NIS2 – Technische Anforderungen und Herausforderungen

Die Umsetzung der EU-Richtlinie NIS2 (Network and Information Security Directive 2) verlangt von Unternehmen, insbesondere aus den Bereichen kritischer Infrastrukturen (KRITIS) und wesentlicher digitaler Dienste eine Umsetzung verschärfter Sicherheitsvorgaben umzusetzen und bestehende IT-Strukturen auf ein höheres Sicherheitsniveau zu heben.

Ein zentrales Element der NIS2-Anforderungen ist die Stärkung der Cybersicherheit auf technischer Ebene. Dazu gehört unter anderem die systematische Risikobewertung der IT-Systeme, die Identifikation kritischer Assets und die kontinuierliche Analyse potenzieller Bedrohungen. Es müssen Werkzeuge und Verfahren implementiert werden, mit denen Schwachstellen erkannt, priorisiert und behoben werden können. Technisch bedeutet das den Einsatz von Schwachstellenscannern, Endpoint Detection & Response (EDR) sowie die Anbindung an Threat-Intelligence-Feeds.

Ein weiteres wesentliches technisches Ziel von NIS2 ist die Verbesserung der Netzwerksicherheit. Hierzu zählen Maßnahmen wie Netzwerksegmentierung, die Einführung von Zero-Trust-Architekturen, verschlüsselte Kommunikation sowie der Einsatz moderner Firewalls, Intrusion Detection/Prevention-Systeme (IDS/IPS) und VPN-Technologien. Auch müssen Mechanismen zur Zugangskontrolle gestärkt werden – insbesondere durch Multi-Faktor-Authentifizierung (MFA), rollenbasierte Zugriffskonzepte (RBAC) und ein zentrales Identitätsmanagement.

NIS2 fordert eine lückenlose Protokollierung und Überwachung von sicherheits-relevanten Ereignissen. Die daraus gewonnenen Informationen müssen nicht nur für interne Sicherheitsprozesse genutzt werden, sondern auch im Rahmen der NIS2-Meldepflichten an zuständige Behörden übermittelt werden können.

Logdaten und Sicherheitsereignissen erzeugen hohe Anforderungen an Speicher, Datenmanagement und Datenschutz. Es muss nicht nur sichergestellt werden, dass Daten vollständig und konsistent erfasst werden, sondern auch, dass sie konform zur DSGVO verarbeitet werden, insbesondere wenn es um die Speicherung personenbezogener Daten geht.

Die technische Absicherung von Schnittstellen zu Drittanbietern, Cloud-Services oder Fernzugriffslösungen erfordert klare Sicherheitsstandards und laufende Überprüfungen.

Zudem verlangt NIS2 eine verbesserte Resilienz gegenüber IT-Ausfällen und Cyberangriffen. Technisch bedeutet das unter anderem die Einführung redundanter Systeme, Hochverfügbarkeitslösungen, regelmäßige Backups und die klare Definition von Wiederherstellungszeiten (RTO/RPO).

Cyber Complete GmbH
Weststraße 4
57392 Schmallenber

Ein weiterer Schwerpunkt liegt auf der Reaktionsfähigkeit im Ernstfall. Incident-Response-Plänen müssen entwickelt und technisch umgesetzt werden, die klare Abläufe für die Erkennung, Eindämmung und Beseitigung von Sicherheitsvorfällen vorsehen. Dazu gehört auch die regelmäßige Durchführung technischer Tests und Notfallübungen, um die Widerstandsfähigkeit der IT-Infrastruktur gegen reale Bedrohungsszenarien zu prüfen.

Die Herausforderung liegt nicht nur in der Einführung neuer Technologien, sondern vor allem in der nachhaltigen und integrierten Umsetzung sicherer IT-Strukturen im gesamten Unternehmen. Eine langfristig erfolgreiche NIS2-Compliance erfordert deshalb ein Zusammenspiel aus technischem Know-how, Prozessverständnis und interdisziplinärer Zusammenarbeit.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenber

NIS2-Betroffenheits-Checkliste

Ziel: Herausfinden, ob dein Unternehmen als **wesentliche oder wichtige Einrichtung** gemäß der NIS2-Richtlinie eingestuft wird – und damit unter die **Cybersicherheitsvorgaben der EU** fällt.

1. Branchenzugehörigkeit

A. Ist Ihr Unternehmen in einem kritischen Sektor gemäß NIS2 tätig?

(Wenn „Ja“, weitere Prüfung zwingend erforderlich)

Sektor	Ja	Nein
Energie (Strom, Öl, Gas, Wasserstoff, Fernwärme, etc.)	☐	☐
Verkehr (Luft-, Bahn-, Schiffs-, Straßenverkehr, Logistikzentren)	☐	☐
Bankwesen (inkl. Kreditinstitute)	☐	☐
Finanzmarktinfrastrukturen	☐	☐
Gesundheitswesen (Krankenhäuser, Kliniken, Labore, Telemedizin, etc.)	☐	☐
Trinkwasser- und Abwasserwirtschaft	☐	☐
Digitale Infrastruktur (DNS, TLD-Registrare, Cloud-Computing, Rechenzentren, CDN)	☐	☐
IKT-Dienstleistungen für kritische Sektoren	☐	☐
Öffentliche Verwaltung (zentral oder regional – je nach Mitgliedsstaat)	☐	☐
Raumfahrt (Satellitenbetrieb, -steuerung etc.)	☐	☐

Cyber Complete GmbH
Weststraße 4
57392 Schmallenber

2. Größe und Bedeutung des Unternehmens

B. Gehören Sie zu den folgenden Größenklassen?

(Wenn „Ja“, hohe Wahrscheinlichkeit der NIS2-Relevanz)

Kriterium	Ja	Nein
≥ 50 Mitarbeitende	☐	☐
≥ 10 Millionen Euro Jahresumsatz **oder** Jahresbilanzsumme	☐	☐
Ihr Unternehmen ist unabhängig von der Größe als **kritisch** eingestuft worden (z. B. durch nationale Behörde)	☐	☐

Hinweis: Auch kleinere Unternehmen (< 50 MA) können betroffen sein, wenn sie **systemisch relevant** sind oder kritische Dienstleistungen bereitstellen.

---

3. Geografischer Tätigkeitsbereich & Auswirkungen

Fragen:	Ja	Nein
Erbringen wir Dienstleistungen oder betreiben wir Infrastruktur in einem EU-Mitgliedsstaat?	☐	☐
Würde ein Cyberangriff auf unser Unternehmen Auswirkungen auf Gesellschaft, Wirtschaft oder Sicherheit haben?	☐	☐

---

4. Regulatorische Hinweise oder Kommunikation

Fragen:	Ja	Nein
Wurden wir von einer nationalen Behörde (z. B. BSI in Deutschland, CERT in Österreich) über eine mögliche NIS2-Einstufung informiert?	☐	☐
Enthalten unsere Verträge mit öffentlichen oder kritischen Auftraggebern Anforderungen zur Cyber- oder Informationssicherheit?	☐	☐

Auswertung der Checkliste

Anzahl "Ja“ Antworten	Einschätzung
0–2	**Wahrscheinlich nicht betroffen**
3–5	**Möglicherweise betroffen** – eingehendere Prüfung empfohlen
6 oder mehr	**Sehr wahrscheinlich betroffen** – Vorbereitung auf NIS2-Compliance dringend empfohlen

---

Cyber Complete GmbH
Weststraße 4
57392 Schmallenber