherzustellen. Sie soll ein hohes Maß an Cybersicherheitsbereitschaft und Reaktionsfähigkeit bei Vorfällen fördern und damit die Verfügbarkeit, Integrität und Vertraulichkeit wichtiger Netze und Systeme schützen.

## Kurz gesagt verschärft die NIS2-Richtlinie die Sicherheitsanforderungen in der EU durch:

- Ausweitung ihres Anwendungsbereichs auf mehr Sektoren und Einrichtungen
- Einführung des Konzepts der „Leitungsorgane“ (Verantwortung auf Unternehmensebene)
- Straffung und Standardisierung der Meldepflichten
- Einführung von Kontroll- und Überwachungsmaßnahmen
- Harmonisierung und Verschärfung der Sanktionen in allen Mitgliedstaaten

Die NIS2-Richtlinie wurde am 27.12.2022 im Amtsblatt L333 der Europäischen Union veröffentlicht und trat am 16.01.2023 in Kraft. In Deutschland wurde die Richtlinie durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt, das am 6. Dezember 2025 in Kraft getreten ist (die EU-Frist zur Umsetzung in nationales Recht war der 17. Oktober 2024). Eine Übergangsfrist für die Umsetzung der Maßnahmen sieht das Gesetz nicht vor; die Pflichten gelten seit dem Inkrafttreten unmittelbar. Betroffene Einrichtungen mussten sich zudem innerhalb von drei Monaten nach Inkrafttreten beim BSI registrieren. Diese Frist ist am 6. März 2026 abgelaufen; bis dahin hatten sich jedoch nur rund 39 % der geschätzt 29 500 betroffenen Unternehmen registriert. Wer noch nicht registriert ist, sollte umgehend handeln, da bereits die Registrierungspflicht selbst bußgeldbewehrt ist.

*NIS2-Richtlinie: https://eur-lex.europa.eu/eli/dir/2022/2555/oj*

# IST MEIN UNTERNEHMEN VON NIS2 BETROFFEN?

Die NIS2-Richtlinie unterscheidet zwischen wesentlichen und wichtigen Einrichtungen. Der wesentliche Unterschied zwischen beiden besteht darin, dass „wichtige Einrichtungen“ niedrigeren Bußgeldern und einer reaktiven Aufsicht durch die Behörden unterliegen, im Gegensatz zur proaktiven Aufsicht, die „wesentlichen Einrichtungen“ vorbehalten ist. In der EU wird es keine unterschiedlichen Mindestschwellen mehr geben; stattdessen wird die Anwendbarkeit anhand „einheitlicher Kriterien“ bestimmt. Mittlere und große Unternehmen sollen von der Regulierung erfasst werden:nies are to be covered by regulation:

### MITTEL

50–250 Beschäftigte

10–50 Euro Umsatz

< 43 million Euro Bilanzsumme

### GROSS

> 250 Beschäftigte

> 50 Euro Umsatz

> 43 million Euro Bilanzsumme

Dies erweitert die Zahl der Einrichtungen, die NIS2 in der EU, einschließlich Deutschlands, einhalten müssen, erheblich.

## NIS2 präzisiert und verschärft die im Gesetz vorgesehenen Bußgelder bei Nichteinhaltung:

- Maßnahmen zum Cybersicherheits-Risikomanagement (Artikel 21)
- Meldepflichten (Artikel 23)

Artikel 34 Absatz 4 der NIS2-Richtlinie sieht Bußgelder bei Nichteinhaltung dieser Pflichten vor. Diese Bußgelder variieren je nachdem, ob es sich um eine wesentliche oder eine wichtige Einrichtung handelt:

- Für wesentliche Einrichtungen: Geldbußen von bis zu mindestens 10 000 000 EUR oder von bis zu mindestens 2 % des gesamten weltweiten Jahresumsatzes.
- Für wichtige Einrichtungen: Geldbußen von bis zu mindestens 7 000 000 EUR oder von bis zu mindestens 1,4 % des gesamten weltweiten Jahresumsatzes.

Die NIS2-Richtlinie führt den Grundsatz der Verantwortung der obersten Leitungsebene für die Sicherheit ein, konkret der „Leitungsorgane“. Ziel ist es, die Geschäftsführung und den Vorstand für die Sicherheit in die Verantwortung zu nehmen. Die Aussicht auf Sanktionen ist am wirksamsten, wenn konkrete Personen als verantwortlich benannt werden. Das bedeutet, dass Cybersicherheit nicht mehr allein in der Verantwortung der IT liegt, sondern zur Angelegenheit des Vorstands und der Geschäftsführung wird, in Deutschland spricht man von „Chefsache“.

