XCUBITOR

CHECKLISTE 1 VON 3

NIS2-Selbstcheck für KMU

In 15 Minuten klären: Sind Sie vom NISG 2026 direkt betroffen, indirekt über Ihre Kunden – oder (noch) nicht? Und wie weit sind die zehn Maßnahmen, die das Gesetz verlangt?

Checkliste zum Ausdrucken und Ausfüllen · Stand: November 2026 · xcubitor.at

A Bin ich betroffen?

Hintergrund Das NISG 2026 (BGBl. I Nr. 94/2025) setzt die EU-Richtlinie NIS2 um. Die Pflichten gelten seit 1. Oktober 2026 für mittlere und große Unternehmen in 18 Sektoren – und indirekt für deren Zulieferer. Kreuzen Sie an, was zutrifft.

FRAGE	JA	NEIN	UNKLAR
1. Hat Ihr Unternehmen **50 oder mehr Beschäftigte**?	☐	☐	☐
2. Liegen Jahresumsatz **und** Bilanzsumme jeweils über **10 Mio. Euro**?	☐	☐	☐
3. Sind Sie in einem der **18 Sektoren** tätig? (u. a. Energie, Verkehr, Bankwesen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, IT-Dienstleistungen, öffentliche Verwaltung, Raumfahrt, Post, Abfall, Chemie, Lebensmittel, Herstellung von Medizinprodukten/Elektronik/Maschinen/Fahrzeugen, digitale Dienste, Forschung)	☐	☐	☐
4. Sind Sie ein Anbieter, der **unabhängig von der Größe** erfasst ist? (z. B. DNS-Dienste, Domain-Registrierung, qualifizierte Vertrauensdienste, öffentliche Kommunikationsnetze)	☐	☐	☐
5. Haben Sie **Kunden, die unter NIS2 fallen** (Spital, Energieversorger, größerer Produktionsbetrieb, Behörde) – mit Fernzugriff, Wartung, Software oder Zutritt?	☐	☐	☐

Direkt betroffen

Frage 3 „Ja“ und (1 oder 2) „Ja“ – oder Frage 4 „Ja“. Weiter mit Teil B und C.

Indirekt betroffen

Nur Frage 5 „Ja“: Ihre Kunden müssen die Lieferkette absichern und werden Nachweise verlangen. Weiter mit Teil B.

Derzeit nicht betroffen

Alles „Nein“: Teil B bleibt trotzdem die beste Grundlage für Versicherung, Ausschreibungen und den Ernstfall.

Bei „Unklar“ holen Sie rechtlichen Rat ein. Maßgeblich ist der Gesetzestext im RIS (ris.bka.gv.at); diese Checkliste ist eine allgemeine Information und keine Rechtsberatung.

B Die zehn Maßnahmen – wie weit sind Sie?

NIS2 verlangt zehn Mindestmaßnahmen (Art. 21). Übersetzt in KMU-Sprache: Kreuzen Sie an und notieren Sie, womit Sie es belegen könnten – genau das fragen Kunden-Fragebögen ab.

#	MASSNAHME IN ALLTAGSSPRACHE	STATUS	NACHWEIS (DOKUMENT, TOOL, VERTRAG)
1	**Risiken kennen.** Es gibt eine Liste der wichtigsten Systeme (E-Mail, Website, Buchhaltung, Kundendaten, Maschinen) und was passiert, wenn sie ausfallen.	☐ ja ☐ teils ☐ nein	
2	**Vorfälle bewältigen.** Ein Notfallplan mit Kontakten und Meldewegen liegt ausgedruckt vor (siehe Checkliste 2).	☐ ja ☐ teils ☐ nein	
3	**Backups und Weiterbetrieb.** Tägliche Sicherung, eine Kopie getrennt vom Netzwerk, Rücksicherung in den letzten 6 Monaten getestet.	☐ ja ☐ teils ☐ nein	
4	**Lieferkette.** Sie wissen, welche Dienstleister Zugang zu Ihren Systemen haben (IT-Betreuer, Agentur, Hoster, Steuerberatung) und was vertraglich zu Sicherheit vereinbart ist.	☐ ja ☐ teils ☐ nein	
5	**Updates und Schwachstellen.** Betriebssysteme, Website-Plugins, Router und Firmware werden regelmäßig aktualisiert; jemand ist dafür zuständig.	☐ ja ☐ teils ☐ nein	
6	**Wirksamkeit prüfen.** Mindestens einmal im Jahr wird geprüft, ob die Maßnahmen greifen (Audit, Sicherheitscheck, Phishing-Test).	☐ ja ☐ teils ☐ nein	
7	**Schulung und Hygiene.** Alle Mitarbeitenden wurden in den letzten 12 Monaten zu Phishing und sicherem Arbeiten geschult; die Geschäftsleitung ebenfalls.	☐ ja ☐ teils ☐ nein	
8	**Verschlüsselung.** Laptops und Handys sind verschlüsselt, die Website läuft nur über HTTPS, E-Mail-Versand ist mit SPF, DKIM und DMARC abgesichert.	☐ ja ☐ teils ☐ nein	
9	**Zugänge und Geräte.** Jede Person hat ein eigenes Konto, Admin-Rechte nur wer sie braucht, Zugänge werden beim Ausscheiden entzogen (siehe Checkliste 3), Geräteliste vorhanden.	☐ ja ☐ teils ☐ nein	
10	**Zwei-Faktor-Authentifizierung.** Für E-Mail, Microsoft 365/Google, Fernzugänge, Website-Admin, Bank und Hosting ist 2FA eingeschaltet – ohne Ausnahme für den Chef.	☐ ja ☐ teils ☐ nein	

