

IoT Security Checklist

Die Mindestanforderungen, bevor ein vernetztes Gerät in Ihr Produktionsnetz geht – inklusive NIS2-Einordnung.

6 Bereiche	26 Kontrollen	NIS2 berücksichtigt
----------------------	-------------------------	-------------------------------

Jeder vernetzte Sensor ist ein zusätzlicher Zugangspunkt. Diese Checkliste ist bewusst knapp gehalten: Sie deckt die Kontrollen ab, die in der Praxis den Unterschied machen, nicht den vollständigen Normenkatalog.

Lieber gemeinsam durchgehen?

Im kostenlosen Erstgespräch ordnen wir Ihre Ergebnisse ein und benennen den nächsten Schritt.

[Erstgespräch vereinbaren](#)

[KI-Readiness-Check >](#)

1. Netzarchitektur

- ☐ OT- und IT-Netz sind getrennt, per VLAN oder physisch
- ☐ Übergänge laufen über eine kontrollierte Stelle
- ☐ IoT-Geräte liegen in einem eigenen Segment
- ☐ Kommunikationsbeziehungen sind dokumentiert und auf das Nötige begrenzt
- ☐ Es besteht kein direkter Internetzugang aus dem OT-Segment

2. Geräte und Identitäten

- ☐ Standardpasswörter sind bei allen Geräten geändert
- ☐ Jedes Gerät hat eine eindeutige Identität
- ☐ Ein Inventar aller vernetzten Geräte wird gepflegt
- ☐ Nicht benötigte Dienste und Ports sind deaktiviert
- ☐ Der physische Zugang zu Gateways ist beschränkt

3. Datenübertragung

- ☐ Verbindungen sind mit TLS verschlüsselt
- ☐ Zertifikate werden verwaltet und rechtzeitig erneuert
- ☐ Die Authentifizierung erfolgt beidseitig, wo möglich
- ☐ Das Datenziel liegt in der EU
- ☐ Ein Auftragsverarbeitungsvertrag mit dem Anbieter besteht

4. Updates und Schwachstellen

- ☐ Ein Update-Prozess für Firmware ist definiert
- ☐ Die Verantwortlichkeit für Updates ist benannt
- ☐ Hersteller-Sicherheitsmeldungen werden verfolgt
- ☐ Geräte ohne Update-Fähigkeit sind identifiziert und kompensiert
- ☐ End-of-Life-Termine der Geräte sind bekannt

5. Überwachung und Reaktion

- ☐ Auffällige Kommunikation wird erkannt
- ☐ Logs werden zentral gesammelt und aufbewahrt
- ☐ Ein Notfallplan für den Sicherheitsvorfall existiert
- ☐ Meldewege sind definiert
- ☐ Der Wiederanlauf nach einem Vorfall ist geübt

6. NIS2-Einordnung

Die NIS2-Richtlinie erweitert den Kreis der betroffenen Unternehmen erheblich. Prüfen Sie Ihre Betroffenheit, bevor Sie investieren.

- ☐ Die Betroffenheit wurde geprüft, nach Sektor und Unternehmensgröße
- ☐ Falls betroffen: die Registrierungspflicht ist bekannt
- ☐ Risikomanagement-Maßnahmen sind dokumentiert
- ☐ Meldefristen bei Sicherheitsvorfällen sind bekannt
- ☐ Die Verantwortung der Geschäftsleitung ist adressiert

Wichtig: Diese Checkliste ersetzt keine Rechtsberatung. Sie hilft, den technischen Reifegrad einzuschätzen und die richtigen Fragen zu stellen. Die konkrete NIS2-Betroffenheit sollte rechtlich geprüft werden.