**WICHTIGER HINWEIS:**

Die Behörden teilen Ihnen nicht mit, ob diese Richtlinie für Sie gilt. Ihr Unternehmen oder Ihre Institution muss sich selbst anhand der Kriterien bewerten, einschließlich Sektorzugehörigkeit und Größenmerkmalen. Verfügt eine als „wichtig“ eingestufte Organisation über einen erheblichen Marktanteil in einem bestimmten Sektor, kann sie aufgrund ihrer Größe sogar als wesentliche Einrichtung betrachtet werden.

# PRÜFEN SIE, OB NIS2 FÜR IHR UNTERNEHMEN GILT

Sie gelten als wesentliche Einrichtung, wenn beide der folgenden Kriterien zutreffen:

## 1. IHR UNTERNEHMEN ERFÜLLT DIESE KRITERIEN:

- > **250** Beschäftigte
- > **50** Mio. Euro Umsatz
- > **43** Mio. Euro Bilanzsumme

*Trifft keines davon zu? →*

*Sehen Sie sich die wichtigen Einrichtungen.*

## 2. IHR UNTERNEHMEN IST IN EINEM DIESER SEKTOREN TÄTIG:

- ENERGIE
- VERKEHR
- BANKWESEN
- FINANZMARKTINFRASTRUKTUREN
- GESUNDHEIT
- TRINKWASSER
- ABWASSER
- DIGITALE INFRASTRUKTUR
- WELTRAUM
- ÖFFENTLICHE VERWALTUNG
- VERWALTUNG VON IKT-DIENSTEN

Sie gelten als wichtige Einrichtung, wenn beide der folgenden Kriterien zutreffen:

## 1. IHR UNTERNEHMEN ERFÜLLT DIESE KRITERIEN:

**50–250** Beschäftigte

**10–50** Mio. Euro Umsatz

**< 43** Mio. Euro Bilanzsumme

*Trifft keines davon zu? → Sehen Sie sich die wesentlichen Einrichtungen an.*

## 2. IHR UNTERNEHMEN IST IN EINEM DIESER SEKTOREN TÄTIG:

- ABFALLBEWIRTSCHAFTUNG
- FORSCHUNG
- DIGITALE DIENSTEANBIETER
- POST- UND KURIERDIENSTE
- VERARBEITENDES GEWERBE
- HERSTELLUNG/VERTRIEB VON CHEMIKALIEN
- PRODUKTION VON LEBENSMITTELN
- VERARBEITUNG/VERTRIEB VON LEBENSMITTELN

### SIE SIND IN KEINEM DER OBEN GENANNTEN SEKTOREN TÄTIG?

**DANN GILT NIS2 NICHT FÜR SIE.**

*(Detaillierte Sektorlisten weiter unten.)*

# NIS2 FÜR ZULIEFERER WICHTIGER UND WESENTLICHER EINRICHTUNGEN

Die Folgen, die die Einführung von NIS2 für Unternehmen haben kann, die lediglich als Zulieferer tätig sind, also nicht direkt der Regulierung unterliegen, lassen sich besonders deutlich am Finanzsektor erkennen. Banken und Versicherungen unterlagen seit jeher strengen Regeln, und die „bankaufsichtlichen Anforderungen an die IT“ (BAIT) sind ein integraler Bestandteil ihres Risikomanagements. Für Drittdienstleister kann dies bedeuten, dass ein Auftraggeber deren Cybersicherheit bewerten und das Ergebnis in den von Wirtschaftsprüfungsgesellschaften erstellten Jahresabschluss einbeziehen muss. Das heißt: IT-Dienstleister und andere Zulieferer müssen damit rechnen, Lieferantenaudits unterzogen zu werden, um die Robustheit ihrer Informationssicherheit zu prüfen.
De facto bedeutet dies, dass die Lieferkette dieselben Anforderungen erfüllen muss, die für regulierte Auftraggeber gelten.

# WAS IST DIE NIS2-RICHTLINIE?

Betroffene Unternehmen und Organisationen müssen in Bereichen wie Cyber-Risikomanagement, Lieferkettensicherheit, Business-Continuity-Management, Penetrationstests sowie Erkennung von, Reaktion auf und Meldung von Vorfällen an die Behörde und deren Behebung angemessene Maßnahmen ergreifen.

NIS2 ist eine hervorragende Gelegenheit für Chief Information Security Officers (CISOs), ihre Position im Unternehmen zu stärken. Nach der Richtlinie ist die oberste Leitungsebene für das Management von Cybersicherheitsrisiken verantwortlich, und Verstöße werden mit empfindlichen Strafen geahndet. Der CISO ist nicht nur Berater, sondern Wegweiser und Entscheider. Mit NIS2 wird der CISO zum unternehmensweiten Vermittler und Verfechter von Cybersicherheitsrichtlinien und Best Practices.

