

NIS2 für Scaleups

Die NIS2-Checkliste für Founder & CEOs: von der Betroffenheit bis zur Meldefähigkeit

Für Scaleups ist NIS2 kein fernes Konzerntema, sondern eine **konkrete Pflicht mit Chefsache-Charakter**. Sobald ein wachsendes Unternehmen in einem betroffenen Sektor die Größenschwellen erreicht, greifen technische, organisatorische und persönliche Pflichten, in Deutschland geregelt über das **NIS2-Umsetzungsgesetz (NIS2UmsuCG)**. Entscheidend ist die Frage, ob und wie früh ein Scaleup betroffen ist.

In diesen vier Situationen wird NIS2 für Scaleups kritisch:

BETROFFENHEIT & SEKTOR

Wann NIS2 greift

- Besonders wichtige vs. wichtige Einrichtungen unterscheiden
- Grobe Schwelle: rund 50 Beschäftigte oder 10 Mio. Euro Umsatz
- Schnell wachsende B2B-Tech-Firmen fallen oft früh darunter
- Betroffenheit früh und dokumentiert klären

RISIKOMANAGEMENT

Technische & organisatorische Pflichten

- Risikoanalyse, Zugriffskontrolle, Lieferkette, Backup, Notfallkonzept
- Maßnahmen nachweisbar dokumentieren
- Sicherheitsprozesse mit dem Wachstum mitskalieren
- Nachweise für Behörden und Kunden bereithalten

MELDUNG & REGISTRIERUNG

Fristen sicher einhalten

- Erhebliche Vorfälle mehrstufig an die Behörde melden
- Erstmeldung sehr kurzfristig, danach Folgemeldungen
- Einrichtung fristgerecht registrieren
- Meldeprozess vorab aufsetzen, nicht erst im Ernstfall

GESCHÄFTSFÜHRUNG

Haftung der Leitungsebene

- GF muss Risikomaßnahmen billigen und überwachen
- Schulungspflicht für die Leitungsebene
- Verstöße können persönlich relevant werden
- Cybersicherheit wird zur Chefsache



~50 / 10 Mio.

Beschäftigte bzw. Euro Umsatz als grobe Größenschwelle in betroffenen Sektoren

Mehrstufig

Meldepflicht bei erheblichen Vorfällen: erst kurzfristig, dann Folgemeldungen

Chefsache

Leitungsorgane haften für Umsetzung und Überwachung der Risikomaßnahmen

NIS2-Readiness in 6 Schritten

Eine pragmatische Reihenfolge für wachsende Unternehmen im DACH-Raum: von der Betroffenheitsprüfung bis zur Meldefähigkeit.

SCHRITT 01

Betroffenheit klären

- ☐ Sektor-Einordnung prüfen (z. B. digitale Dienste, IT, Cloud, SaaS)
- ☐ Größenmerkmale gegen die Schwellen abgleichen, inkl. Wachstumsprognose
- ☐ Einstufung ableiten: wichtige vs. besonders wichtige Einrichtung
- ☐ Konzernstruktur und Tochtergesellschaften mitprüfen
- ☐ Betroffenheit bei Unsicherheit fachlich gegenprüfen und festhalten

SCHRITT 02

Registrierung vorbereiten

- ☐ Zuständige Behörde und Meldewege identifizieren
- ☐ Kontaktstelle und Verantwortliche benennen
- ☐ Stammdaten der Einrichtung zusammenstellen
- ☐ Registrierungsfristen im Kalender verankern
- ☐ Änderungen an Stammdaten laufend aktuell halten

SCHRITT 03

Risiken analysieren

- ☐ Kritische Assets und Datenflüsse erfassen
- ☐ Bedrohungen und Schwachstellen je Asset bewerten
- ☐ Risiken nach Eintritt und Schaden priorisieren
- ☐ Maßnahmen ableiten und Verantwortliche zuordnen
- ☐ Ergebnis als nachvollziehbares Risikoregister führen

SCHRITT 04

Maßnahmen umsetzen

- ☐ Zugriffskontrolle, MFA und Härtung etablieren
- ☐ Backups, Verschlüsselung und Patch-Prozesse aufsetzen
- ☐ Lieferkette und Dienstleister-Risiken adressieren
- ☐ Business Continuity und Notfallpläne festlegen
- ☐ Maßnahmen als verbindliche Richtlinien dokumentieren

SCHRITT 05

Vorfälle & Meldung

- ☐ Incident-Response-Prozess definieren und testen
- ☐ Meldekette und Eskalationsstufen festlegen
- ☐ Fristen für Erst-, Folge- und Abschlussmeldung kennen
- ☐ Vorlagen für Erst- und Folgemeldungen vorbereiten
- ☐ Verantwortlichkeiten für den Ernstfall klären

SCHRITT 06

Leitung & Schulung

- ☐ Geschäftsführung in Risikomaßnahmen einbinden
- ☐ Billigung und Überwachung dokumentieren
- ☐ Schulungen für Leitung und Team einplanen
- ☐ Wirksamkeit der Maßnahmen regelmäßig prüfen
- ☐ Reviews und Nachbesserungen fest verankern

Häufige Stolperfallen und Quick Wins

Was Scaleups bei NIS2 typischerweise unterschätzen, und womit sich früh Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

Betroffenheit zu spät geprüft

- ☐ **Annahme** »zu jung für NIS2« ungeprüft übernommen, statt sie sauber zu belegen
- ☐ **Größenschwelle** bei schnellem Wachstum früher erreicht als im Team gedacht
- ☐ **Betroffenheit** erst durch eine Kundenanfrage oder ein Audit bemerkt
- ☐ **Frühe, dokumentierte Einordnung** spart später Hektik und Nacharbeit

QUICK WIN 01

Dokumentation zentralisieren

- ☐ **Richtlinien und Nachweise** an einem zentralen, auffindbaren Ort bündeln
- ☐ **Strukturiert und versioniert** ablegen, statt später mühsam zu sammeln
- ☐ **Verantwortliche** und Review-Zyklen je Dokument festlegen
- ☐ **Audits und Kundenfragen** lassen sich so spürbar schneller beantworten

STOLPERFALLE 02

Lieferkette ignoriert

- ☐ **Sub-Dienstleister** und der genutzte Cloud-Stack im Risiko unterschätzt
- ☐ **Sicherheitsanforderungen** nicht vertraglich mit Dienstleistern verankert
- ☐ **Keine Übersicht**, welche Abhängigkeiten wirklich geschäftskritisch sind
- ☐ **Kundenanforderungen** aus deren NIS2-Pflicht schlagen auf das Scaleup durch

QUICK WIN 02

Synergien mit ISO 27001

- ☐ **Überlappung**: viele NIS2-Maßnahmen decken sich mit den ISO-27001-Controls
- ☐ **Ein einmal aufgebautes ISMS** deckt beide Welten weitgehend gemeinsam ab
- ☐ **Bestehende Controls** gezielt auf die NIS2-Anforderungen mappen
- ☐ **Doppelarbeit** vermeiden und den Umsetzungsaufwand spürbar bündeln

STOLPERFALLE 03

Kein Meldeprozess

- ☐ **Meldekette** im Vorfall unklar, niemand weiß, wer zuerst zu informieren ist
- ☐ **Zuständigkeiten** und Vertretung für Meldungen vorab nicht benannt
- ☐ **Enge Meldefristen** werden im Ernstfall unter Zeitdruck verpasst
- ☐ **Vorbereitete Vorlagen** und ein klarer Ablauf entschärfen den Ernstfall

QUICK WIN 03

Früh einordnen lassen

- ☐ **Betroffenheit und Einstufung** fachlich gegenprüfen lassen, statt zu raten
- ☐ **Maßnahmen** nach Wirkung und Aufwand statt nach Bauchgefühl priorisieren
- ☐ **Readiness-Roadmap** mit klaren Meilensteinen realistisch aufsetzen
- ☐ **Von diffuser Unsicherheit** zu planbarer, nachweisbarer Readiness kommen



Mit SECJUR zu 100 % NIS2-Compliance

Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

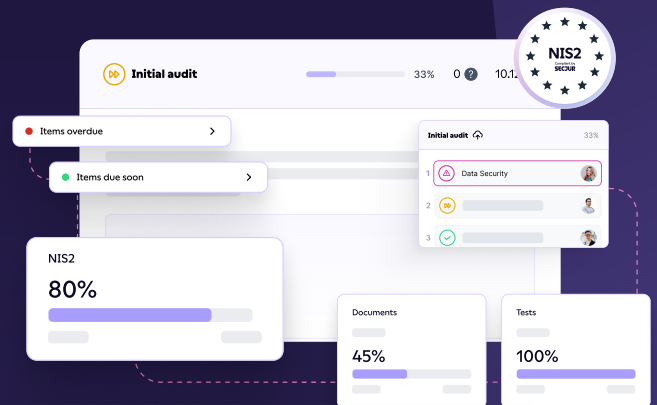
Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- ✓ Aufbau und Betrieb eines NIS2-konformen ISMS inkl. Risiko- und Incident-Management
- ✓ Klare Verantwortlichkeiten, Dokumentation und Nachweise für Behörden
- ✓ Profitieren Sie von der dedizierten Erfahrung unserer TÜV-geprüften Expert:innen

Reduzieren Sie manuellen Aufwand deutlich, gewinnen Transparenz über Ihren Compliance-Status und schaffen eine belastbare Grundlage für regulatorische Prüfungen und anspruchsvolle Kundenanforderungen.

Für unsere Bestandskunden bieten wir attraktive Konditionen, um frühzeitig Klarheit zu schaffen und NIS2-Readiness planbar umzusetzen.

→ [Jetzt informieren](#)



Mit SECJUR zu Informationssicherheitszertifizierungen:

“Dank Kundenvertrauen auf die Financial-Times-1000-Liste”



René Schluß
Founder & Managing
Director, reanmo



FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR



www.secjur.com