Für eine zügige Implementierung im Unternehmen

Leitfaden zur NIS2-Richtlinie - mit praktischen Tipps zur Umsetzung und Verbesserung der Cybersicherheit

digitalpreview GmbH
...the way beyond

Inhaltsverzeichnis

Investitionen in Cybersicherheit:
Datenschutz, Schulungen und NIS2-Richtlinie für eine
stärkere Unternehmensresilienz 02

Was ist die NIS2-Richtlinie? 03

Umsetzung und Auswirkungen der NIS2:
Neue Standards für Cybersecurity in der EU 04

Welche Unternehmen sind von der NIS2 betroffen? 05

Ihr Unternehmen fällt unter die NIS2:
Leitfaden zur Vorgehensweise 07

1. Maßnahmen vorbereiten und verstärken
2. Meldepflichten bei Sicherheitsvorfällen
3. Registrierung
4. Sicherheit in der Lieferkette
5. Pflichten der Geschäftsführung

Welche Sanktionen drohen bei Verstößen? 09

Was jetzt zu tun ist? 10

Wir helfen Ihnen weiter!

Investitionen in Cybersicherheit: Datenschutz, Schulungen und NIS2-Richtlinie für eine stärkere Unternehmensresilienz

In Zeiten steigender Cyberangriffe stehen Unternehmen vor großen Herausforderungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet die IT-Sicherheitslage in Deutschland 2023 als „angespannt bis kritisch". Besonders Ransomware, die Daten verschlüsselt und nur gegen Lösegeld freigibt, ist eine wachsende Bedrohung. Fortschritte in Technologien wie Künstliche Intelligenz bieten Hackern zusätzliche Angriffsmöglichkeiten.

„Die Bedrohung im Cyberraum ist so hoch wie nie zuvor."

Seit 2020 sind Cybervorfälle um bis zu 600 % gestiegen, begünstigt durch vermehrte Remote-Arbeit, die neue Schwachstellen schafft. Angriffe betreffen nicht nur Unternehmen, sondern auch Bildungseinrichtungen und andere Organisationen, mit immer ausgefeilteren Methoden.*

Unternehmen müssen in Cybersicherheitsmaßnahmen investieren, um sich zu schützen. Wichtige Maßnahmen umfassen Datenschutz, regelmäßige Mitarbeiterschulungen und aktuelle Sicherheitssoftware. Die NIS2-Richtlinie fordert Unternehmen auf, ihre IT-Sicherheit zu priorisieren und ihre Resilienz zu stärken, um in einer vernetzten Welt widerstandsfähiger zu werden.

Dieser Leitfaden bietet praxisnahe Tipps zur Umsetzung der NIS2-Richtlinie und zur Verbesserung der Cybersicherheit.

Quelle: „Die Lage der IT-Sicherheit in Deutschland 2023", Bundesamt für Sicherheit in der Informationstechnik

Hintergrundwissen

Was ist die NIS2-Richtlinie?

Die NIS2-Richtlinie (EU 2022/2555) ist eine Überarbeitung der ursprünglichen Richtlinie für Netz- und Informationssysteme (NIS) von 2016, die aufgrund zunehmender Cyberbedrohungen entwickelt und 2022 verabschiedet wurde.
Die EU-Mitgliedsstaaten sind angewiesen die NIS-2 Richtlinien bis 18.10.2024 umzusetzen. In Deutschland ist hingegen erst mit einem Inkrafttreten im März 2025 zu rechnen.

Hintergrund zur ursprünglichen NIS-Richtlinie

Die erste NIS-Richtlinie (EU 2016/1148) setzte einheitliche Cybersicherheitsstandards für kritische Infrastruktursektoren wie Energie, Verkehr und Finanzen. Betreiber dieser Infrastrukturen mussten Sicherheitsvorfälle melden und Schutzmaßnahmen ergreifen. Die Richtlinie erwies sich jedoch als unzureichend und wurde inkonsistent umgesetzt.

