NIS2-Richtlinie

Was österreichische Unternehmer jetzt wissen müssen.

Die Grundlagen verstehen: Was ist NIS2 und warum betrifft es Sie?

Die NIS2-Richtlinie ist Europas Antwort auf die dramatisch gestiegenen Cyberbedrohungen der letzten Jahre. Stellen Sie sich vor, Ihr Unternehmen wäre Teil eines europaweiten Sicherheitsnetzes, das kritische Infrastrukturen und wichtige Wirtschaftszweige vor Cyberangriffen schützt. Genau das bewirkt diese EU-Richtlinie vom 14. Dezember 2022. Sie ersetzt die ursprüngliche NIS-Richtlinie von 2016 und erweitert den Schutzbereich erheblich – von wenigen tausend auf über 160.000 Unternehmen europaweit.

Bin ich betroffen? Die entscheidenden Kriterien

Die Betroffenheit folgt einem klaren System. Zunächst prüfen Sie Ihren Sektor:
Energie, Verkehr, Finanzwesen, Gesundheit, Trinkwasser, digitale Infrastruktur, öffentliche Verwaltung gelten als „wesentliche Einrichtungen". Post, Abfall, Lebensmittel, verarbeitendes Gewerbe und digitale Dienste fallen unter „wichtige Einrichtungen".

Der entscheidende zweite Faktor ist Ihre Unternehmensgröße. Mittlere Unternehmen mit mindestens 50 Mitarbeitern oder über 10 Millionen Euro Jahresumsatz sind erfasst. Große Unternehmen mit über 250 Mitarbeitern oder mehr als 50 Millionen Euro Umsatz fallen automatisch darunter. Eine wichtige Ausnahme: Kleine Unternehmen unter 50 Mitarbeitern und 10 Millionen Euro Umsatz sind grundsätzlich ausgenommen, es sei denn, sie sind Telekommunikationsanbieter oder DNS-Dienstleister.

Die aktuelle Lage in Österreich: Verzögerung mit Konsequenzen

Hier wird die Situation komplex. Österreich hätte die Richtlinie bis 17. Oktober 2024 umsetzen müssen, doch das nationale Umsetzungsgesetz NISG 2025 ist noch nicht verabschiedet.
Der erste Entwurf wurde im Februar 2024 abgelehnt, ein Initiativantrag für den 1. Juni 2025 scheiterte an der notwendigen Zweidrittelmehrheit. Die EU-Kommission hat bereits ein Vertragsverletzungsverfahren eingeleitet. Diese Verzögerung schafft eine paradoxe Situation: Rechtlich könnten bereits jetzt einzelne Bestimmungen der EU-Richtlinie unmittelbar anwendbar sein, während gleichzeitig das österreichische Vollzugsrecht fehlt. Für Sie als Unternehmer bedeutet das erhöhte Rechtsunsicherheit, aber auch zusätzliche Vorbereitungszeit.

TOMORIS GmbH | Saturnstraße 1, 4614 Marchtrenk | www.tomoris.com | contact@tomoris.com | +43 7243 53091

Ihre Pflichten: Was konkret von Ihnen erwartet wird

Die NIS2-Anforderungen lassen sich in vier Kernbereiche gliedern. Erstens: Risikomanagement wird zur Chefsache. Die Geschäftsleitung trägt persönliche Verantwortung für die Cybersicherheit und muss regelmäßige Risikoanalysen durchführen lassen. Zweitens: Technische Schutzmaßnahmen umfassen Firewalls, Verschlüsselung, Zugriffskontrollen und regelmäßige Sicherheitsupdates. Drittens: Organisatorische Maßnahmen erfordern Sicherheitsrichtlinien, Mitarbeiterschulungen und Notfallpläne. Viertens: Meldepflichten verpflichten Sie, erhebliche Sicherheitsvorfälle binnen 24 Stunden den Behörden zu melden. Besonders wichtig ist die Lieferkettensicherheit – Sie müssen auch die Cybersicherheit Ihrer wichtigsten Dienstleister und Lieferanten bewerten und sicherstellen.