**Als CISO sollte sich der Aktionsplan für die NIS2-Compliance auf vier Kernbereiche konzentrieren:**


# WAS WESENTLICHE UND WICHTIGE EINRICHTUNGEN TUN MÜSSEN

Nach der Gesetzgebung (Artikel 21) müssen wesentliche und wichtige Einrichtungen mindestens die folgenden zehn Maßnahmen ergreifen:

1. Konzepte in Bezug auf die Risikoanalyse und die Sicherheit von Informationssystemen
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung des Betriebs, etwa Backup-Management und Wiederherstellung nach einem Notfall, sowie Krisenmanagement

"Geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, sowie um Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten."

(NIS2 Artikel 21)

4. Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren direkten Anbietern oder Diensteanbietern
5. Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
6. Konzepte und Verfahren (Tests und Audits) zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von Kryptografie und, soweit angemessen, Verschlüsselungn
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

# NIS2 VS ISO 27001:2022

Die Einhaltung der NIS2-Richtlinie kann ein komplexer Prozess sein, der sich über mehrere Jahre erstreckt. Um dies zu erleichtern, hat Mondoo ein Bewertungswerkzeug entwickelt, das die NIS2-Anforderungen auf die Norm ISO/IEC 27002:2022 abbildet. Da die NIS2-Anforderungen in Deutschland inzwischen durch das NIS2UmsuCG, insbesondere die Maßnahmen nach § 30 BSIG, konkretisiert sind, bieten diese Standards einen guten Ausgangspunkt, um einzuschätzen, wie weit ein Unternehmen oder eine Organisation mit ihren Cybersicherheitsmaßnahmen bereits fortgeschritten ist.

ISO 27001 bietet einen Rahmen aus Best Practices für Richtlinien, Verfahren und Kontrollen der Informationssicherheit, um das Risiko von Sicherheitsverletzungen zu minimieren. ISO 27002 konzentriert sich auf die Umsetzung von Kontrollen und Leitlinien. Beim Abgleich der NIS2-Maßnahmen mit der Norm ISO 27001:2022 stammen die meisten relevanten Kontrollen aus Anhang A, der die beste Kontrollperspektive bietet.

Anhang A der ISO/IEC 27001:2022 ist ein Abschnitt der Norm, der eine Reihe von Sicherheitskontrollen auflistet, mit denen Organisationen die Konformität mit ISO/IEC 27001 6.1.3 (Behandlung von Informationssicherheitsrisiken) und der zugehörigen „Erklärung zur Anwendbarkeit“ nachweisen können. Die Erklärung zur Anwendbarkeit (Statement of Applicability, SoA) ist ein verbindliches Dokument, das die Anhang-A-Kontrollen auflistet, die eine Organisation umsetzen sollte, um die Anforderungen der Norm zu erfüllen. Jeder, der eine ISO-27001-Zertifizierung anstrebt, muss diesen Schritt durchführen.

# NIS2 VS. ISO 27001

| NIS2 (Artikel der Gesetzgebung) | ISO27001:2022 |
|---|---|
| **Article 21.2** a) Konzepte in Bezug auf die Risikoanalyse und die Sicherheit von Informationssystemen | **5.2** Politik<br>**6.1.2** Informationssicherheitsrisikobeurteilung<br>**6.1.3** Informationssicherheitsrisikobeurteilung<br>**8.2** Informationssicherheitsrisikobeurteilung<br>**8.3** Informationssicherheitsrisikobeurteilung<br>**A.5.1** Informationssicherheitsrichtlinien<br>**A.5.12** Klassifizierung von Informationen<br>**A.5.2** Informationssicherheitsrollen und -verantwortlichkeiten<br>**A.5.7** Threat intelligence<br>**A.5.37** Dokumentierte Betriebsabläufe |
| **Article 21.2** b) Bewältigung von Sicherheitsvorfällen | **A.5.24** Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen<br>**A.5.25** Beurteilung und Entscheidung über Informationssicherheitsereignisse<br>**A.5.26** Reaktion auf Informationssicherheitsvorfälle<br>**A.5.27** Lernen aus Informationssicherheitsvorfällen<br>**A.5.28** Sammlung von Beweismaterial<br>**A.6.8** Meldung von Informationssicherheitsereignissen<br>**A.8.15** Protokollierung<br>**A.8.16** Überwachungsaktivitäten |
| **Article 21.2** c) Aufrechterhaltung des Betriebs, etwa Backup-Management und Wiederherstellung nach einem Notfall, sowie Krisenmanagement | **A.5.29** Informationssicherheit während einer Störung<br>**A.5.30** IKT-Bereitschaft für die Aufrechterhaltung des Betriebs<br>**A.5.37** Dokumentierte Betriebsabläufe<br>**A.8.13** Sicherung von Informationen<br>**A.8.14** Redundanz von informationsverarbeitenden Einrichtungen<br>**A.8.15** Protokollierung<br>**A.8.16** Überwachungsaktivitäten |
| **Article 21.2** d) Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren direkten Anbietern oder Diensteanbietern | **A.5.19** Informationssicherheit in Lieferantenbeziehungen<br>**A.5.20** Behandlung der Informationssicherheit in Lieferantenvereinbarungen<br>**A.5.21** Umgang mit der Informationssicherheit in der IKT-Lieferkette<br>**A.5.22** Überwachung, Überprüfung und Änderungsmanagement von Lieferantenleistungen<br>**A.5.23** Informationssicherheit bei der Nutzung von Cloud-Diensten |

