ÜBERSICHT: ENTGEHEN SIE DER HAFTUNGSFALLE NIS-2

Der regulatorische Rahmen: NIS-2 kommt – auch für den Mittelstand

Die NIS-2-Richtlinie der EU und das darauf aufbauende deutsche Umsetzungsgesetz – das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – markieren eine neue Ära der Cybersicherheitsregulierung. Die Richtlinie (EU) 2022/2555 ersetzt die bisherige NIS-Richtlinie aus dem Jahr 2016 und erweitert den Anwendungsbereich erheblich: Insgesamt 18 Wirtschaftssektoren werden direkt angesprochen.

Direkte Betroffenheit: Sind Sie dabei?

Direkt in den Anwendungsbereich fallen Unternehmen, die als „besonders wichtige" oder „wichtige Einrichtungen" klassifiziert werden. Maßgeblich sind Größe, Branche und gesellschaftliche Relevanz. Zu den direkt regulierten Sektoren gehören Energieversorgung, Gesundheitswesen, Wasserwirtschaft, Transportsektor, Finanzwirtschaft, digitale Infrastruktur und die öffentliche Verwaltung. **Auch wenn Ihr Unternehmen formal nicht zu den 30.000 direkt betroffenen Einrichtungen zählt, können Sie trotzdem in die Pflicht genommen werden. § 28 des deutschen BSI-Gesetzentwurfs nimmt zwar „vernachlässigbare" Tätigkeiten aus dem Anwendungsbereich aus – definiert diesen Begriff jedoch nicht. Unternehmen mit einer regulierten Nebentätigkeit (z. B. digitale Dienstleistungen neben dem klassischen Außenhandel) können in den Anwendungsbereich fallen, obwohl ihre Hauptgeschäftstätigkeit nicht reguliert ist.**

In Deutschland werden insgesamt etwa 30.000 Unternehmen als direkt betroffen eingestuft.

Prüfen Sie für Ihr Unternehmen, ob Sie:

- digitale Dienste für Kunden bereitstellen (z. B. Online-Plattformen für Bestellabwicklung)
- Teil einer kritischen Lieferkette sind (z. B. Zulieferer für Unternehmen der Energie- oder Gesundheitsbranche)
- IT-Dienstleistungen für kritisch eingestufte Sektoren erbringen oder empfangen

Fällt Ihr Unternehmen in eine dieser Kategorien, droht bei Nichterfüllung der Pflichten sofortige bußgeldbewehrte Compliance – ohne Übergangsfrist.

Indirekte Betroffenheit: Der Druck aus der Lieferkette

Auch wer formal nicht zur Zielgruppe gehört, gerät unter Druck – sobald größere Geschäftspartner NIS-2-pflichtig sind. Die Richtlinie verpflichtet betroffene Unternehmen, ihre Lieferketten systematisch zu analysieren und sicherzustellen, dass externe Partner angemessene Sicherheitsstandards einhalten.

Konkret bedeutet das für Außenhandelsunternehmen: Ihre Kunden und Auftraggeber werden Sicherheitsanforderungen vertraglich weitergeben, Audits einfordern und im Zweifel den Lieferanten wechseln, der nicht nachweislich NIS-2-konform arbeitet. Besonders betroffen sind:

- **Logistikunternehmen**, die essenzielle Dienstleistungen für regulierte Sektoren wie Energie, Gesundheit oder Lebensmittel erbringen
- **Maschinenbauer und Komponentenhersteller**, die in globale Lieferketten eingebunden sind und für NIS-2-pflichtige Industrieunternehmen produzieren
- **IT-Dienstleister und Cloud-Anbieter**, die die technische Basis für betroffene Organisationen stellen
- **Handelsunternehmen**, die ERP-Systeme oder digitale Plattformen nutzen und mit kritischen Sektoren kooperieren – etwa im Großhandel für medizinische Geräte oder Chemikalien

Risikomanagement: Was das Gesetz konkret fordert

Direkt betroffene Unternehmen müssen ein umfassendes Risikomanagementsystem für ihre IT-Infrastruktur einführen. Zu den Pflichtmaßnahmen gehören:

- Durchführung von Risikoanalysen und regelmäßige Evaluierung der IT-Sicherheitsstrategie
- Einführung von Zugangskontrollsystemen, Verschlüsselungstechnologien und Sicherheitsüberprüfungen von Drittanbietern
- Erstellung und Pflege von Notfall- und Wiederherstellungsplänen
- Einbindung externer Dienstleister (Cloud, Logistik, Wartung) in das Risikomanagement

Die Meldepflichten bei Sicherheitsvorfällen sind gestuft: Innerhalb von 24 Stunden ist eine Erstmeldung zu erstatten, nach 72 Stunden ein Zwischenbericht, spätestens nach einem Monat ein Abschlussbericht.

Führen Sie frühzeitig ein Informationssicherheits-Managementsystem (ISMS) ein – auch wenn Ihr Unternehmen formal nicht direkt betroffen ist. Ein ISMS hilft Ihnen, Ihre Risikolage systematisch zu erfassen, Lieferantenbeziehungen vertraglich abzusichern und im Fall eines Kundenaudits nachweisbare Compliance vorweisen zu können. Nutzen Sie dafür anerkannte Normen wie ISO/IEC 27001 als Orientierungsrahmen.

Managementverantwortung und Sanktionen: Persönliche Haftung der Geschäftsführung

Die NIS-2-Richtlinie verankert die Verantwortung für Cybersicherheit ausdrücklich auf Ebene der Unternehmensleitung. Geschäftsführende Organe sind verpflichtet, die Einhaltung der Sicherheitsvorgaben aktiv zu überwachen, sich regelmäßig zu IT-Sicherheitsthemen fortzubilden und interne Kontrollmechanismen einzurichten. Bei grober Fahrlässigkeit oder unterlassener Aufsicht haften Geschäftsführer **persönlich**.

Das geplante Sanktionsregime ist gestaffelt: Bei besonders gravierenden Verstößen drohen Bußgelder in Millionenhöhe. Das BSI erhält erweiterte Befugnisse – darunter das Recht auf Vor-Ort-Prüfungen, die Anordnung von Sicherheitsmaßnahmen und die öffentliche Bekanntmachung von Sicherheitsmängeln.

Handlungsempfehlungen für Ihr Unternehmen

Prüfen Sie Ihren Status: Bewerten Sie anhand der NIS-2-Sektoren und der gesetzlichen Schwellenwerte (Umsatz, Mitarbeiterzahl), ob Ihr Unternehmen direkt betroffen ist. Analysieren Sie gleichzeitig Ihre Lieferkette: Sind Sie wesentlicher Lieferant für eine regulierte Einrichtung?

Erhöhen Sie Ihr IT-Sicherheitsniveau: Führen Sie ein ISMS ein, erstellen Sie einen Notfallplan und etablieren Sie technische Maßnahmen wie Backup-Strategien, Verschlüsselung und sichere Kommunikation.

Sichern Sie Ihre Lieferantenbeziehungen vertraglich ab: Passen Sie Ihre Verträge mit IT-Dienstleistern und Cloud-Anbietern an und dokumentieren Sie die Risikoklassifizierung Ihrer Lieferanten im ISMS.

Bereiten Sie Meldeprozesse vor: Definieren Sie interne Prozesse zur Erkennung und Meldung von Sicherheitsvorfällen, schulen Sie Ihre Mitarbeitenden und legen Sie klare Zuständigkeiten fest.