Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

NIS2: Ein Mindestniveau für die IT-Sicherheit in Europa

Was ist NIS2?

NIS2 ist die Abkürzung für „Network and Information Security 2“ und betitelt die schon 2023 in Kraft getretene Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (EU-Richtlinie 2022/2555). Der Fokus von NIS2 liegt auf den Bereichen Cybersecurity und Informationstechnik. Die NIS2-Richtlinie ersetzt vollständig die NIS-Richtlinie von 2016.

Welches Ziel verfolgt NIS2?

Mit NIS2 stellt die Europäische Union Mindestanforderungen zur Stärkung der IT-Sicherheit und der Verbesserung der Resilienz kritischer Wirtschaftsbereiche. So sollen große Teile der europäischen Wirtschaft geschützt und eine einheitliche Umsetzung von Cybersecurity in der Europäischen Union erreicht werden.

Ab wann gilt NIS2?

Mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (kurz: NIS2UmsuCG) soll die EU-Richtlinie in Deutschland umgesetzt werden. Eine finale Fassung des Umsetzungsgesetzes liegt noch nicht vor. Der 4. Referentenentwurf mit Stand vom 24.06.2024 ist hier zu finden:
https://www.securepoint.de/fileadmin/securepoint/allgemein/downloads/pdfs/nis2/NIS2-Vergleichsfassung-zum-Bearbeitungsstand-07.05.2024-10-19.pdf

In Österreich gibt es bereits einen Gesetzesentwurf.

Für wen gilt NIS2?

Der Anwendungsbereich der NIS2-Richtlinie geht weit über die bisher bekannten kritischen Infrastrukturen (KRITIS) hinaus. Unternehmen fallen dann in den Anwendungsbereich der NIS2, wenn sie

- den definierten Schwellenwerten entsprechen,
- in den in NIS2 aufgeführten 18 Wirtschaftssektoren tätig sind und/oder
- Dienste im Zusammenhang der Netzwerk- und Informationssicherheit erbringen.

Grundsätzlich findet NIS2 Anwendung für mittlere Unternehmen oder für Unternehmen, die die Schwellenwerte für mittlere Unternehmen überschreiten.

Mittleres Unternehmen

- Mindestens 50 und weniger als 250 Beschäftigte **und**
- entweder einen Jahresumsatz von mindestens 10 Mio. Euro, aber höchstens 50 Mio. Euro oder
- eine Jahresbilanzsumme von mindestens 10 Mio. Euro, aber höchstens 43 Mio. Euro.

Unabhängig von der Größe der Einrichtungen gilt die NIS2-Richtlinie auch für Einrichtungen, die in einem der in NIS2 aufgeführten 18 Sektoren tätig sind. Dazu zählen

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

z. B. der Sektor Energie oder Verwaltung von IKT-Diensten bzw. Verarbeitendes Gewerbe/Herstellung von Waren oder Anbieter digitaler Dienste.

Wesentliche und wichtige Einrichtungen
NIS2 unterscheidet darüber hinaus noch „wesentliche Einrichtungen“ und „wichtige Einrichtungen“.

Unternehmen gelten als „wesentliche Einrichtung“, wenn sie in einem Sektor mit hoher Kritikalität tätig sind sowie den Schwellenwert für ein mittleres Unternehmen überschreiten, d. h. mindestens 250 Beschäftigte zählen und entweder über 50 Mio. Jahresumsatz oder eine Bilanzsumme von über 43 Mio. Euro aufweisen. Folgende Wirtschaftssektoren gehören zu den Branchen mit hoher Kritikalität:

1. Energie
2. Verkehr
3. Bankwesen
4. Finanzmarktinfrastrukturen
5. Gesundheitswesen
6. Trinkwasser
7. Abwasser
8. Digitale Infrastruktur
9. Verwaltung von IKT-Diensten (Business-to-Business)
10. Öffentliche Verwaltung
11. Weltraum

Unternehmen gelten als „wichtige Einrichtung“, wenn sie in einem der insgesamt aufgeführten 18 Sektoren tätig sind und nicht unter die Definition der „wesentlichen Einrichtungen“ fallen.

1. Post- und Kurierdienste
2. Abfallbewirtschaftung
3. Produktion, Herstellung und Handel mit chemischen Stoffen
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln
5. Verarbeitendes Gewerbe/Herstellung von Waren
6. Anbieter digitaler Dienste
7. Forschung

Die genannten Sektoren unterteilt NIS2 noch in weitere Teilsektoren

Klein- und Kleinstunternehmen können ebenfalls unter die Richtlinie fallen, wenn sie in einem der 18 Sektoren bzw. in einem von NIS2 als Sonderfälle benannten Diensten tätig sind.

