COMPLIANCE · CHECKLISTE

Sind Sie NIS2-bereit? 26 Pflichtpunkte im Check.

Diese Checkliste führt Sie in zwei Schritten durch NIS2: erst sechs Fragen zur Betroffenheit, dann 26 Pflichtpunkte. Abhaken, was nachweisbar erfüllt ist – alles Offene ist Ihre Roadmap.

GELTUNGSBEREICH	MELDEFRISTEN	RISIKO
18 Sektoren, ab 50 Mitarbeitenden oder 10 Mio. € Umsatz	24 Stunden Erstmeldung ans BSI, 72 Stunden Detailbericht	Bis 10 Mio. € oder 2 % Umsatz – plus persönliche Haftung der Leitung

Teil 1 Betroffenheit klären

ZUTREFFEND?

- ☐ Wir sind in einem der **18 NIS2-Sektoren** tätig (u. a. Energie, Verkehr, Gesundheit, Wasser, digitale Infrastruktur, IKT-Dienste, Produktion, Chemie, Lebensmittel, Post, Abfall, Forschung)
- ☐ Wir sind **Zulieferer oder IT-Dienstleister** eines betroffenen Unternehmens (Lieferkettenpflichten greifen durch)
- ☐ Die **Registrierung beim BSI** ist erfolgt oder terminiert
- ☐ Wir haben **mindestens 50 Mitarbeitende** oder **10 Mio. € Jahresumsatz**
- ☐ Uns ist klar, ob wir als **wesentliche** oder **wichtige** Einrichtung eingestuft sind
- ☐ Es ist schriftlich festgehalten, **wer die Betroffenheit geprüft** hat – mit Datum

Teil 2 · A Governance und Haftung

ABGEHAKT?

- ☐ Die **Geschäftsleitung hat die Risikomanagement-Maßnahmen förmlich gebilligt** und überwacht deren Umsetzung
- ☐ Es gibt eine **benannte verantwortliche Person** für Informationssicherheit mit Budget und Mandat
- ☐ Die Leitungsebene hat an einer **Cybersicherheits-Schulung** teilgenommen (Pflicht, nicht Kür)
- ☐ NIS2-Pflichten sind in **Rollen, Vertretungen und Zielen** verankert – nicht nur in einer Präsentation

Teil 2 · B Risikomanagement nach Art. 21

ABGEHAKT?

- ☐ **Risikoanalyse** und Sicherheitskonzept für Informationssysteme liegen aktuell vor
- ☐ **Backup-, Notfall- und Krisenmanagement** inklusive Wiederanlaufzeiten definiert
- ☐ **Sicherheit bei Beschaffung, Entwicklung und Wartung** geregelt, inkl. Schwachstellenbehandlung
- ☐ **Cyberhygiene und Awareness-Schulungen** laufen wiederkehrend für alle Mitarbeitenden
- ☐ **Personalsicherheit, Zugriffskontrolle und Asset-Management** sind umgesetzt und aktuell
- ☐ **Bewältigung von Sicherheitsvorfällen** ist als Prozess beschrieben und geübt
- ☐ **Sicherheit der Lieferkette** bewertet – je Lieferant, nicht pauschal
- ☐ **Wirksamkeit der Maßnahmen** wird regelmäßig bewertet und dokumentiert
- ☐ **Kryptografie und Verschlüsselung** sind per Richtlinie geregelt
- ☐ **Multi-Faktor-Authentisierung** und gesicherte Kommunikation im Notfall stehen bereit

Teil 2 · C Meldeprozess – die Uhr läuft ab Kenntnis

ABGEHAKT?

- ☐ **Erstmeldung binnen 24 Stunden** ans BSI ist als Ablauf hinterlegt – inkl. Vertretung nachts und am Wochenende
- ☐ **Abschlussbericht binnen eines Monats** ist eingeplant (Ursachen, Maßnahmen, Auswirkungen)
- ☐ **Zugang zum BSI-Meldeportal** ist eingerichtet und mindestens einmal getestet
- ☐ **Detailbericht binnen 72 Stunden** mit Erstbewertung von Schwere und Auswirkungen vorbereitet
- ☐ Die **DSGVO-Meldung binnen 72 Stunden** an die Datenschutzbehörde ist mitgedacht, wenn Personenbezug vorliegt
- ☐ **Meldevorlagen und Entscheidungskriterien** („erheblich?“) liegen ausgefüllt griffbereit

Teil 2 · D Erkennung, Reaktion, Lieferkette

ABGEHAKT?

- ☐ **Zentrales Logging** relevanter Systeme mit definierter Aufbewahrungsdauer
- ☐ **Incident-Response-Plan** existiert, ist verteilt und wurde in den letzten 12 Monaten geübt
- ☐ **Lieferantenübersicht** mit Kritikalitätsbewertung ist gepflegt
- ☐ **Angriffserkennung rund um die Uhr** – intern oder als Managed Service
- ☐ **Externe Forensik- und IR-Kapazität** ist vorab vertraglich gesichert – nicht erst im Ernstfall gesucht
- ☐ **Sicherheitsanforderungen in Verträgen** mit kritischen Lieferanten verankert und nachgewiesen

Auswertung über die 26 Pflichtpunkte aus Teil 2:

23–26 erfüllt

Solide Basis. Jetzt Nachweise bündeln und die Wirksamkeit turnusmäßig prüfen lassen.

15–22 erfüllt

Typischer Stand. Priorisieren Sie Meldeprozess, Lieferkette und Nachweisführung.

unter 15 erfüllt

Handlungsbedarf. Beginnen Sie mit einer Gap-Analyse und einem belastbaren Meldeprozess.

Der häufigste Fehler: Maßnahmen sind vorhanden, aber nicht nachweisbar. NIS2 verlangt Dokumentation und regelmäßige Wirksamkeitsprüfung – ein gelebter Prozess ohne Protokoll zählt im Zweifel nicht. Fangen Sie deshalb dort an, wo Nachweis und Frist zusammentreffen: beim Meldeweg.

Aus der Checkliste wird ein Plan.

Ein Cyber Security Assessment mit Compliance-Fokus klärt Betroffenheit und Ist-Stand, priorisiert die Lücken und liefert den Meldeprozess gleich mit. Auf Wunsch übernehmen wir Erkennung und Reaktion anschließend rund um die Uhr aus dem Cyber Defense Center.

Notfall-Hotline +49 89 45 24 24-112 · 24/7/365 · kontakt@argos.security

argos.security/kontakt

Rechtlicher Hinweis: Diese Checkliste ist eine praxisorientierte Orientierungshilfe und ersetzt keine Rechtsberatung. Maßgeblich sind die NIS-2-Richtlinie (EU) 2022/2555, das deutsche NIS2-Umsetzungsgesetz und die Auslegung der zuständigen Behörden. **Stand: 07/2026.**