

NIS2-Betroffenheit prüfen: Checkliste für den Mittelstand

In 15 Minuten klären, ob Ihr Unternehmen betroffen ist – und was dann gilt.

Die NIS2-Richtlinie erweitert die Pflichten zur Cybersicherheit deutlich – und trifft erstmals auch viele mittelständische Unternehmen, die sich bisher nicht angesprochen fühlten. Diese Checkliste führt Sie durch die drei Fragen, die über eine Betroffenheit entscheiden, und zeigt, welche Pflichten daraus folgen.

Kurz gesagt

Betroffen sind Sie, wenn alle drei Bedingungen zutreffen: Ihr Sektor steht in der Anlage der Richtlinie, Sie überschreiten die Größenschwelle, und Sie erbringen Ihre Leistung in der EU. Treffen zwei zu, lohnt die genaue Prüfung trotzdem – über Lieferketten geraten auch kleinere Unternehmen in die Pflicht.

Schritt 1: Gehört Ihr Sektor dazu?

- ☐ **Energie, Verkehr, Bankwesen, Finanzmarkt**
Klassische Sektoren mit hoher Kritikalität – hier gilt in der Regel die strengste Stufe.
- ☐ **Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur**
Dazu zählen auch Labore, Hersteller von Medizinprodukten und Rechenzentrumsdienste.
- ☐ **Öffentliche Verwaltung, Weltraum**
Kommunen und Stadtwerke fallen je nach Landesrecht und Aufgabe darunter.
- ☐ **Post- und Kurierdienste, Abfallwirtschaft, Chemie, Lebensmittel**
Sektoren der zweiten Anlage – „wichtige Einrichtungen“ mit etwas geringeren Auflagen.
- ☐ **Verarbeitendes Gewerbe: Medizinprodukte, Elektronik, Maschinenbau, Fahrzeugbau**
Dieser Punkt überrascht viele Mittelständler. Maschinenbau ist ausdrücklich genannt.
- ☐ **Digitale Dienste, Forschung**
Anbieter von Online-Marktplätzen, Suchmaschinen und sozialen Netzwerken, Forschungseinrichtungen.

Schritt 2: Überschreiten Sie die Größenschwelle?

- ☐ **50 oder mehr Beschäftigte**
Gezählt werden Vollzeitäquivalente inklusive verbundener Unternehmen.
- ☐ **Mehr als 10 Mio. Euro Jahresumsatz oder Bilanzsumme**
Es genügt eines der beiden Kriterien zusätzlich zur Beschäftigtenzahl.
- ☐ **Unabhängig von der Größe: Sie sind alleiniger Anbieter einer kritischen Leistung**
Dann greift die Richtlinie auch unterhalb der Schwellen.

Schritt 3: Wenn Sie betroffen sind – diese Pflichten kommen

- ☐ **Registrierung bei der zuständigen Behörde**
In Deutschland beim BSI, mit Frist nach Inkrafttreten der nationalen Umsetzung.
- ☐ **Risikomanagement für Cybersicherheit**
Richtlinien, Risikoanalyse, Maßnahmen und deren regelmäßige Überprüfung.
- ☐ **Meldepflicht bei Sicherheitsvorfällen**
Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht binnen eines Monats.
- ☐ **Business Continuity und Backup-Management**
Wiederanlaufpläne, getestete Rücksicherung, Krisenkommunikation.
- ☐ **Sicherheit in der Lieferkette**
Anforderungen an Dienstleister vertraglich verankern und prüfen.
- ☐ **Schulung und Nachweis**
Für die Geschäftsleitung ausdrücklich verpflichtend – inklusive persönlicher Haftung.
- ☐ **Einsatz von Kryptografie und Zugriffskontrolle**
Verschlüsselung, Mehr-Faktor-Authentifizierung, Rechtekonzept.

Was in der Praxis am häufigsten fehlt

Nach unserer Erfahrung aus Mandaten in Mittelfranken scheitert es selten am Willen, sondern an drei Punkten: Es gibt keine aktuelle Übersicht der Systeme und Dienstleister. Die Rücksicherung des Backups wurde nie unter Realbedingungen getestet. Und es existiert zwar Technik, aber kein Dokument, das einer Prüfung standhält.

Nächster Schritt

Die Betroffenheitsprüfung ist in der Regel an einem Vormittag erledigt. Wenn Sie wollen, machen wir sie gemeinsam im kostenfreien Erstgespräch – und Sie bekommen das Ergebnis schriftlich, unabhängig davon, ob Sie mit uns weiterarbeiten.