Einführung und Ziele von NIS2

Die NIS2-Richtlinie erweitert den Geltungsbereich auf weitere kritische Sektoren wie Abfallwirtschaft, Postdienste und Hersteller kritischer Infrastrukturen. Ziel ist die Implementierung grundlegender Cybersicherheitsmaßnahmen in mehr Sektoren und die Verbesserung der Zusammenarbeit bei der Bewältigung von Cyberbedrohungen innerhalb der EU. Hauptpunkte und Neuerungen der NIS2 sind:

- Umfangreichere Schutzmaßnahmen
- Strengere Meldepflichten
- Strengere Aufsicht
- Mehr Pflichten für die Geschäftsführung

Umsetzung und Auswirkungen der NIS2

Neue Standards für Cybersecurity in der EU

In Deutschland wird die Umsetzung durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) erfolgen.

Schätzungen zufolge könnten **bis zu 40.000 Unternehmen** und Organisationen von den neuen Bestimmungen **betroffen sein**.

Die Schlüsselziele der NIS2-Richtlinie:

Erhöhung der Resilienz: Die Richtlinie zielt darauf ab, Unternehmen und Behörden widerstandsfähiger gegen Cyberangriffe zu machen.

Förderung der Zusammenarbeit: Sie stärkt die Kooperation zwischen staatlichen Stellen und der Wirtschaft, um gemeinsame Cybersicherheitsherausforderungen zu bewältigen.

Unternehmen, die ihre Sicherheitsstandards frühzeitig anpassen und bereits über ein ISMS z.B. nach ISO 27001, BSI IT-Grundschutz, VdS 10000 oder ähnliches verfügen, sind im Vorteil. Die Einhaltung der NIS2-Richtlinie ist nicht nur gesetzlich vorgeschrieben, sondern stärkt auch die Cybersicherheit und die digitale Wirtschaft in der EU.

Die EU hat die Pflichten und Sanktionen gegenüber der NIS1 deutlich verschärft. Bei Nichteinhaltung drohen Bußgelder, Betriebsunterbrechungen und persönliche Haftungsrisiken.

Prüfen Sie, ob Ihr Unternehmen unter die NIS2-Richtlinie fällt

Welche Unternehmen sind von der NIS2 betroffen?

Die NIS2-Richtlinie definiert klar, welche Unternehmen zur Einhaltung der neuen Cybersicherheitsvorschriften verpflichtet sind. Sie teilt Einrichtungen in zwei Hauptkategorien ein: **„kritische" und „wichtige"** Einrichtungen, basierend auf der Bedeutung ihrer Dienstleistungen und ihrer Unternehmensgröße.

Die **kritischen Einrichtungen** umfassen Organisationen, deren Dienste von besonders hoher Bedeutung sind. Diese sind in **Anhang I** der Richtlinie aufgeführt. Die **wichtigen Einrichtungen** werden in **Anhang II** gelistet und betreffen weitere kritische Sektoren.

Aufgepasst! Ob Ihr Unternehmen unter die NIS2-Richtlinie fällt und Sie meldepflichtig sind, müssen Sie selbst ermitteln und sich proaktiv bei der zuständigen Behörde registrieren. In Deutschland ist die Meldung an das BSI zu richten.

Sie sind sich nicht sicher, ob Ihr Unternehmen zu den Einrichtungen gehört, die NIS2 einhalten müssen? Machen Sie den interaktiven Selbsttest hier per Scan des QR-Codes oder unter www.bsi.bund.de.

ACHTUNG: NIS2 betrifft auch Lieferketten

Die Richtlinie verlangt, dass auch Ihre Zulieferer und Dienstleister Sicherheitsmaßnahmen ergreifen. Hacker nutzen oft Schwachstellen in Lieferketten, um kompromittierte Software über Partner zu verteilen und großen Schaden anzurichten.

Maßnahmen

Prüfen Sie in bestehenden und künftigen Verträgen, ob alle Parteien ihre IT-Systeme ausreichend schützen.

Einteilung in Kritische und Wichtige Einrichtungen

Kritische Einrichtungen

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastruktur
- Gesundheit
- Trink- und Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)
- Öffentliche Verwaltung
- Weltraum

Wichtige Einrichtungen

- Post- und Kurierdienste
- Abfallwirtschaft
- Produktion und Handel mit chemischen Stoffen
- Lebensmittelproduktion und -verarbeitung
- Verarbeitendes Gewerbe
- Anbieter digitaler Dienste
- Forschung

JA

X **Kleines Unternehmen**
unter 50 Beschäftigte oder
unter 10 Mio € Umsatz p.a. ..... **NIS2 trifft nicht zu**

Ausnahme: Die Tätigkeit des Unternehmens hat kritische Auswirkungen auf die öffentliche Ordnung oder die Betriebsunterbrechung würde zu systemischen Risiken führen.

