NIS-2-Richtlinie

Anwendung und Umsetzung in der Transport- und Logistikbranche

Was ist NIS-2?

Die NIS-2-Richtlinie ist die Richtlinie der Europäischen Union (EU) über Maßnahmen zu einem hohen gemeinsamen Cybersicherheitsniveau. Das Ziel der NIS-2-Richtlinie ist es, ein einheitliches Schutzniveau für Netzwerke und Informationssysteme kritischer Infrastrukturen zu schaffen.

- Mit der NIS-2-Richtlinie wurde **die Zahl der kritischen Sektoren** im Vergleich zur im Jahr 2016 verabschiedeten NIS-Richtlinie um elf Sektoren **erweitert** und genauer definiert.
- Die NIS-2-Richtlinie ist seit dem 16. Januar 2023 in Kraft und muss bis zum **17. Oktober 2024 in nationales Recht umgesetzt werden.**
- Die NIS-2-Richtlinie birgt neben umfangreichen Risikomanagementmaßnahmen ein Bußgeldrisiko sowie **ein erhebliches Haftungsrisiko für die Unternehmensleitung.**

Was ist der Anwendungsbereich NIS-2?

- Reguliert werden zwei Gruppen von Entitäten, die in **18 Sektoren** Leistungen oder Produkte bereitstellen.
- Einrichtungen werden unterteilt in **wesentliche und wichtige Einrichtungen:**
  - Wesentliche Einrichtungen: Große Betreiber aus den elf im Anhang I gelisteten Sektoren (Essential) und Sonderfälle
  - Wichtige Einrichtungen: Große Betreiber aus den sieben im Anhang II gelisteten Sektoren (Important) und mittlere Betreiber aller Sektoren
- Betroffen sind **große und mittlere Unternehmen ab 50 Mitarbeitern und 10 Mio. EUR Umsatz.**

Wie sieht NIS-2 für den Bereich Transport und Logistik aus?

Laut NIS-2 ist Transport (Verkehr) ein Sektor mit hoher Kritikalität (wesentliche Einrichtung – höchste Priorität).

Transport (Verkehr) umfasst Luftverkehr, Schienenverkehr, Schifffahrt und Straßenverkehr.

NIS-2 bringt eine neue Denkweise mit sich: Bislang wurden Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen als Kritische Infrastrukturen (KRITIS) definiert. Diese Bedeutung wurde auf Basis von KRITIS-Anlagen ermittelt, die für die Versorgung der Bevölkerung (allgemeiner Maßstab: Relevanz für die Versorgung von mehr als 500.000 Personen) wichtig sind. Bestrebungen zur Regulierung von Unternehmen von öffentlichem Interesse (UBI2) nach Umsatz oder Anzahl der Mitarbeitenden wurden bislang in Deutschland nicht umgesetzt.

NIS-2 hingegen definiert die Betroffenheit für 18 Sektoren, basierend auf Umsatz und Mitarbeiteranzahl – ab 50 Mitarbeitenden und/ oder 10 Mio. EUR Umsatz, ohne Anlagen-Schwellenwerte. Die betroffenen Unternehmen müssen Cyber-Security-Anforderungen umsetzen.

Darüber hinaus ist die Betroffenheit im Rahmen der Lieferkette des Unternehmens zu überprüfen.

Welche Sorgfaltspflichten bestehen für betroffene Unternehmen?

Die NIS-2-Erweiterung bringt zahlreiche Anforderungen mit sich, die von der Organisation über die Personalsicherheit bis hin zur technischen Erwartung reichen. Risiken sind durch Unternehmen aktiv zu mitigieren.

- Einrichtungen müssen **geeignete und verhältnismäßige technische, prozessuale und organisatorische Maßnahmen ergreifen.** Grundlage dafür ist ein nachvollziehbares Risikomanagement.
- Diese müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, **Sicherheitsvorfälle zu vermeiden oder zu minimieren.**
- Diese Maßnahmen müssen mindestens Folgendes umfassen, um Geldbußen zu vermeiden:
  - Governance, Incident Management, Continuity, Supply Chain Security, Asset Management, Sicherheitsmaßnahmen bei Erwerb und Instandhaltung, Cyberhygiene und Schulungen, Human Resources Security, Identity und Access Management, Authentifizierung, gesicherte Kommunikation, Kryptographie

Warum sollen Logistik-Unternehmen jetzt schon NIS-2 umsetzen?

Quelle: KPMG, Deutschland, 2023

Welche Bußgelder und Sanktionen drohen bei Verstößen?

Bei wesentlichen Einrichtungen sind Behörden befugt, Aufsichtsmaßnahmen durchzuführen, unter anderem: Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, regelmäßige und gezielte Sicherheits- oder Ad-hoc-Prüfungen.

Gegen wesentliche Einrichtungen (Essential Entities), die gegen Art. 21 oder 23 verstoßen, wird, je nachdem, welcher Betrag höher ist, eine Geldbuße mit einem Höchstbetrag von

- 10.000.000 EUR oder
- 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes

verhängt.

Zusätzlich können bei Datenschutz-Verstößen Strafen bis zu 10.000.000 EUR oder einem Höchstbetrag von 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes verhängt werden, je nachdem, welcher der Beträge höher ist.

Wie könnte eine beispielhafte Projektumsetzung mit KPMG aussehen?

Quelle: KPMG, Deutschland, 2023

Welche Chancen und welcher Nutzen ergeben sich für Unternehmen durch die Umsetzung?

Die Umsetzung von NIS-2 bietet die Chance, die Resilienz und den Schutz einer Einrichtung zu verbessern und gleichzeitig einen Beitrag zu einer sicheren und geschützten Zukunft zu leisten.

- Erhöhung des Cybersicherheitsniveaus
- Steigerung der guten Reputation und des Vertrauens
- Steigerung der Resilienz
- Steigerung der Konkurrenzfähigkeit
- Höhere Qualifikationsanforderungen bei Mitarbeitenden und Organen
- Schnellere Reaktionszeiten bei Vorfällen

Warum KPMG?

KPMG in Deutschland verfügt über mehr als 200 Cyber-Security-Expert:innen und hat über das Netzwerk der KPMG-Organisation unabhängiger Mitgliedsfirmen Zugang zu mehr als 6.000 Cyber-Security-Expert:innen weltweit. Innerhalb der letzten Jahre begleiteten wir erfolgreiche Cyber-Projekte in verschiedenen Branchen und an unterschiedlichen Standorten in Deutschland, unter anderem auch in der Transport- und Logistikbranche. Dadurch erhalten Sie Zugang zu Benchmarks und Best Practices aus Ihrer und anderen Branchen.

Kontakt

KPMG AG Wirtschaftsprüfungsgesellschaft

Klingelhöferstraße 18
10785 Berlin

Dr. Michael Falk
Partner, Consulting –
Cyber Security
mfalk@kpmg.com

Justina Stunzenaite
Managerin, Consulting –
Cyber Security
jstunzenaite@kpmg.com

Ulrich Balke
Director,
Markets
ubalke@kpmg.com

Dr. Steffen Wagner
Partner, Deal Advisory,
Head of Transport & Leisure
Head of Infrastructure
steffenwagner@kpmg.com

www.kpmg.de
www.kpmg.de/socialmedia