8–10 × „ja“
Sie können Fragebögen von Kunden heute beantworten. Nachweise sammeln und jährlich wiederholen.

4–7 × „ja“
Typisch für KMU. Reihenfolge: zuerst 10, 3 und 2 – sie verhindern die teuersten Vorfälle.

0–3 × „ja“
Beginnen Sie diese Woche mit 2FA (Maßnahme 10) und einem getrennten Backup (3). Beides kostet fast nichts.

C Pflichten, wenn Sie direkt betroffen sind

- [ ] Registrierung beim Bundesamt für Cybersicherheit innerhalb von 3 Monaten nach Betroffenheit
  Unterlagen: Firmendaten, Sektor, Einstufung als wesentliche oder wichtige Einrichtung, Ansprechperson
- [ ] Meldeweg für erhebliche Vorfälle festgelegt: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht binnen 1 Monat
  Wer meldet? Wer vertritt? Wo liegen die Zugangsdaten zum Meldeportal?
- [ ] Geschäftsleitung hat eine Cybersicherheits-Schulung besucht und die Verantwortung dokumentiert
  Die Geschäftsleitung haftet für die Umsetzung – das lässt sich nicht delegieren
- [ ] Selbstdeklaration 12 Monate nach Registrierung vorbereitet (in der Regel bis 1. Oktober 2027)
  Die Nachweise aus Teil B sind die Grundlage
- [ ] Wesentliche Einrichtung: Prüfbericht einer unabhängigen Stelle eingeplant (organisatorisch frühestens ab 10/2028, technisch ab 09/2030)
  Eine ISO-27001-Zertifizierung kann dafür dienen

Strafrahmen: bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes für wesentliche Einrichtungen, bis zu 7 Mio. Euro oder 1,4 % für wichtige Einrichtungen. Entscheidender als die Strafe ist für KMU meist der Vertrag mit dem Kunden, der ohne Nachweise nicht verlängert wird.

D Wenn Sie indirekt betroffen sind: der typische Kunden-Fragebogen

Das fragen Spitäler, Energieversorger und Industriebetriebe ihre Dienstleister. Wer heute „ja“ ankreuzen kann, hat bei der nächsten Vertragsverlängerung einen Vorteil.

- ☐ Zwei-Faktor-Authentifizierung für alle Zugänge zu Systemen des Kunden, insbesondere Fernwartung
- ☐ Benannte Ansprechperson für Sicherheitsvorfälle mit Vertretung und Erreichbarkeit
- ☐ Zusage, Sicherheitsvorfälle, die den Kunden betreffen können, unverzüglich zu melden
- ☐ Geregelte Updates für alle beim Kunden eingesetzten Geräte und Software (inkl. Steuerungen, Firmware)
- ☐ Aktuelle, getrennte Datensicherung der eigenen Systeme
- ☐ Keine Standardpasswörter auf beim Kunden installierter Technik; Zugangsdaten dokumentiert übergeben
- ☐ Mitarbeitende, die beim Kunden arbeiten, sind zu Phishing und sicherem Umgang mit Zugängen geschult

Meine nächsten drei Schritte

Quellen: NISG 2026 (BGBl. I Nr. 94/2025), Richtlinie (EU) 2022/2555 Art. 21 und 23, Informationen des Bundesamts für Cybersicherheit und von CERT.at (Stand Oktober 2026). Mehr: xcubitor.at/lexikon/nis2/ · Allgemeine Information, keine Rechtsberatung.

Sicherheit, die Ihnen erklärt wird

Xcubitor überwacht Website und Webhosting Ihres Unternehmens rund um die Uhr und warnt Sie in verständlicher Sprache. Zum Start prüfen wir, ob niemand mehr drin ist.

xcubitor.at/preise