// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

NIS2 / NISG 2026: Auch ohne direkte Pflicht relevant für KMU?

NISG 2026 bringt NIS2 nach Österreich. Warum das Gesetz für viele KMU nicht direkt gilt – für Geschäftsführer aber trotzdem jetzt relevant ist.

AUTOR
Natascha Reiner

VERÖFFENTLICHT
28. April 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/nis2-nisg-2026-oesterreich-kmu/

Viele Geschäftsführer in Österreich hören derzeit zum ersten Mal von NIS2 oder dem neuen NISG 2026 — meist im Kontext großer Konzerne, kritischer Infrastruktur oder neuer EU-Vorgaben. Das klingt auf den ersten Blick nach einem Thema für Energieversorger, Banken und Ministerien. Für den Großteil österreichischer Unternehmen wirkt es weit weg.

Ganz so einfach ist es nicht.

Denn auch wenn das neue Netz- und Informationssystemsicherheitsgesetz (NISG 2026) viele kleine Unternehmen nicht direkt gesetzlich verpflichtet, verändert es dennoch die Spielregeln für Cybersicherheit in Österreich spürbar. Nicht primär über Strafen. Sondern über Haftung, Lieferketten, Kundenerwartung und die Frage, wie belastbar ein Unternehmen digital tatsächlich aufgestellt ist.

Genau dort wird das Thema für Geschäftsführer relevant.

Was ist NIS2 – und warum betrifft das Österreich jetzt?

Mit der NIS2-Richtlinie hat die Europäische Union den regulatorischen Rahmen für Cybersicherheit deutlich verschärft. Ziel ist ein einheitlich höheres Sicherheitsniveau für Netz- und Informationssysteme innerhalb der EU — insbesondere in kritischen und digital stark vernetzten Sektoren.

Die Richtlinie selbst ist europäisches Recht. In Österreich erfolgt die nationale Umsetzung über das neue NISG 2026, das das bisherige NISG 2018 ablöst. Das Gesetz wurde Ende 2025 kundgemacht und tritt mit 1. Oktober 2026 in Kraft. Damit entsteht in Österreich erstmals ein deutlich breiteres und verbindlicheres Cybersicherheitsregime für Unternehmen.

Das ist ein klarer Bruch mit der bisherigen Realität: Unter dem NISG 2018 waren nur vergleichsweise wenige Unternehmen direkt erfasst. Mit NISG 2026 erweitert sich dieser Kreis massiv.

Was sich mit NISG 2026 tatsächlich ändert

Die wichtigste Veränderung ist nicht technischer Natur. Sie ist organisatorisch.

Cybersicherheit wird mit NISG 2026 nicht länger als rein operative IT-Aufgabe behandelt, sondern ausdrücklich zur Führungsaufgabe. Das ist die eigentliche Zäsur.

Geschäftsführer betroffener Unternehmen müssen Sicherheitsmaßnahmen künftig nicht nur umsetzen lassen, sondern aktiv billigen, überwachen und nachvollziehbar dokumentieren. Die Verantwortung wandert damit aus der IT-Abteilung direkt in die Geschäftsführung.

Das ist der eigentliche Kern von NIS2: Cybersicherheit ist nicht mehr nur Technik. Sie ist Governance.

Sind österreichische KMU überhaupt direkt betroffen?

Für die meisten klassischen kleinen Unternehmen: **nein, nicht direkt**.

Das ist die wichtigste Einordnung in der gesamten Debatte.

Der Großteil österreichischer EPUs, kleiner Dienstleister, Agenturen, Handwerksbetriebe oder lokaler Handelsunternehmen fällt nicht unmittelbar unter das NISG 2026. Die direkte Betroffenheit setzt in der Regel voraus, dass ein Unternehmen:

1. in einem regulierten bzw. kritischen Sektor tätig ist und
2. eine gewisse Unternehmensgröße erreicht.

Für viele kleine Unternehmen ist beides schlicht nicht gegeben.

Wer als lokaler Betrieb, kleines Beratungsunternehmen oder klassischer Gewerbebetrieb unterwegs ist, wird mit hoher Wahrscheinlichkeit nicht direkt registrierungspflichtig.

Das bedeutet aber nicht, dass das Thema irrelevant ist.

Warum das Thema für kleine Unternehmen trotzdem relevant ist

Für viele KMU kommt NIS2 nicht über das Gesetz. Sondern über den Markt.

Das ist der entscheidende Punkt.

Denn größere Unternehmen, die direkt unter NISG 2026 fallen, müssen ihre Lieferketten absichern. Genau dadurch wandert das Thema in Richtung kleiner Zulieferer, Dienstleister und Partner weiter.

Das bedeutet in der Praxis:

- größere Kunden verlangen Sicherheitsnachweise
- Ausschreibungen setzen Mindeststandards voraus
- IT-Dienstleister müssen Sicherheitsprozesse dokumentieren
- Versicherer erwarten technische Mindestmaßnahmen
- Partner prüfen Zugriffe, Datenflüsse und Ausfallsicherheit

Das Gesetz trifft viele kleine Unternehmen nicht direkt. Die Marktwirkung trifft sie trotzdem.