| NIS2 (Artikel der Gesetzgebung) | ISO27001:2022 |
|---|---|
| **Article 21.2** e) Sicherheit bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen | **A.5.37** Dokumentierte Betriebsabläufe<br>**A.8.8** Handhabung technischer Schwachstellen<br>**A.8.9** Konfigurationsmanagement<br>**A.8.19** Installation von Software auf Systemen im Betrieb<br>**A.8.20** Netzwerksicherhei<br>**A.8.21** Sicherheit von Netzwerkdiensten |
| **Article 21.2** f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit | **9.1** Überwachung, Messung, Analyse und Bewertung<br>**9.2** Internes Audit<br>**9.3** Managementbewertung<br>**A.5.35** Unabhängige Überprüfung der Informationssicherheit<br>**A.5.36** Einhaltung von Richtlinien, Regeln und Standards für die Informationssicherheit |
| **Article 21.2** g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit | **7.2** Kompetenz<br>**7.3** Bewusstsein<br>**7.4** Kommunikation<br>**A.5.10** Zulässige Nutzung von Informationen und anderen damit verbundenen Werten;<br>**A.5.15** Zugangssteuerung<br>**A.5.16** Identitätsmanagement<br>**A.6.3** Bewusstsein, Ausbildung und Schulung für Informationssicherheit |
| **Article 21.2** h) Konzepte und Verfahren für den Einsatz von Kryptografie und, soweit angemessen, Verschlüsselung | **A.8.17** Uhrensynchronisation<br>**A.8.24** Nutzung von Kryptografie |
| **Article 21.2** i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen | **A.5.2** Informationssicherheitsrollen und -verant wortlichkeiten<br>**A.5.3** Aufgabentrennung<br>**A.5.9** Inventar der Informationen und anderer damit verbundener Werte<br>**A.5.10** Zulässige Nutzung von Informationen und anderen damit verbundenen Werten<br>**A.5.11** Rückgabe von Werten<br>**A.5.15** Zugangssteuerung<br>**A.5.16** Identitätsmanagement<br>**A.5.17** Authentisierungsinformationen<br><br>*(cont. on next page)* |

| NIS2 (Artikel der Gesetzgebung) | ISO27001:2022 |
|---|---|
| **Article 21.2** i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen *(cont.)* | **A.5.18** Zugangsrechte<br>**A.6.1** Screening<br>**A.6.2** Beschäftigungs- und Vertragsbedingungen<br>**A.6.3** Bewusstsein, Ausbildung und Schulung für Informationssicherheit<br>**A.6.4** Disziplinarverfahren<br>**A.6.5** Verantwortlichkeiten bei Beendigung oder Wechsel des Beschäftigungsverhältnisses<br>**A.6.6** Vertraulichkeits- oder Geheimhaltungsvereinbarungen<br>**A.6.7** Remote-Arbeit<br>**A.7.7** Aufgeräumter Arbeitsplatz und Bildschirmsperre<br>**A.7.9** Sicherheit von Werten außerhalb der Räumlichkeiten<br>**A.7.10** Speichermedien<br>**A.7.14** Sichere Entsorgung oder Wiederverwendung von Geräten<br>**A.8.1** Endgeräte der Benutzer<br>**A.8.2** Privilegierte Zugangsrechte<br>**A.8.3** Informationszugangsbeschränkung<br>**A.8.4** Zugang zum Quellcode<br>**A.8.5** Sichere Authentisierung |
| **Article 21.2** j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung | **A.5.14** Informationsübertragung<br>**A.5.16** Identitätsmanagement<br>**A.5.17** Authentisierungsinformationen<br>**A.8.5** Sichere Authentisierung |
| **Article 21.3** Die Mitgliedstaaten stellen sicher, dass die Einrichtungen die spezifischen Schwachstellen der einzelnen direkten Anbieter und Diensteanbieter sowie die allgemeine Qualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter, einschließlich ihrer sicheren Entwicklungsverfahren, und die Ergebnisse der koordinierten Sicherheitsrisikobewertungen kritischer Lieferketten nach Artikel 22(1) berücksichtigen | **A.8.25** Sicherer Entwicklungslebenszyklus<br>**A.8.26** Anforderungen an die Anwendungssicherheit<br>**A.8.27** Sichere Systemarchitektur und -entwicklung sprinzipien<br>**A.8.28** Sichere Codierung<br>**A.8.29** Sicherheitsprüfung in Entwicklung und Abnahme<br>**A.8.30** Ausgelagerte Entwicklung<br>**A.8.31** Trennung von Entwicklungs-, Test- und Produktionsumgebungen<br>**A.8.32** Änderungsmanagement<br>**A.8.33** Testinformationen |
| **Article 23** Meldepflichten | **A.5.14** Informationsübertragung<br>**A.6.8** Meldung von Informationssicherheitsereignissen |

