

NIS2 für Startups

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

Für Startups fühlt sich NIS2 schnell wie ein Konzernthema an, doch das täuscht. Wer in einem betroffenen Sektor arbeitet oder an regulierte Kunden liefert, gerät oft **früher in den Anwendungsbereich als gedacht**. Sobald die Größenschwellen erreicht sind, greifen technische, organisatorische und persönliche Pflichten, in Deutschland geregelt über das **NIS2-Umsetzungsgesetz (NIS2UmsuCG)**. Entscheidend ist die Frage, ob und wie früh ein Startup betroffen ist.

In diesen vier Situationen wird NIS2 für Startups kritisch:

BETROFFENHEIT & SEKTOR

Wann NIS2 greift

- Besonders wichtige vs. wichtige Einrichtungen unterscheiden
- Grobe Schwelle: rund 50 Beschäftigte oder 10 Mio. Euro Umsatz
- Junge B2B-Tech- und SaaS-Startups fallen oft früher darunter als gedacht
- Betroffenheit früh und dokumentiert klären

ENTERPRISE-VERTRIEB

NIS2 als Deal-Kriterium

- Enterprise- und regulierte Kunden geben NIS2-Pflichten über die Lieferkette weiter
- Sicherheitsfragebögen und Vertragsklauseln landen beim Startup
- Nachweisbare Sicherheit wird zum Vertriebsvorteil
- Ohne Nachweise droht das Aus in der Vorqualifizierung

RISIKOMANAGEMENT & MELDUNG

Pflichten ab Tag eins

- Technische und organisatorische Maßnahmen nachweisbar umsetzen
- Erhebliche Vorfälle mehrstufig an die Behörde melden
- Einrichtung fristgerecht registrieren
- Meldeprozess vorab aufsetzen, nicht erst im Ernstfall

GRÜNDER-HAFTUNG

Chefsache im jungen Team

- Geschäftsführung muss Risikomaßnahmen billigen und überwachen
- Schulungspflicht für die Leitungsebene
- Verstöße können persönlich relevant werden
- Cybersicherheit ist Chefsache, auch bei schlanken Strukturen



~50 / 10 Mio.

Beschäftigte bzw. Euro Umsatz als grobe Größenschwelle in betroffenen Sektoren

Lieferkette

Enterprise- und regulierte Kunden geben NIS2-Anforderungen an Startups weiter

Chefsache

Leitungsorgane haften für Umsetzung und Überwachung der Risikomaßnahmen

NIS2-Readiness in 6 Schritten

Eine pragmatische Reihenfolge für junge, schnell wachsende Unternehmen: 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
- ☐ Betroffenheit über regulierte Kunden und Lieferkette mitprüfen
- ☐ Einstufung ableiten: wichtige vs. besonders wichtige Einrichtung
- ☐ Ergebnis 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, Daten und Cloud-Dienste erfassen
- ☐ Bedrohungen und Schwachstellen bewerten
- ☐ Risiken nach Eintritt und Schaden priorisieren
- ☐ Maßnahmen ableiten und Verantwortliche zuordnen
- ☐ Ergebnis als nachvollziehbares Risikoregister führen

SCHRITT 04

Maßnahmen umsetzen

- ☐ Zugriffskontrolle, MFA und Härting etablieren
- ☐ Backups, Verschlüsselung und Patch-Prozesse aufsetzen
- ☐ Sichere Entwicklung und CI/CD-Zugänge absichern
- ☐ Lieferketten- und Dienstleister-Risiken adressieren
- ☐ 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 Startups bei NIS2 typischerweise unterschätzen, und womit sich früh Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

»Zu klein für NIS2«

- ☐ Annahme »zu jung oder zu klein für NIS2« ungeprüft übernommen
- ☐ Schwelle bei schnellem Wachstum früher erreicht als gedacht
- ☐ Betroffenheit erst bei Kundenanfrage oder Audit bemerkt
- ☐ Frühe, dokumentierte Einordnung spart später Hektik

QUICK WIN 01

Dokumentation zentralisieren

- ☐ Richtlinien und Nachweise von Anfang an an einem Ort bündeln
- ☐ Strukturiert und versioniert ablegen, statt später zu sammeln
- ☐ Verantwortliche je Dokument festlegen
- ☐ Audits und Kundenfragen später leichter beantworten

STOLPERFALLE 02

Lieferkette ignoriert

- ☐ Eigene Sub-Dienstleister und Cloud-Stack unterschätzt
- ☐ Sicherheitsanforderungen nicht vertraglich verankert
- ☐ Keine Übersicht über kritische Abhängigkeiten
- ☐ Kundenanforderungen schlagen direkt auf das Startup durch

QUICK WIN 02

Synergien mit ISO 27001

- ☐ Überlappung: viele NIS2-Maßnahmen decken sich mit den ISO-27001-Controls
- ☐ Ein ISMS deckt beide Welten weitgehend gemeinsam ab
- ☐ Bestehende Controls gezielt auf NIS2 mappen
- ☐ Doppelarbeit vermeiden, Aufwand bündeln

STOLPERFALLE 03

Kein Meldeprozess

- ☐ Meldekette im Vorfall unklar, niemand weiß, wer zuerst informiert
- ☐ Zuständigkeiten für Meldungen vorab nicht benannt
- ☐ Enge Meldefristen werden unter Druck verpasst
- ☐ Vorbereitete Vorlagen entschärfen den Ernstfall

QUICK WIN 03

Sicherheit als Vertriebsvorteil

- ☐ Nachweisbare Compliance öffnet die Tür zu Enterprise-Kunden
- ☐ Security wird vom Kostenfaktor zum echten Differenzierer
- ☐ Zertifikate und Nachweise verkürzen Vendor-Assessments
- ☐ Von Unsicherheit zu planbarer, nachweisbarer Readiness



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.

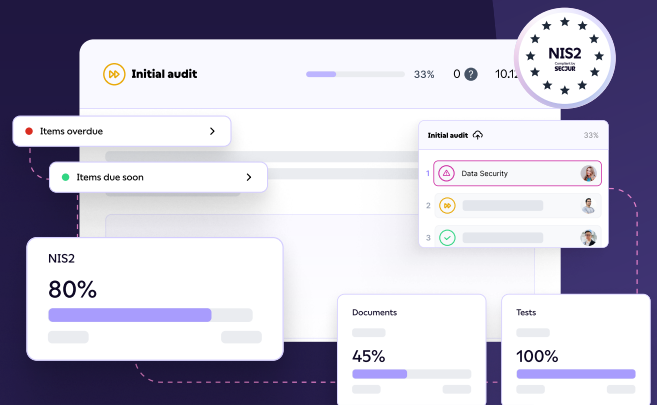
Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- ✓ 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:

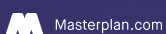
“Dank Kundenvertrauen auf die Financial-Times-1000-Liste”



René Schlöß
Founder & Managing
Director, reanmo



FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR



www.secjur.com