Wer künftig mit größeren Kunden arbeiten will, wird immer öfter zeigen müssen, dass Zugriffe, Daten, Backups und Prozesse sauber abgesichert sind — auch ohne formale NISG-Pflicht.

Was Geschäftsführer konkret verstehen sollten

Auch wenn das eigene Unternehmen nicht direkt unter NISG 2026 fällt, bleibt die Verantwortung für digitale Risiken nicht bei der IT.

Sie bleibt bei der Geschäftsführung.

Das ist kein neues Prinzip. Aber NIS2 macht es erstmals regulatorisch sichtbar.

Die entscheidende Frage lautet deshalb nicht nur: „Sind wir direkt betroffen?„

Sondern: „Wie verwundbar ist unser Betrieb, wenn digital etwas ausfällt?“

Für viele Unternehmen ist genau das die relevantere Frage.

Denn ein Cybervorfall wird selten deshalb teuer, weil eine Behörde fragt. Er wird teuer, weil der Betrieb steht.

Drei Fragen, die Geschäftsführer jetzt beantworten sollten

Auch ohne direkte NISG-Pflicht sollten Geschäftsführungen heute drei Fragen sauber beantworten können.

1. Wie verwundbar ist unser Betrieb digital wirklich?

Welche Systeme sind kritisch? Was passiert bei Ausfall von E-Mail, ERP, Telefonie, Cloud-Zugängen oder Kundendaten?

Viele Unternehmen sind digital deutlich abhängiger, als sie im Alltag wahrnehmen.

2. Wie abhängig ist unser Umsatz von digitalem Vertrauen?

Kunden kaufen nicht nur Leistungen. Sie kaufen Verlässlichkeit.

Wer Daten verliert, länger ausfällt oder Sicherheitsvorfälle schlecht kommuniziert, verliert nicht nur Zeit — sondern Vertrauen.

3. Was kostet uns kein Vorfall – und was kostet uns einer?

Das ist die betriebswirtschaftlich relevante Frage.

Nicht: „Brauchen wir das wirklich?„

Sondern: Was kostet Prävention im Verhältnis zu Stillstand, Haftung, Reputationsschaden und Auftragsverlust?

Genau dort wird Cybersecurity zur Managementfrage.

Was NISG 2026 direkt verlangt – wenn man betroffen ist

Für direkt betroffene Unternehmen bringt NISG 2026 klare Pflichten:

- Registrierung beim Bundesamt für Cybersicherheit
- strukturierte Selbstdeklaration der Sicherheitsmaßnahmen
- dokumentierte Risikoanalyse
- Sicherheitsmaßnahmen nach Stand der Technik
- Lieferkettenprüfung
- Meldeprozesse für Sicherheitsvorfälle
- Management-Schulungen
- dokumentierte Billigungs- und Überwachungspflichten

Das ist keine rein technische Checkliste. Es ist ein Governance-System.

Und genau deshalb ist das Thema strategisch relevant — auch für Unternehmen, die formal nicht unmittelbar erfasst sind.

Förderungen: Warum sich frühes Handeln gerade jetzt lohnt

Der österreichische Förderrahmen ist derzeit ungewöhnlich günstig.

Unternehmen, die ihre Sicherheitsbasis jetzt strukturieren, können einen Teil der Kosten noch gezielt fördern lassen.

Besonders relevant sind aktuell:

- **KMU.DIGITAL** (WKO / BMAW) für Analyse, Strategie und Umsetzung
- **Cyber! Aber sicher** der SFG für steirische Unternehmen
- **Cyber Security Schecks** der FFG
- **Skills Schecks** für Schulung und Weiterbildung von Geschäftsführung und Mitarbeitern

Gerade für KMU ist das relevant, weil sich damit nicht nur Technik, sondern auch Struktur, Prozesse und Awareness wirtschaftlich sinnvoll aufbauen lassen.

Fazit: Für viele KMU kein Gesetzesproblem – aber ein sehr klares Marktsignal

Für viele kleine Unternehmen in Österreich ist NISG 2026 kein unmittelbares Gesetzesproblem.

Es ist aber ein sehr klares Marktsignal.

Wer nicht direkt reguliert ist, wird trotzdem indirekt an denselben Standards gemessen — durch Kunden, Partner, Versicherer und Haftungsfragen.

Die eigentliche Frage lautet deshalb nicht, ob Ihr Unternehmen formal unter NIS2 fällt.

Sondern ob Ihr Betrieb digital belastbar genug aufgestellt ist, wenn ein Vorfall nicht theoretisch bleibt.

Genau dort beginnt unternehmerische Resilienz.

Nicht bei Paragraphen. Sondern bei Handlungsfähigkeit.

Wie gut ist Ihr Unternehmen auf digitale Risiken vorbereitet?

Wenn Sie einschätzen möchten, wie verwundbar Ihr Betrieb heute tatsächlich ist — technisch, organisatorisch und strategisch — ist eine strukturierte Bestandsaufnahme meist der sinnvollste erste Schritt.

In unserer Potentialanalyse prüfen wir gemeinsam, wo reale Risiken liegen, welche Maßnahmen wirtschaftlich sinnvoll sind und wo sich Sicherheit pragmatisch verbessern lässt — ohne unnötige Komplexität.

Potentialanalyse unverbindlich anfragen

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

https://wissen.strukturaflow.it.com