| NIS2 (Artikel der Gesetzgebung) | ISO27001:2022 |
| --- | --- |
| **Article 24** Nutzung europäischer Schemata für die Cybersicherheitszertifizierung | **A.5.20** Behandlung der Informationssicherheit in Lieferantenvereinbarungen |

# NIS2, ERGÄNZUNGEN ZU ISO 27001

Zu den Anhang-A-Kontrollen der ISO 27001, die nicht in der Zuordnung zur NIS2-Richtlinie enthalten sind, gehören:

- **A.5.4** Verantwortlichkeiten der Leitung
- **A.5.5** Kontakt mit Behörden
- **A.5.6** Kontakt mit speziellen Interessen-gruppen
- **A.5.8** Informationssicherheit im Projekt-management
- **A.5.12** Klassifizierung von Informationen
- **A.5.13** Klassifizierung von Informationen
- **A.5.31** Rechtliche, gesetzliche, regula-torische und vertragliche Anforderungen
- **A.5.32** Geistige Eigentumsrechte
- **A.5.33** Schutz von Aufzeichnungen
- **A.5.34** Privatsphäre und Schutz personenbezogener Daten (PII)
- **A.7.1** Physische Sicherheitsperimeter
- **A.7.2** Physischer Zutritt
- **A.7.3** Sicherung von Büros, Räumen und Einrichtungen
- **A.7.4** Physische Sicherheitsüberwachung
- **A.7.5** Schutz vor physischen und umweltbedingten Bedrohungen
- **A.7.6** Arbeiten in Sicherheitsbereichen
- **A.7.8** Platzierung und Schutz von Gerätenn
- **A.7.11** Versorgungseinrichtungen
- **A.7.12** Verkabelungssicherheit
- **A.7.13** Wartung von Geräten
- **A.8.6** Kapazitätsmanagement
- **A.8.7** Schutz vor Schadsoftware
- **A.8.10** Löschung von Informationen
- **A.8.11** Datenmaskierung
- **A.8.12** Verhinderung von Datenlecks
- **A.8.17** Uhrensynchronisation
- **A.8.18** Nutzung privilegierter Hilfsprogramme
- **A.8.22** Trennung von Netzwerken
- **A.8.23** Web-Filterung
- **A.8.34** Schutz von Informationssystemen während Audit-Tests

**ZUSAMMENFASSEND LÄSST SICH SAGEN:**

Wenn ein Unternehmen ISO 27001 befolgt, befindet es sich in einer guten Ausgangs-position für NIS2. Es gibt nur einen Bereich, der zur Einhaltung von NIS2 ergänzt werden muss: die Bewältigung und Meldung von Sicherheitsvorfällen.

# MELDUNG VON VORFÄLLEN OPTIMIEREN

Die NIS2-Richtlinie schreibt strengere Pflichten zur Reaktion auf Vorfälle und kürzere Fristen vor. Zur Vorbereitung sollte der erste Schritt darin bestehen, einen Notfallreaktionsplan (Incident-Response-Plan) zu erstellen oder zu überprüfen. Dieser Plan sollte Ihre Verfahren und Richtlinien für die Reaktion auf Vorfälle darlegen und so den Prozess vereinfachen, wenn eine Meldepflicht eintritt.

Die erste NIS-Richtlinie verwendet den Schwellenwert „Anzahl der betroffenen Nutzer“ nicht mehr. Stattdessen beruht die NIS2-Richtlinie auf zwei unterschiedlichen Konzepten für die Pflichten zur Reaktion auf Vorfälle:

## SICHERHEITSVORFÄLLE

Jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der über Netz- und Informationssysteme angebotenen oder zugänglichen Dienste beeinträchtigt *(Artikel 6 Absatz 6).*

## CYBERBEDROHUNGEN

Jeder potenzielle Umstand, jedes Ereignis oder jede Handlung, die Netz- und Informationssysteme, die Nutzer solcher Systeme und andere Personen schädigen, stören oder auf andere Weise beeinträchtigen könnten *(Artikel 2 Absatz 8 des Rechtsakts zur Cybersicherheit, auf den in Artikel 6 Absatz 10 von NIS2 verwiesen wird).*

**Artikel 23 sieht vor, dass ein Vorfall als erheblich gilt, wenn:**

1. Er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betroffene Einrichtung verursacht hat oder verursachen kann;
2. Er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

