NIS2 – KURZE EINFÜHRUNG

Die Abkürzung NIS steht für NIS2 = **Network & Security für Systeme 2.0**. Die bindende EU-Richtlinie wurde 2023 durch die EU als Nachfolger von NIS beschlossen und ist durch die einzelnen Mitgliedsstaaten bis Ende 2024 in die lokale Gesetzgebung umzusetzen.

Inzwischen gibt es nach dem Regierungswechsel einen **neuen Regierungsentwurf mit 213 Seiten vom 25.Juli 2025** mit dem Plan, diesen Ende 2025 bzw. **Anfang 2026 final als Gesetz** zu verabschieden.

Dies bedeutet viel mehr als die seit Jahren vorliegenden Empfehlungen des BSI-Grundschutzes, da bei Verstößen nun auch Bußgelder drohen.

Eines der Hauptmerkmale von NIS2 ist die deutliche Erweiterung der bisherigen Definition, welche Unternehmen zur KRITIS-Gruppe gehören, mit dem Ziel, die Cybersicherheit in Deutschland zu erhöhen.

KRITIS steht für „Kritische IT-Infrastruktur“ und umfasste bisher Unternehmen aus der Energiewirtschaft, der Gesundheitsversorgung oder der Verteidigung.

Nach der **neuen Definition** fallen sehr viele Branchen und Firmen (30.000+ deutsche Unternehmen) mit einer Größe > 50 Mitarbeiter oder > 10 Mio. Umsatz entweder in die NIS2 Kategorie „Wichtige Einrichtungen“ oder „Besonders wichtige Einrichtungen“! Nun inkludierte Branchen sind z.B. Verkehr, Transport/Logistik, Medizin, Finanzwirtschaft, Energiewirtschaft, Maschinenbau, Chemie, Elektrotechnik und Lebensmittel.

Die Anforderungen und Auflagen sind für beide Kategorien gleich – sie unterscheiden sich lediglich in der Überprüfungsart und der Bußgeldhöhe.

Die eigentlichen **neuen Anforderungen an die IT** – jetzt sogar von einem Gesetz gefordert - sind auf den folgenden Seiten beschrieben. Ebenso auch wie man diese mit konkreten Maßnahmen umsetzt. Siehe dazu auch die CAIRO Checkliste „*NIS 2 TOM*“.

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim

NIS2 IT-ANFORDERUNGEN

Die Anforderungen lassen sich mit dem Dachbegriff „Risikomanagement“ gut beschreiben:

- Wirksamkeitsbewertung von Risiko-Management-Maßnahmen (z.B. Schwachstellen-Management)
- Sicherheitsmaßnahmen bei Entwicklung u. Betrieb von IT-Systemen
- Sicherheit des Personals und der Zugriffskontrolle
- Einsatz von Kryptografie und Verschlüsselung
- Durchführung umfassender Risikoanalysen
- Bewältigung von Sicherheitsvorfällen & Notfallpläne für Krisenmanagement
- Pläne für Betriebserhaltung/Business Continuity Management (BCM)
- Cyberhygiene und Security-Schulungen (IT-Risiko-Schulungen, auch für die Leitungsebene)
- Sicherheit der Lieferkette
- Unterrichtungs- und Meldepflichten (24h/72h) bei „erheblichen“ Sicherheitsvorfällen an Behörden
- Kann: Anonyme Meldungen als Information an das Amt

Diese Punkte sind nicht neu, aber oft nicht vollständig oder nicht nach dem Stand der Technik umgesetzt. Der **Stand der Technik** bzw. der Verfahren ist z.B. in den Publikationen der EU https://www.enisa.europa.eu/ oder im BSI-IT-Grundschutz beschrieben und sollte nach dem Gesetz auch eingehalten werden!

NIS2-BUßGELDER

Verstöße gegen die Auflagen sind Ordnungswidrigkeiten, die mit Bußgeldern belegt werden. Bei wichtigen Einrichtungen betragen diese bis zu 7.Mio.€, bei besonders wichtigen Einrichtungen bis zu 10 Mio. €. Bei großen Unternehmen können die Bußgelder zudem umsatzabhängig ausfallen. Was sind nun „Verstöße“ in der Bewertung durch die Gesetzgeber? Bewertet werden die Maßnahmen für die Umsetzung der Anforderungen oder Meldungen. Verstöße sind, wenn dies „vorsätzlich“ oder „fahrlässig“:

- nicht
- nicht richtig
- nicht vollständig
- nicht rechtzeitig

erfolgen.

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim

UMSETZUNG DER NIS2-ANFORDERUNGEN

Die folgenden **Maßnahmen** sind nötig, um gesetzeskonform die IT zu betreiben und um die vorher genannten gesetzlichen Anforderungen abzudecken:

- Erstellung eines normgerechten **ISMS**
- **Schwachstellen-Management** (Analyse, Behebung, Härtungen & Konfigurationen)
- Nutzung von **SSO** (Single Sign-On) und **MFA** (Multi-Faktor-Authentifizierung)
- Nutzung von **IDS und IPS-Systeme** (Intrusion Detection und Intrusion Prevention)
- Erstellung und Schulung von **Notfallplänen** für Anwender und das IT-Team
- **Organisation:** Etablierung eines Informationssicherheitsbeauftragten (ISB) und einer Datenschutzmanager- Position (DSM)
- **Training** der **Mitarbeiter &** aller **Führungskräfte** (Training nicht delegierbar)
- **Lieferkette:** Verträge mit „Partnern“ zum Thema „Cybersecurity“
- **Reporting** (Prozessdefinition!) von Vorfällen an Behörden

Wenn Sie schon nach ISO 27000, TISAX oder VDS 10000 zertifiziert sind, haben Sie typischerweise einige der obigen Punkte abgedeckt.

Trotzdem zeigt die Praxis vieler Unternehmen, dass noch **erhebliche Lücken** existieren, insbesondere im Hinblick auf den „Stand der Technik“ und der Organisation. Dazu gehören beispielsweise Lücken im Bereich Schwachstellen-Monitoring, IDS/IPS, automatisches Patching auf Servern, bei Security-Trainings mit Lernkontrolle im Bereich Phishing oder bei der Risikoanalyse, insbesondere kritischer Systeme.

CAIRO, als IT-Compliance- und Security-Beratungsfirma mit Infrastruktur-Experten, kann diese Lücken schnell und kostengünstig schließen. Im Regelfall starten wir mit einem **CAIRO CyberRisikoCheck** (CRC) oder einem **CAIRO CyberSecurity- Check** (CSC) für die Planung der notwendigen Schutzmaßnahmen. Beide Überprüfungen sind BSI-konform. Der CSC beinhaltet auch eine NIS2 GAP-Analyse.

Wir liefern **spezielle Lösungen** für Schwachstellen-Monitoring und -Behebung, für Security-Awareness-Trainings sowie fertige ISMS-Baukästen und Bausteine für Sicherheitsprozesse und -verfahren, die Ihnen helfen, sofort gesetzeskonform zu werden.

All dies erfolgt mittelstandsgerecht, ohne dass neues Personal eingestellt werden muss und ohne unnötigen formalen Overhead zu erzeugen.

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim