FOGLIA
Datenschutz & Informationssicherheit

Whitepaper

NIS-2-Betroffenheitsanalyse

Orientierung für Unternehmen zur Einordnung nach der NIS-2-Richtlinie

Inhalt

Hinweis zur Nutzung 2
1. Hintergrund: Was ist NIS-2? 2
2. Warum eine Betroffenheitsanalyse notwendig ist 3
3. Grundlogik der NIS-2-Betroffenheitsprüfung 3
3.1 Art der Einrichtung 3
3.2 Zuordnung zu Sektoren und Teilsektoren 3
3.3 Unternehmensgröße 4
3.4 Besonders wichtige und wichtige Einrichtungen 5
4. Vereinfachte Übersicht zur Einordnung 5
5. Ergebnisarten der Betroffenheitsprüfung 6
5.1 Nicht betroffen 6
5.2 Wichtige Einrichtung 6
5.3 Besonders wichtige Einrichtung 6
6. Grenzen der Betroffenheitsprüfung 7
7. Praxis-Checkliste: Erste Selbsteinschätzung 7
8. Ihr nächster sinnvoller Schritt 7
9. Über den Autor 8

Hinweis zur Nutzung

Dieses Whitepaper dient als **Orientierungs- und Entscheidungshilfe** zur ersten Einschätzung, ob ein Unternehmen vom Anwendungsbereich der NIS-2-Richtlinie erfasst sein kann. Es ersetzt **keine rechtlich verbindliche Selbstidentifizierung**, keine individuelle Rechtsberatung und keine behördliche Entscheidung.

Die Darstellung basiert auf:

- der EU-Richtlinie (EU) 2022/2555 (NIS-2),
- dem aktuellen Stand des deutschen NIS-2-Umsetzungsgesetzes (NIS2UmsuCG),
- sowie der öffentlich zugänglichen Betroffenheitsprüfung des Bundesamts für Sicherheit in der Informationstechnik (BSI).

1. Hintergrund: Was ist NIS-2?

Die NIS-2-Richtlinie (EU) 2022/2555 ist die Weiterentwicklung der bisherigen NIS-Richtlinie und verfolgt das Ziel, ein **einheitlich hohes Cybersicherheitsniveau innerhalb der Europäischen Union** sicherzustellen.

In Deutschland wird die Richtlinie durch das **NIS-2-Umsetzungsgesetz (NIS2UmsuCG)** in nationales Recht überführt. Mit dem Inkrafttreten werden deutlich mehr Unternehmen als bisher gesetzlichen Anforderungen an die Informationssicherheit unterliegen.

Gegenüber der bisherigen NIS-Richtlinie erweitert NIS-2 insbesondere:

- den **Anwendungsbereich** (mehr Sektoren, mehr Unternehmen),
- die **Pflichten zur Umsetzung von Sicherheitsmaßnahmen**,
- die **Verantwortung der Geschäftsleitung**,
- sowie die **Sanktions- und Aufsichtsbefugnisse** der Behörden.

Betroffene Unternehmen sind verpflichtet, angemessene **technische, organisatorische und personelle Maßnahmen** zur Informationssicherheit umzusetzen und erhebliche Sicherheitsvorfälle innerhalb definierter Fristen zu melden.

2. Warum eine Betroffenheitsanalyse notwendig ist

Die NIS-2 folgt dem Prinzip der **Selbstidentifizierung**. Unternehmen werden grundsätzlich **nicht aktiv** durch Behörden über ihre Betroffenheit informiert, sondern müssen eigenständig prüfen, ob sie unter den Anwendungsbereich fallen.

Zur Unterstützung stellt das BSI eine freiwillige NIS-2-Betroffenheitsprüfung zur Verfügung. Diese:

- erfolgt anonym,
- basiert auf gesetzlich definierten Kriterien,
- liefert eine Ersteinschätzung,
- ist rechtlich nicht bindend.

Die **Verantwortung für die korrekte Einordnung** verbleibt jedoch vollständig beim Unternehmen und damit bei der Geschäftsleitung.

3. Grundlogik der NIS-2-Betroffenheitsprüfung

Die Einordnung nach NIS-2 erfolgt entlang eines strukturierten Prüfschemas. Maßgeblich sind insbesondere die folgenden Kriterien.

3.1 Art der Einrichtung

Zunächst wird geprüft, ob es sich um eine private oder öffentliche Organisation handelt, die grundsätzlich in den Anwendungsbereich fällt. Einrichtungen der Bundes-, Landes- und Kommunalverwaltung werden in der BSI-Betroffenheitsprüfung regelmäßig nicht betrachtet, da sie gesonderten Regelungen unterliegen.

3.2 Zuordnung zu Sektoren und Teilsektoren

Die NIS-2-Richtlinie definiert in ihren **Anhängen I und II** eine Vielzahl besonders relevanter Sektoren und Teilsektoren, deren Funktionsfähigkeit von zentraler Bedeutung für Gesellschaft und Wirtschaft ist.

Beispiele sind:

- Energie
- Verkehr und Transport

- Gesundheit
- Wasser
- Digitale Infrastruktur
- Finanzwesen
- Abfallwirtschaft, Chemie, Lebensmittel
- Digitale Dienste und Forschung

Nur Unternehmen, die Tätigkeiten in diesen gesetzlich definierten Sektoren ausüben, können grundsätzlich vom Anwendungsbereich der NIS-2 erfasst sein.

3.3 Unternehmensgröße

Die Unternehmensgröße ist ein zentrales, jedoch **nicht allein entscheidendes** Kriterium der Betroffenheitsprüfung.

Die NIS-2 orientiert sich an der EU-KMU-Definition:

- **Mittlere Unternehmen**:
  ≥ 50 Mitarbeitende oder ≥ 10 Mio. € Jahresumsatz bzw. Bilanzsumme
- **Große Unternehmen**:
  ≥ 250 Mitarbeitende oder ≥ 50 Mio. € Jahresumsatz und ≥ 43 Mio. € Bilanzsumme

Eine Betroffenheit ergibt sich stets aus der **Kombination von Unternehmensgröße und Tätigkeit** in einem relevanten Sektor.

Grundsätze:

- Unternehmen außerhalb der definierten Sektoren sind unabhängig von ihrer Größe nicht betroffen.
- Mittlere und große Unternehmen können betroffen sein, sofern sie relevante Tätigkeiten ausüben.
- In bestimmten gesetzlich definierten Sonderfällen kann eine Betroffenheit unabhängig von der Größe bestehen.

Bei **verbundenen Unternehmen und Konzernstrukturen** sind die Größenkriterien auf Gruppenebene zu prüfen.

3.4 Besonders wichtige und wichtige Einrichtungen

Das deutsche Umsetzungsgesetz unterscheidet zwischen:

- **Besonders wichtigen Einrichtungen** (§ 28 Abs. 1 NIS2UmsuCG)
- **Wichtigen Einrichtungen** (§ 28 Abs. 2 NIS2UmsuCG)

Die konkrete Zuordnung erfolgt anhand der **Anlagen 1 und 2** des Gesetzes.

Besonders wichtige Einrichtungen sind Organisationen, deren Ausfall erhebliche Auswirkungen auf Gesellschaft, Wirtschaft oder Sicherheit hätte. Wichtige Einrichtungen erfüllen ebenfalls eine bedeutende Funktion, unterliegen jedoch einer etwas geringeren aufsichtsrechtlichen Intensität.