## Im Falle einer Cyberbedrohung oder eines erheblichen Vorfalls müssen wesentliche und wichtige Einrichtungen unverzüglich Folgendes melden:

- Die zuständigen Behörden oder das nationale Computer-Notfallteam (CSIRT), wobei auch alle Informationen zu übermitteln sind, die die Feststellung etwaiger grenzüberschreitender Auswirkungen des Vorfalls ermöglichen;
- Gegebenenfalls die Empfänger ihrer Dienste, wenn der Vorfall die Erbringung dieses Dienstes voraussichtlich beeinträchtigt;
- Gegebenenfalls die Empfänger im Hinblick auf die Bedrohung selbst. Bei einer erheblichen Cyberbedrohung sollten auch mögliche Gegenmaßnahmen oder Abhilfemaßnahmen mitgeteilt werden.

# MELDUNG AN DAS CSIRT

Bei der Meldung an die zuständigen Behörden oder das Computer-Notfallteam (CSIRT) sind Organisationen verpflichtet, bestimmte Informationen zu übermitteln. Dazu gehören alle relevanten Angaben, die für die Behörden als wichtig erachtet werden:

1. eine erste Meldung innerhalb von 24 Stunden, nachdem die Einrichtung Kenntnis von dem Vorfall erlangt hat, mit dem Hinweis, ob der Verdacht besteht, dass er durch rechtswidrige oder böswillige Handlungen verursacht wurde oder grenzüberschreitende Auswirkungen haben könnte;
2. innerhalb von 72 Stunden nach Kenntniserlangung von dem erheblichen Vorfall eine Vorfallmeldung, die gegebenenfalls die vorherigen Informationen aktualisiert und eine erste Bewertung des erheblichen Vorfalls angibt, einschließlich seiner Schwere und Auswirkungen sowie, soweit verfügbar, der Kompromittierungsindikatoren;
3. auf Ersuchen einer zuständigen Behörde oder eines CSIRT einen Zwischenbericht über relevante Statusaktualisierungen;
4. einen Abschlussbericht spätestens einen Monat nach Übermittlung der ersten Meldung, der mindestens Folgendes enthält:
    - eine detaillierte Beschreibung des Vorfalls, seiner Schwere und Auswirkungen;
    - die Art der Bedrohung oder die Grundursache, die den Vorfall wahrscheinlich ausgelöst hat;
    - angewandte und laufende Abhilfemaßnahmen;
    - sowie gegebenenfalls die grenzüberschreitenden Auswirkungen des Vorfalls;

5. ist der Vorfall zum Zeitpunkt der Übermittlung des Abschlussberichts noch nicht abgeschlossen, sollten die Einrichtungen zu diesem Zeitpunkt einen Fortschrittsbericht und innerhalb eines Monats nach Bewältigung des Vorfalls einen Abschlussbericht vorlegen.

Jeder Mitgliedstaat verfügt über ein eigenes Computer-Notfallteam (CSIRT), an das Vorfälle gemeldet werden können. Darüber hinaus haben einige Länder „zuständige Behörden“ benannt. Im Kontext der aktuellen NIS-Richtlinie sind die ANSSI in Frankreich, das CCB in Belgien und das BSI in Deutschland als zuständige Behörden benannt.

# ALS WESENTLICHE SEKTOREN IM ANWENDUNGSBEREICH VON NIS2 EINGESTUFTE SEKTOREN

Aufgeführt in Anhang I der NIS2.

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| **ENERGIE** | Elektrizität | Elektrizitätsversorgungsunternehmen, Verteilnetzbetreiber, Übertragungsnetzbetreiber, Stromerzeuger, Strommarktbetreiber und ausgewählte Marktteilnehmer |
| | Fern-wärme/-kälte | Betreiber von Fernwärme- oder Fernkälteversorgung |
| | Öl | Betreiber von Öl-Fernleitungen, Betreiber von Anlagen zur Ölförderung, -raffination und -aufbereitung, zur Speicherung und zum Transport, ausgewählte zentrale Bevorratungsstellen |
| | Gas | Versorgungsunternehmen, Verteilnetzbetreiber, Fernleitungsnetzbetreiber, Speicheranlagenbetreiber, LNG-Anlagenbetreiber, Erdgasunternehmen |
| **VERKEHR** | Luftverkehr | Luftfahrtunternehmen, Flughafenleitungsorgane, Anbieter von Flugverkehrskontrolldiensten (ATC) |
| | Schienenverkehr | Infrastrukturbetreiber, Eisenbahnunternehmen |

