NIS2-QUICK-CHECK

Zielgruppe: Unternehmen mit möglicher NIS2-Betroffenheit
Dauer: 10-15 Minuten
Ergebnis: 0-40 Punkte → Ampel + Next Steps

A) Betroffenheit & Governance

	Ja	Teilw.	Nein
Unsere Branche fällt unter NIS2 (z.B. Energie, Gesundheit, Transport, IT-.Dienstleistung, öffentliche Verwaltung).	☐	☐	☐
Wir haben >50 Mitarbeitende oder >10 Mio. € Umsatz **oder** erbringen kritische Dienstleistungen.	☐	☐	☐
Es gibt eine Person in der Geschäftsleitung, die ausdrücklich die Verantwortung für Cybersecurity trägt.	☐	☐	☐
Es existiert eine kurze, zugängliche und allgemeingültige Sicherheitsleitlinie (2-3 Seiten).	☐	☐	☐
Schulungen/Sensibilisierung zur IT-Sicherheit finden mindestens einmal pro Jahr statt.	☐	☐	☐

Warum wichtig: NIS2 macht die Geschäftsleitung persönlich verantwortlich.
Tipp: Benennen Sie einen Verantwortlichen, der regelmäßig berichtet.

B) Risiken & Partner

	Ja	Teilw.	Nein
Wir wissen, welche unsere wichtigsten Dienstleistungen und Systeme sind.	☐	☐	☐
Wir haben die größten Cyber-Risiken der letzten 12 Monate bewertet.	☐	☐	☐
Unsere wichtigsten Lieferanten/Dienstleister wurden auf Risiken überprüft (z.B. Cloud-Anbieter).	☐	☐	☐
Es gibt einen Maßnahmenplan (Wer macht was bis wann?).	☐	☐	☐
Es existiert ein Wiederanlaufplan (z.B. was tun bei Stromausfall, Cyberangriff).	☐	☐	☐

Warum wichtig: Lieferanten und Partner sind Teil Ihrer Wertschöpfung - sie können auch durch Ihren Vorfall getroffen werden.

C) Technische Basis

	Ja	Teilw.	Nein
Wichtige Zugänge (z.B. Cloud, Unternehmensnetz) sind durch Zwei-Faktor-Login geschützt (z.B. App, Code).	☐	☐	☐
Sicherheits-Updates werden regelmäßig und mit festen Fristen installiert.	☐	☐	☐
Es werden zentrale Protokolle/Logfiles geführt, um Angriffe nachvollziehen zu können.	☐	☐	☐
Backups existieren und wurden im letzten Jahr auf Wiederherstellbarkeit getestet.	☐	☐	☐
Unsere E-Mails sind gegen Fälschung/Phishing abgesichert (z.B. SPF/DMARC).	☐	☐	☐

Hinweis: Sie müssen das nicht technisch verstehen - wichtig ist, dass Ihr IT-Team dies bestätigen kann.

D) Reaktionsfähigkeit

	Ja	Teilw.	Nein
Es gibt einen schriftlichen Plan, wie wir im Notfall reagieren (Incident-Plan).	☐	☐	☐
Wir haben in den letzten 12 Monaten eine Notfall-Übung durchgeführt.	☐	☐	☐
Es ist klar geregelt, wer außerhalb der Bürozeiten im Notfall erreichbar ist.	☐	☐	☐
Es existiert eine Vorlage für Erstmeldungen an Behörden oder Kunden im Ernstfall.	☐	☐	☐
Unsere Sicherheits-Dokumente sind versioniert und zentral abgelegt.	☐	☐	☐
Die Mitarbeitenden wissen, an wen Sie sich bei einem Notfall wenden sollen.	☐	☐	☐

Warum wichtig: Sie müssen nach NIS2 binnen 24 Stunden einen Vorfall melden können - ohne einen Plan verlieren Sie wertvolle Zeit.

Score & Ampel

0-15 Rot: Akuter Handlungsbedarf, Erste Schritte: Verantwortliche benennen, MFA aktivieren, Notfall-Plan beginnen.

16-30 Orange: Basis vorhanden, Fokus: Lieferanten prüfen, Übungen durchführen, Nachweise sammeln.

31-40 Grün: Gute Basis, Nächste Schritte: Feinschliff & regelmäßige Reviews.

Ihr Ergebnis

Ihr Score (ausfüllen): _____

Ihre Top-3-Handlungsfelder (ausfüllen):

1

2

3

Nächste Schritte

Kurzfristig: Verantwortlichkeiten & MFA

Mittelfristig: Notfall-Übungen & Lieferantenbewertung

Langfristig: Audit-Vorbereitung & kontinuierliche Verbesserungen

Kostenlose Erstberatung buchen - wir erklären Ihnen, welche NIS2-Pflichten konkret für Sie gelten.