4. Vereinfachte Übersicht zur Einordnung

Kategorie	Unternehmensgröße	Tätigkeit / Sektor	Einordnung
Anlage-1-Sektoren (z. B. Energie, Verkehr, Gesundheit, Wasser, digitale Infrastruktur, Weltraum)	Großunternehmen	Tätigkeit im jeweiligen Sektor	Besonders wichtige Einrichtung
Anlage-1-Sektoren	Mittlere Unternehmen	Tätigkeit im jeweiligen Sektor	Wichtige Einrichtung
Anlage-2-Sektoren (z. B. Abfallwirtschaft, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Dienste, Forschung, Post/Kurier)	Mittlere oder große Unternehmen	Tätigkeit im jeweiligen Sektor	Wichtige Einrichtung
Qualifizierte Vertrauensdienste	Unabhängig von der Größe	Erbringung qualifizierter Vertrauensdienste	Besonders wichtige Einrichtung
DNS-Dienste, TLD-Registries, Root-Zonen	Unabhängig von der Größe	Betrieb gesetzlich definierter DNS-	Besonders wichtige

Kategorie	Unternehmensgröße	Tätigkeit / Sektor	Einordnung
		Funktionen	Einrichtung
Öffentliche TK-Netze	In der Regel unabhängig von der Größe	Betrieb öffentlicher TK-Netze	Besonders wichtige Einrichtung
Öffentliche TK-Dienste	Ab mittlerer Größe	Erbringung öffentlicher TK-Dienste	Wichtige Einrichtung
Betreiber Kritischer Anlagen (KRITIS)	Unabhängig von der Größe	KRITIS gemäß BSI-KritisV	Besonders wichtige Einrichtung

Diese Übersicht dient ausschließlich der Orientierung. Maßgeblich sind Gesetz und Anlagen.

5. Ergebnisarten der Betroffenheitsprüfung

5.1 Nicht betroffen

Auf Basis der Angaben ergibt sich keine unmittelbare Betroffenheit. Indirekte Anforderungen durch Kunden, Partner oder Lieferketten sind dennoch möglich.

5.2 Wichtige Einrichtung

Wichtige Einrichtungen unterliegen unter anderem:

- Pflichten zum Risikomanagement,
- Meldepflichten bei Sicherheitsvorfällen,
- Anforderungen an technische und organisatorische Maßnahmen.

5.3 Besonders wichtige Einrichtung

Besonders wichtige Einrichtungen unterliegen:

- erweiterten Sicherheitsanforderungen,

- intensiver behördlicher Aufsicht,
- einer besonderen Verantwortung der Geschäftsleitung (Genehmigungs-, Kontroll- und Schulungspflichten).

6. Grenzen der Betroffenheitsprüfung

Die Betroffenheitsprüfung:

- basiert auf Eigenangaben,
- entfaltet keine rechtliche Bindungswirkung,
- ersetzt keine vertiefte juristische Bewertung.

Insbesondere bei Mischkonstellationen, Konzernstrukturen oder ausgelagerten IT-Leistungen ist eine vertiefte Analyse erforderlich.

7. Praxis-Checkliste: Erste Selbsteinschätzung

Je mehr Fragen mit „Ja“ beantwortet werden, desto wahrscheinlicher ist eine Betroffenheit.

☐ ≥ 50 Mitarbeitende oder ≥ 10 Mio. € Umsatz
☐ Tätigkeit in einem NIS-2-Sektor
☐ Kritische IT für den Geschäftsbetrieb
☐ Abhängigkeit von IT- oder Cloud-Dienstleistern
☐ Kunden stellen Sicherheitsanforderungen

8. Ihr nächster sinnvoller Schritt

Bei Unsicherheit empfiehlt sich eine strukturierte Betroffenheitsanalyse mit:

- klarer rechtlicher Einordnung,
- nachvollziehbarer Dokumentation,
- konkreten Handlungsempfehlungen.

9. Über den Autor

Foglia Datenschutz & Informationssicherheit unterstützt Unternehmen, Praxen und Kommunen bei der pragmatischen Umsetzung regulatorischer Anforderungen im Bereich Datenschutz und Informationssicherheit.

Sensibilisierungsschulungen zur Prävention von Cyberkriminalität (z.B Phishing, Quishing und Social Engineering) sowie der richtige Umgang mit personenbezogenen Daten gemäß Datenschutzgrundverordnung (DSGVO), runden das Angebot ab.

Mehr Informationen über den Autor finden Sie auf der Homepage

www.foglia-datenschutz-informationssicherheit.de

oder per Kontaktaufnahme

info@foglia-datenschutz-informationssicherheit.de