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| | Schifffahrt | Passagier- und Frachtschifffahrtsunternehmen der Binnen-, See- und Küstenschifffahrt, Leitungsorgane von Häfen, Betreiber von Schiffsverkehrsdiensten |
| | Straßenverkehr | Straßenverkehrsbehörden, delegierte Verkehrsmanagementkontrollen, Betreiber intelligenter Verkehrssysteme |
| **BANKWESEN** | | Kreditinstitute |
| **FINANZMARKT-INFRASTRUKTUREN** | | Betreiber von Handelsplätzen, zentrale Gegenparteien (CCPs) |
| **GESUNDHEIT** | Pharma, Herstellung, Labore, Dienste | Gesundheitsdienstleister, Einrichtungen, die während einer gesundheitlichen Notlage kritische Medizinprodukte herstellen, EU-Referenzlabore, Einrichtungen für Forschung und Entwicklung von Arzneimitteln, Einrichtungen zur Herstellung pharmazeutischer Grundstoffe und Zubereitungen |
| **TRINKWASSER** | | Lieferanten und Verteiler von Wasser für den menschlichen Gebrauch, ausgenommen solche, bei denen dies nicht die Haupttätigkeit ist |
| **ABWASSER** | | Unternehmen, die kommunales, häusliches und industrielles Abwasser sammeln, entsorgen oder behandeln, sofern dies wesentlicher Teil ihrer Tätigkeit ist |
| **WELTRAUM** | Infrastruktur, Dienste | Betreiber bodengestützter Infrastruktur, die im Eigentum von Mitgliedstaaten oder privaten Parteien stehen, von diesen verwaltet und betrieben werden und weltraumgestützte Dienste unterstützen |
| **B2B-IKT-DIENSTE** | | Managed Services Provider (MSP), Managed Security Services Provider (MSSP) |

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| **DIGITALE INFRASTRUKTUR** | | Betreiber von Internet-Knoten (IXP), DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content-Delivery-Netzwerken, Vertrauensdiensteanbieter, Anbieter öffentlicher elektronischer Kommunikationsnetze, Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste |
| **ÖFFENTLICHE VERWALTUNG** | | Einrichtungen der öffentlichen Verwaltung von Zentral- und Regionalregierungen, wie von einem Mitgliedstaat nach nationalem Recht bestimmt |

# ALS WICHTIGE SEKTOREN IM ANWENDUNGSBEREICH VON NIS2 EINGESTUFTE SEKTOREN

Aufgeführt in Anhang II der NIS2.

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| **POST- UND KURIERDIENSTE** | | Anbieter von Postdiensten, einschließlich Anbieter von Kurierdiensten |
| **ABFALLBE-WIRTSCHAFTUNG** | | Unternehmen der Abfallbewirtschaftung, ausgenommen solche, für die die Abfallbewirtschaftung nicht die wirtschaftliche Haupttätigkeit ist |
| **PRODUKTION, VERARBEITUNG UND VERTRIEB VON LEBENSMITTELN** | | Einrichtungen des Großhandels sowie der industriellen Produktion und Verarbeitung jeglicher Lebensmittel und Getränke. Kein Lebensmittelbetrieb (z. B. Futtermittel, lebende Tiere, sofern nicht für den menschlichen Verzehr, Pflanzen vor der Ernte) |
| **HERSTELLUNG, PRODUKTION UND VERTRIEB VON CHEMIKALIEN** | | Unternehmen, die Stoffe und Erzeugnisse herstellen, produzieren und vertreiben |

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| **PRODUKTION, VERARBEITUNG UND VERTRIEB VON LEBENSMITTELN** | | Lebensmittelbetriebe, die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind |
| **VERARBEITENDES GEWERBE** | Medizinprodukte und In-vitro-Diagnostika | Entities manufacturing medical devices |
| | Computer, elektronische und optische Erzeugnisse | Einrichtungen, die Computer, elektronische und optische Erzeugnisse, elektronische Bauelemente und Leiterplatten, Kommunikationsausrüstung, Unterhaltungselektronik, Mess-, Prüf- und Navigationsinstrumente, Uhren, Bestrahlungs-, elektromedizinische und elektrotherapeutische Geräte, optische Instrumente und fotografische Ausrüstung sowie magnetische und optische Datenträger herstellen |
| | Elektrische Ausrüstung | Einrichtungen, die elektrische Ausrüstung, Motoren, Generatoren, Transformatoren und Verteil-/Schaltapparate, Batterien und Akkumulatoren, Kabel und Installationsmaterial, Lichtwellenleiter, Beleuchtungsausrüstung, Haushaltsgeräte und sonstige elektrische Ausrüstung herstellen |
| | Maschinenbau a. n. g. | Einrichtungen, die Mehrzweck- und Spezialmaschinen, Motoren und Turbinen, Pumpen und Kompressoren, Armaturen, Lager und Getriebe, Hebe- und Fördereinrichtungen, land- und forstwirtschaftliche Maschinen, Werkzeugmaschinen, Maschinen für Metallurgie, Bergbau, Bauwesen, Nahrungs-/Getränke-, Textil-, Papier-, Kunststoff- und Gummiverarbeitung sowie sonstige Maschinen a. n. g. herstellen |
| | Kraftwagen, Anhänger und Sattelanhänger | Einrichtungen, die Kraftwagen, Anhänger und Sattelanhänger, Aufbauten (Karosserien), Teile und Zubehör sowie elektrische und elektronische Ausrüstung für Kraftfahrzeuge herstellen |