Mittleres Unternehmen
mind. 50 Beschäftigte oder
10 Mio. € Umsatz p.a. ..... **NIS2 trifft zu**

Großes Unternehmen
mind. 250 Beschäftigte oder
über 50 Mio. € Umsatz p.a. ..... **NIS2 trifft zu**

Diese Abbildung gibt einen grundlegenden Überblick darüber, ob Ihr Unternehmen von der NIS2-Richtlinie betroffen ist, wobei zu beachten ist, dass die Richtlinie in Artikel 2 weitere spezifische Ausnahmen und Sonderfälle regelt, die hier nicht abgebildet sind.

Maßnahmen zum Risikomanagement vorbereiten und verstärken

Ihr Unternehmen fällt unter die NIS2 - Leitfaden zur Vorgehensweise

Die NIS2-Richtlinie sieht eine Reihe von Pflichten für Unternehmen, aber auch für das Management vor. Hier ein Überblick über die fünf wichtigsten Punkte:

1. Maßnahmen zum Risikomanagement vorbereiten und verstärken

Sie müssen folgende Cybersicherheitsmaßnahmen umsetzen:

- **Risikoanalyse und IT-Sicherheit:** Entwickeln Sie Konzepte zur Erkennung und Eindämmung von Sicherheitsvorfällen.
- **Betriebskontinuität:** Stellen Sie sicher, dass der Betrieb auch im Krisenfall weiterläuft.
- **Sicherheit der Lieferkette:** Sichern Sie die Beziehungen zu Ihren Lieferanten gegen Cyberrisiken ab.
- **IT-Systeme:** Integrieren Sie Sicherheitsmaßnahmen beim Erwerb, der Entwicklung und Wartung Ihrer IT-Infrastruktur.
- **Wirksamkeit bewerten:** Überprüfen Sie regelmäßig die Effektivität Ihrer Sicherheitsmaßnahmen.
- **Schulungen und Cyberhygiene:** Schulen Sie Ihre Mitarbeiter in sicherem Verhalten und implementieren Sie grundlegende Sicherheitspraktiken.
- **Kryptografie:** Verwenden Sie Verschlüsselung für die sichere Authentifizierung und Kommunikation.
- **Personalsicherheit:** Implementieren Sie Konzepte zur Zugriffskontrolle und zum Schutz Ihrer Mitarbeiter.

Achtung: Für diese Maßnahmen sieht die Richtlinie einen gefahren übergreifenden Ansatz vor, d.h. Sie müssen Ihre IT-Systeme zusammen mit ihrer physischen Umgebung schützen.

2. Meldepflichten bei Sicherheitsvorfällen

Erhebliche Sicherheitsvorfälle müssen sofort an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden:

- **Innerhalb von 24 Stunden:** Frühwarnung mit einer ersten Einschätzung des Vorfalls.
- **Innerhalb von 72 Stunden:** Aktualisierte Meldung mit Details zur Schwere und den Auswirkungen.
- **Innerhalb eines Monats:** Abschlussbericht mit vollständiger Analyse und Abhilfemaßnahmen.

3. Registrierung

Registrieren Sie Ihr Unternehmen bei der zuständigen nationalen Behörde ab dem Datum des Inkrafttretens von NIS2. Nach der Registrierung müssen Sie Vorfälle melden und die Einhaltung der Sicherheitsanforderungen gewährleisten.

4. Sicherheit in der Lieferkette

Stellen Sie sicher, dass keine Sicherheitsrisiken durch Ihre Lieferkette entstehen. Überprüfen Sie die Sicherheitsstandards Ihrer Zulieferer und Partner.

5. Pflichten der Geschäftsführung

Die Geschäftsführung ist ab Inkrafttreten der NIS2-Richtlinie direkt verantwortlich für die Cybersicherheit. Geschäftsführer müssen Cybersicherheitsmaßnahmen umsetzen, überwachen und sicherstellen, dass das gesamte Unternehmen ausreichend geschult ist. Die Missachtung dieser Pflichten kann zu persönlicher Haftung führen.

