NIS2 QuickCheck für KMU in Köln

Praktischer Leitfaden: Betroffenheit prüfen, Pflichten verstehen, erste Maßnahmen umsetzen

Tech Hilfe Pro · Remote & vor-Ort-Service · Tel +49 15565029989 · info@techhilfepro.de · techhilfepro.de

1) Sind wir von NIS2 betroffen?

Grundregel (Size-Cap): NIS2 gilt in der Regel für mittlere und große Unternehmen in gelisteten Sektoren (≥50 Mitarbeitende oder ≥10 Mio. € Umsatz/Bilanzsumme). Ausnahmen: kleinere Unternehmen können betroffen sein, wenn sie kritische Leistungen erbringen. Unternehmen müssen ihre Betroffenheit eigenständig prüfen und sich – wenn betroffen – beim BSI registrieren.

- Sektor-Check: Branchen aus Anhang I (besonders kritisch) und Anhang II (wichtig).
- Größen-Check: ≥50 Mitarbeitende oder ≥10 Mio. € Umsatz/Bilanzsumme (Faustregel).
- Selbstprüfung & Registrierung: Betroffene Einrichtungen registrieren sich beim BSI innerhalb von 3 Monaten.
- Ressource: BSI Betroffenheitsprüfung (Online-Tool) und Informationen der IHK Köln.

2) Pflichten auf einen Blick (Art. 21 NIS2)

Diese Kernbereiche müssen angemessen, verhältnismäßig und risikobasiert adressiert sein:

- Richtlinien zu Risikoanalyse & Informationssicherheit
- Incident Handling (Erkennung, Reaktion, Lessons Learned)
- Business Continuity & Krisenmanagement (inkl. Backup/Restore-Tests)
- Lieferkettensicherheit (inkl. MSP/Cloud/Software)
- Sichere Beschaffung/Entwicklung/Wartung (inkl. Vulnerability-Management & Disclosure)
- Wirksamkeitsmessung der Maßnahmen (KPIs, Audits)
- Cyber-Hygiene & Schulungen (Awareness, Phishing-Trainings)
- Crypto & Verschlüsselung, MFA, starke Passwörter
- Logging, Monitoring, SIEM/MDR nach Risiko
- Sichere Remote-Zugänge & Zugriffskontrollen (Least Privilege)

3) Meldepflichten bei Sicherheitsvorfällen (Art. 23 NIS2)

- Frühwarnung: innerhalb von 24 Stunden nach Kenntnis eines erheblichen Vorfalls.
- Incident-Notification: innerhalb von 72 Stunden mit Erstbewertung und Indikatoren (IoCs).
- Abschlussbericht: spätestens innerhalb von 1 Monat (oder Zwischenberichte bis zum Abschluss).

4) Verantwortung der Leitung & Sanktionen (Art. 34 NIS2)

Management trägt Verantwortung für die Umsetzung. Mögliche Höchstbußgelder: • Besonders wichtige Einrichtungen (Essential): bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes • Wichtige Einrichtungen (Important): bis zu 7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes

5) 10-Punkte-QuickCheck (Ja/Nein)

	Checklist
■	Betroffenheitsprüfung durchgeführt (Sektor & Größe) und Ergebnis dokumentiert
■	BSI-Registrierung vorbereitet/erledigt (falls betroffen) inkl. Ansprechstelle
■	MFA ausgerollt (alle kritischen Konten) und Passwort-Policy aktuell
■	Regelmäßige, getestete Backups (Restore-Tests protokolliert)
■	Patch-Management mit definierten SLAs (Kritikalität-basiert)
■	Incident-Response-Plan (Meldewege 24h/72h/1 Monat) geübt
■	Lieferkettensicherheit: vertragliche Mindestanforderungen, MSP/Cloud bewertet
■	Protokollierung/Monitoring angemessen (z. B. zentrale Logs, Alarmierung)
■	Awareness-Programm aktiv (Phishing-Simulationen, jährliche Schulung)
■	Management-Review & KPI/Cyber-Risikoquartalsbericht etabliert

6) Erste 14 Tage – Umsetzung in Sprints

- Tag 1–2: Betroffenheit prüfen (BSI-Tool), Verantwortliche bestimmen, Risiko-Workshop terminieren
- Tag 3–5: Inventar & Kronjuwelen (Daten/Prozesse) erfassen, MFA-Plan, Backup-Check & Restore-Test einplanen
- Tag 6–9: Incident-Playbook draften, Meldewege und Kontaktstellen festlegen, Lieferantenliste bewerten
- Tag 10–14: Patch-SLAs definieren, Monitoring-Minimum umsetzen, Awareness-Kickoff, Management-Review vorbereiten

Kontakt

Tech Hilfe Pro · Remote & vor-Ort-Service · Tel +49 15565029989 · info@techhilfepro.de · techhilfepro.de

Quellen (Auswahl):

- ENISA (2025): Mapping NIS2 obligations & Incident timeline (Art. 21/23).
- European Commission (2024): Implementing Regulation (EU) 2024/2690 (technische Anforderungen).
- EUR-Lex (2022): Directive (EU) 2022/2555, insbesondere Art. 21, 23, 34.
- IHK Köln (2025): Hinweise zur NIS2-Betroffenheit & Registrierung beim BSI.
- BSI (2025): NIS-2-Betroffenheitsprüfung und Registrierung.

Stand: 03.10.2025