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| | Sonstiger Fahrzeugbau | Einrichtungen, die Schiffe und Boote, Schienenlokomotiven und rollendes Material, Luft- und Raumfahrzeuge und zugehörige Maschinen, militärische Kampffahrzeuge, Krafträder, Fahrräder und Behindertenfahrzeuge sowie sonstige Fahrzeuge a. n. g. herstellen |
| **DIGITALE DIENSTEANBIETER** | | Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke |
| **FORSCHUNG** | | Forschungseinrichtungen |

# ZUSAMMENFASSUNG

Die NIS2-Cybersicherheitsrichtlinie aktualisiert und erweitert die Cybersicherheitsvorschriften der EU mit dem Ziel, die Widerstandsfähigkeit gegenüber Cyberbedrohungen zu erhöhen. Sie dehnt die Verantwortung auf die oberste Leitungsebene aus und sieht empfindliche Bußgelder bei Nichteinhaltung vor. Darüber hinaus betrifft sie Zulieferer und verlangt Bewertungen der Cybersicherheit von Drittparteien. Strengere Anforderungen an die Reaktion auf Vorfälle schreiben eine rasche Meldung an die nationalen CSIRTs oder zuständigen Behörden vor und betonen einen proaktiven Ansatz für die Cybersicherheit.

Organisationen sollten ihre Cybersicherheitspraktiken gründlich bewerten und ihre Einstufung nach der Richtlinie bestimmen. Diese Selbstbewertung hilft dabei, Verbesserungsbereiche zu identifizieren und die Einhaltung der regulatorischen Anforderungen sicherzustellen.

Um die Komplexität von Compliance-Standards wie NIS2 oder ISO/IEC 27002:2022 zu bewältigen, können Organisationen Werkzeuge wie Mondoo nutzen. Mondoo bietet umfassendes Schwachstellenmanagement und Compliance-Überwachung und unterstützt Organisationen dabei, Sicherheitslücken in ihrer Infrastruktur zu erkennen und zu beheben.

Durch die Integration von Mondoo in ihre Sicherheitsprozesse können Organisationen die künftige Einhaltung der NIS2-Anforderungen sicherstellen, proaktive Schritte zur Stärkung ihrer Cybersicherheit unternehmen und zu einer sichereren digitalen Umgebung für alle beitragen.

# WIE MONDOO BEI DER NIS2-COMPLIANCE HILFT

## Compliance ist ein Weg, aber er muss nicht manuell sein.

NIS2 zu erfüllen bedeutet nicht, immer längere Listen von Findings zu produzieren. Es geht darum, sie zu schließen, kontinuierlich, und dies auch nachweisen zu können. **Genau hier verändert Mondoo die Gleichung.**

Mondoo ist eine agentische Plattform für Exposure Management, die eine einzige, kontinuierliche geschlossene Schleife über Ihren gesamten Bestand hinweg betreibt. Sie erkennt Schwachstellen und Fehlkonfigurationen, priorisiert sie nach realem Risiko, spielt den Fix aus und verifiziert, dass der Fix Bestand hat. Diese Schleife bildet genau das ab, was Artikel 21 verlangt, vom Management und der Offenlegung von Schwachstellen bis hin zur laufenden Bewertung, wie wirksam Ihre Sicherheitsmaßnahmen tatsächlich sind.

Mondoo deckt zudem den gesamten Weg vom Quellcode bis zur Produktion ab. Statische Codeanalyse und Secret Scanning, angetrieben von Mondoos Open-Source-Werkzeug xgrep über mehr als 34 Sprachen hinweg, sichern Software an der Quelle, während kontinuierliche Bewertung Cloud, Container und den übrigen Technologie-Stack härtet. Da NIS2 die Verantwortung tief in die Lieferkette hinein ausweitet, liefert diese Abdeckung vom Quellcode bis zum verifiziert geschlossenen Fix sowohl regulierten Einrichtungen als auch ihren Zulieferern die Nachweise für sichere Entwicklung und Drittparteien-Sicherheit, die die Richtlinie verlangt.

Und weil Mondoo seine Kontrollen von Haus aus auf NIS2 und ISO/IEC 27002:2022 abbildet, wandelt sich Compliance von einer mehrjährigen manuellen Übung in eine kontinuierliche, evidenzbasierte Überwachung, die Sie einem Prüfer direkt vorlegen können.

## SIE FINDEN NICHT NUR DIE LÜCKEN. SIE SCHLIESSEN SIE, UND SIE KÖNNEN IHRE ARBEIT BELEGEN.

MONDOO.COM