Sanktionen: Die finanziellen Konsequenzen verstehen

Die Strafrahmen sind beträchtlich und sollen echte Anreize zur Compliance schaffen. Wesentliche Einrichtungen riskieren bei Verstößen bis zu zehn Millionen Euro oder zwei Prozent ihres weltweiten Jahresumsatzes – je nachdem, welcher Betrag höher ist. Wichtige Einrichtungen können mit bis zu sieben Millionen Euro oder 1,4 Prozent des Umsatzes bestraft werden. Für administrative Verstöße wie verspätete Registrierung sind niedrigere Strafen von 50.000 bis 100.000 Euro vorgesehen. Diese Summen verdeutlichen: NIS2 ist keine bürokratische Übung, sondern ein ernsthaftes Sicherheitsprogramm mit entsprechenden Konsequenzen.

Praktische Schritte: Ihr Fahrplan zur Compliance

Beginnen Sie mit einer ehrlichen Bestandsaufnahme Ihrer aktuellen Cybersicherheit. Führen Sie eine Gap-Analyse durch: Wo stehen Sie heute, wo müssen Sie hin? Entwickeln Sie daraufhin einen strukturierten Implementierungsplan mit realistischen Zeiträumen und Budgets. Investieren Sie in Mitarbeiterschulungen – der Mensch bleibt oft das schwächste Glied in der Sicherheitskette. Dokumentieren Sie alle Maßnahmen sorgfältig, denn bei Prüfungen müssen Sie nachweisen können, was Sie unternommen haben. Etablieren Sie Prozesse für die Incident Response und üben Sie diese regelmäßig. Vergessen Sie nicht die Lieferantenbewertung – erstellen Sie eine Liste kritischer Dienstleister und bewerten Sie deren Sicherheitsstandards.

Zeitmanagement: Warum jetzt handeln trotz Rechtsunsicherheit

Die verzögerte österreichische Umsetzung ist paradoxerweise ein Vorteil für vorausschauende Unternehmer. Sie haben zusätzliche Zeit für eine durchdachte, schrittweise Implementierung statt hektischer Last-Minute-Maßnahmen. Die Grundprinzipien der EU-Richtlinie stehen fest und werden sich in der österreichischen Fassung nicht grundlegend ändern. Cybersicherheitsinvestitionen zahlen sich unabhängig von regulatorischen Anforderungen aus – sie schützen vor realen Bedrohungen, die täglich zunehmen. Ein strukturierter Ansatz jetzt erspart Ihnen Stress und Kosten später.

Registrierung und Compliance-Management

Sobald das österreichische Gesetz in Kraft tritt, haben betroffene Unternehmen drei Monate Zeit für die Registrierung bei der zuständigen Behörde. Nutzen Sie diese Frist weise und bereiten Sie alle notwendigen Unterlagen vor. Entwickeln Sie ein Compliance-Management-System, das kontinuierliche Überwachung und Verbesserung ermöglicht. NIS2-Compliance ist kein einmaliges Projekt, sondern ein dauerhafter Prozess der organisatorischen Reifung.

TOMORIS GmbH | Saturnstraße 1, 4614 Marchtrenk | www.tomoris.com | contact@tomoris.com | +43 7243 53091

Fazit: Chance statt Belastung

Betrachten Sie NIS2 nicht als bürokratisches Hindernis, sondern als Modernisierungsimpuls für Ihr Unternehmen. Robuste Cybersicherheit stärkt das Kundenvertrauen, schützt Geschäftsgeheimnisse und kann zum Wettbewerbsvorteil werden. Die aktuelle Rechtslage in Österreich gibt Ihnen die seltene Gelegenheit, sich in Ruhe und systematisch vorzubereiten. Nutzen Sie diese Zeit weise – Ihre zukünftige Geschäftssicherheit hängt davon ab.

TOMORIS GmbH – Ihr Partner für strukturierte NIS2-Compliance
Wir begleiten Sie durch alle Phasen der NIS2-Umsetzung – von der Bestandsanalyse bis zur dauerhaften Compliance.

www.tomoris.com/kontakt

www.tomoris.com/nis2-check