Klingt zunächst nach einer Menge Aufwand? Durch die Einhaltung dieser Anforderungen tragen Sie wesentlich zur Widerstandsfähigkeit Ihres Unternehmens gegen Cyber-Bedrohungen bei und vermeiden potenzielle Sanktionen.

Welche Sanktionen drohen bei Verstößen?

Unternehmen, die unter die NIS2-Richtlinie fallen, sollten die Vorgaben dringend einhalten, um empfindliche Strafen zu vermeiden. Die möglichen Geldbußen für NIS2-Verstöße betragen (jeweils der höhere Betrag gilt):

- Wichtige Einrichtungen: Bis zu **7 Mio. € oder 1,4** % des weltweiten Vorjahresumsatzes
- Wesentliche Einrichtungen: Bis zu **10 Mio. € oder 2** % des weltweiten Vorjahresumsatzes
- Besonders schwere Fälle: Bis zu **20 Mio. € oder 4** % des weltweiten Vorjahresumsatzes

Zusätzlich können Behörden die Aussetzung des Geschäftsbetriebs anordnen. Führungskräfte müssen zudem mit persönlichen Haftungsrisiken rechnen.

Weil sich Cyber-Resilienz lohnt

Ein Sicherheitsvorfall ohne angemessene Maßnahmen kann zu erheblichen Schäden führen, darunter Imageverlust, Rechtskosten, Umsatzverluste, Lösegeldzahlungen und Datenschutzverstöße. Daher ist es für „kritische“ und „wichtige“ Einrichtungen entscheidend, die NIS2-Richtlinie ernst zu nehmen und notwendige Cybersicherheitsmaßnahmen zu ergreifen.

Unternehmen Sie jetzt folgende Schritte:

Um bis zur Inkraftsetzung gut vorbereitet zu sein, ist es wichtig, jetzt die folgenden Schritte zu unternehmen:

Betroffenheit prüfen:
Ermitteln Sie, ob Ihre Organisation von der NIS2-Richtlinie betroffen ist. Nutzen Sie ein kostenfreies Beratungsgespräch, um dies festzustellen und registrieren Sie sich rechtzeitig beim BSI.

Risikobewertung und Schwachstellenanalyse:
Bewerten Sie Risiken und bestehende IT-Sicherheitsmaßnahmen, identifizieren Sie Schwachstellen und entwickeln Sie Pläne zur Schließung dieser Lücken – auch in Ihren Lieferketten.

Umsetzung und Schulung:
Implementieren Sie die NIS2-Anforderungen, erstellen Sie Pläne für Sicherheitsvorfälle und schulen Sie Ihre Mitarbeiter. Überwachen und optimieren Sie kontinuierlich die umgesetzten Maßnahmen.

Tipp: Starten Sie frühzeitig mit der Umsetzung der NIS2-Richtlinie. Wir unterstützen Sie dabei, Ihre Cybersicherheits-Pflichten zu erfüllen und Ihre IT-Systeme zu schützen.

Sie haben Fragen?

Sie wünschen eine unverbindliche Beratung zur NIS2-Implementierung in Ihrem Unternehmen, zum Datenschutzmanagement und zum Thema externer Datenschutzbeauftragter?

Rufen Sie uns gerne an oder schreiben Sie uns eine E-Mail.
Wir helfen Ihnen weiter!

Tel.: +49 (0) 2542 868 462 0

welcome@digital-preview.de

www.digital-preview.de

Über uns

Wir sind ein erfahrenes Team aus zertifizierten Datenschutzexperten, Digitalisierungsprofis und Informationssicherheitsspezialisten, das mittelständische Unternehmen dabei unterstützt, ihre Prozesse zu digitalisieren, dabei die strengeren Anforderungen der NIS2 zu erfüllen und so ihre Cybersicherheit zu maximieren. Unser Ziel ist es, Ihre Daten sicher und Ihr Unternehmen fit für die digitale Zukunft zu machen.

digital preview GmbH
...the way beyond

digital preview GmbH
Hauptstraße 13
48712 Gescher

Tel: +49 (0) 2542 868 462 0
welcome@digital-preview.de
www.digital-preview.de