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Welche Vorgaben macht NIS2?
NIS2 fordert einen präventiven Ansatz für die Informationssicherheit. Zu den einzelnen IT-Sicherheitsmaßnahmen macht NIS2 zahlreiche Vorgaben – angefangen bei einem Konzept für das Risikomanagement über technische Maßnahmen bis hin zu Berichtspflichten an zuständige Behördenbei Sicherheitsvorfällen.
Durch aktive Registrierungs-, Nachweis- und Berichtspflicht sowie einen verbindlichen Informationsaustausch erweitern sich staatliche Befugnisse.

Netz- und Informationssysteme müssen abgesichert werden. Folgende Maßnahmen sind nach NIS2 u.a. vorgesehen: Risikoanalyse, Bewältigung von Sicherheitsvorfällen, Aufrechterhaltung des Betriebes, Sicherheit der Lieferkette, Bewertung von Risikomanagementmaßnahmen, Schulungen im Bereich der Cybersicherheit.

Übermittlungs-, Registrierungs- und Meldepflichten

Liste von wesentlichen, wichtigen Einrichtungen und DNS-Diensteanbietern
Bis zum 17. April 2025 sollen die Mitgliedsstaaten eine Liste der wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänenamen-Registrierungsdienste erbringen erstellen. Um diese Liste erstellen zu können, sollen die Mitgliedsstaaten den betroffenen Einrichtungen die Übermittlung folgender Informationen an die zuständige Behörde vorschreiben:

- Name der Einrichtung
- Anschrift
- aktuelle Kontaktdaten einschließlich E-Mail-Adressen, IP-Adressbereiche und Telefonnummern
- ggf. Angabe des Tätigkeits- oder Teilsektor
- ggf. eine Liste der EU-Mitgliedstaaten, in denen die Einrichtung Dienste erbringt, die in den Anwendungsbereich der NIS2-Richtlinie fallen

In Deutschland wird gemäß Referentenentwurf zuständige Behörde das Bundesamt für Sicherheit in der Informationstechnik (BSI) sein. Änderungen der gemeldeten Angaben müssen unverzüglich mit Zeitpunkt der Änderung, in jedem Fall aber innerhalb von zwei Wochen nach Änderung von der Einrichtung angegeben werden.

Diese Informationen werden von den Mitgliedsstaaten an die Kommission und die Kooperationsgruppen weitergeleitet. Damit wird der von NIS2 bezweckte Informationsaustausch und die Transparenz für die grenzüberschreitende Zusammenarbeit in der EU ermöglicht.

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Registrierung von Anbietern digitaler Dienste
Bis zum 17. Januar 2025 sollen sich Anbieter digitaler Dienste bei der nationalen Behörde registrieren müssen. Diese Frist gilt für:

- Domänennamen-Registrierungsdienste
- Anbieter von Cloud-Computing-Diensten
- Anbieter von Rechenzentrumsdiensten
- Betreiber von Inhaltszustellnetzen
- Anbieter von verwalteten Diensten (MSP)
- Anbieter von verwalteten Sicherheitsdiensten (MSSP)
- Anbieter von Online-Marktplätzen, Online-Suchmaschinen
- Plattformen für Dienste sozialer Netzwerke

Änderungen müssen innerhalb von drei Monaten angegeben werden.

Meldepflichten
Mit der Richtlinie soll die Reaktion auf und Handhabung von Cybersicherheitsvorfällen und -krisen innerhalb der EU verbessert werden. Dafür werden klare Verantwortlichkeiten benannt.
NIS2 beinhaltet zudem einen mehrstufigen Ansatz für die Meldung von Sicherheitsvorfällen. Betroffene Unternehmen haben 24 Stunden ab dem Zeitpunkt, zu dem sie auf einen erheblichen Sicherheitsvorfall aufmerksam werden. Die Meldepflichten umfassen die Schwere eines Sicherheitsvorfalls, den Zeitrahmen für die Meldung, den Inhalt der Meldung und den oder die Empfänger der Meldung. Eine Warnung muss an die CSIRT oder die zuständige nationale Behörde erfolgen. Diese ermöglichen bei Bedarf Unterstützung bei Leitlinien oder operative Beratung bei der Umsetzung möglicher Minderungsmaßnahmen. Auf die Frühwarnung sollte innerhalb von 72 Stunden nach Kenntnisnahme des Vorfalls eine Meldung des Vorfalls und spätestens einen Monat später ein Abschlussbericht folgen.

Innerhalb der EU soll außerdem der Austausch von Informationen zu Sicherheitsvorfällen zwischen Betreibern gefördert und unterstützt werden.

Was bedeutet Cyberhygiene nach NIS2?
Vor dem Hintergrund der Zunahme von Cyberangriffen und einer hohen Bedrohungslage wird Prävention in der IT-Sicherheit immer wichtiger. Mit der NIS2-Richtlinie wird die bessere Vorbeugung gegen IT-Sicherheitsvorfälle europaweit verankert. Der Grundsatz lautet: Eine zuverlässige Cyberhygiene schützt die Hard- und Software sowie die Geschäfts- und Endnutzerdaten von Unternehmen. Dazu gehören zum Beispiel regelmäßige Updates, ein ordentliches Passwortmanagement, systematische Datensicherungen oder sichere Multifaktor-Authentifizierung.

Die wesentlichen und wichtigen Einrichtungen sollten eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden, z. B. Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Zugriffsmanagement oder Sensibilisierung der Nutzer, Schulungen für ihre Beschäftigten organisieren und das Bewusstsein für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken schärfen.

Wer trägt die Verantwortung bei Verstößen und welche Sanktionen sind zu erwarten?
NIS2 sieht vor, dass Leitungsorgane oder ihre Mitglieder für Verstöße gegen NIS2 verantwortlich gemacht werden. Im Sinne einer guter Governance müssen die Leitungsorgane u.a. die Umsetzung der Maßnahmen aktiv überwachen, an Schulungen teilnehmen und diese Beschäftigten anbieten.

Mit NIS2 gehen erweiterte Sanktionsvorschriften mit neuen, eindeutig definierten Bußgeldtatbeständen und erhöhten Bußgeldern:

- Wichtige Einrichtungen: Geldbuße mit einem Höchstbetrag von mindestens 7 Mio. EUR oder mit einem Höchstbetrag von mindestens 1,4 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr erreichten Umsatzes des Unternehmens, dem die Einrichtung angehört. Der jeweils höhere Betrag zählt.
- Wesentliche Einrichtungen: Geldbuße mit einem Höchstbetrag von mindestens 10 Mio. EUR oder einem Höchstbetrag von mindestens 2 Prozent des gesamten weltweiten im vorangegangenen Geschäftsjahr erreichten Umsatzes des Unternehmens, dem die Einrichtung angehört. Der jeweils höhere Betrag zählt.

Umsetzung NIS2 in nationales Recht

Seit wann gilt NIS2 in der EU?
NIS2 ist als europäische Richtlinie am 16. Januar 2023 in Kraft getreten. In der Richtlinie wird festgelegt, dass bis zum 17. Oktober 2024 die EU-Mitgliedsstaaten die erforderlichen Vorschriften erlassen und veröffentlichen, sprich in nationales Recht umgesetzt müssen. Entsprechend sollen die Vorschriften ab dem 18. Oktober 2024 in den jeweiligen EU-Mitgliedstaaten anzuwenden sein.

Deutsche Gesetzgebung
Der aktuelle Referentenentwurf des NIS2-Umsetzungsgesetzes befindet sich weiterhin in der Ressortabstimmung. Am 24.07.2024 entscheidet das Kabinett der Bundesregierung darüber, ob der Gesetzesentwurf in das parlamentarische Verfahren übergeht. Ob der 17. Oktober 2024 für die Umsetzung der NIS2-Richtlinie gehalten werden kann, ist derzeit noch offen. Das gleiche gilt für das weitere Verfahren bis zu einer möglichen Verabschiedung des Gesetzes. Es ist nicht unrealistisch, dass sich die Umsetzung in nationales Recht verzögert.

Bedeutung von NIS2 für IT-Dienstleister & -Fachhändler
Für IT-Dienstleister und -Fachhändler gilt der Anwendungsbereich von NIS2, wenn sie

- durch ihre Tätigkeit in Nr. 9 der Sektoren mit hoher Kritikalität, "Verwaltung von IKT-Diensten (Business-to-Business)", selbst eine wesentliche oder wichtige Einrichtung sind.

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

- als IKT-Dienstleister für eine wesentliche oder wichtige Einrichtung tätig sind. Sie sind unabhängig von ihrer eigenen Größe Teil der Lieferkette dieser Unternehmen.

Die hohe Kritikalität von IKT-Diensten

IT-Dienstleister und -Fachhändler fallen gemäß der EU-Richtlinie unter NIS2, wenn sie Anbieter von verwalteten Diensten ("Managed Services Provider", kurz MSP) oder Anbieter von verwalteten Sicherheitsdiensten ("Managed Security Services Provider", kurz MSSP) sind. Das bedeutet:

- Ein Anbieter verwalteter Dienste erbringt Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne.
- Ein Anbieter verwalteter Sicherheitsdienste ist ein auf Tätigkeiten im Zusammenhang mit dem Management von Cybersicherheitsrisiken spezialisierter Anbieter verwalteter Dienste.

Was bedeutet IKT-Produkt, -Dienst und -Prozess?

- IKT-Produkt bezeichnet ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems.
- IKT-Dienst bezeichnet einen Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht.
- IKT-Prozess bezeichnet jegliche Tätigkeiten, mit denen ein IKT-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.

Landingpage NIS2

https://www.securepoint.de/fuer-partner/alles-zu-nis-2