NIS2-Gesetz im Überblick

Neue Richtlinien für mehr Cybersicherheit

CAIRO

secure • digital • IT-infrastructures

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.
In Deutschland wird das Gesetz „NIS2UmsuCG" heißen. Am 24.07.2024 beschloss das Bundeskabinett das „NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz".
Mittlerweile gibt es dazu den 6. Referentenentwurf vom 24.6.2024 und aktuell befindet sich das Gesetz innerhalb der Verfahren zwischen Parlament und Bundesrat.

Was definiert NIS2 ?

Eines der Hauptmerkmale von NIS2 ist die deutliche Erweiterung der bisherigen Definition, welche Unternehmen zur KRITIS-Gruppe gehören. KRITIS steht für „Kritische IT-Infrastruktur" und umfasste bisher Unternehmen aus der Energiewirtschaft, der Gesundheitsversorgung oder der Verteidigung.

Kurz zusammengefasst: Nahezu alle Branchen und Firmen (30.000 + deutsche Unternehmen) mit einer Größe > 50 Mitarbeiter oder > 10 Mio. Umsatz fallen inzwischen entweder in die NIS2 Kategorie „Wichtig" oder „Besonders wichtig"!

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

	Betreiber kritischer Anlagen		Einrichtungen	
			Besonders wichtig	Wichtig
Gesetz	NIS2UmsuCG	DachG	NIS2UmsuCG	NIS2UmsuCG
Zeitraum	ab 2024	ab 2026	ab 2024	ab 2024
Pflicht	§39 (1)	§11	§64	§65
Form	Audits	Audits	BSI Stichproben	BSI Stichproben
Inhalt	Meldepflicht SzA	Resilienz	Meldepflicht	Meldepflicht
Scope	Kritische Anlage	Kritische Anlage	Unternehmen	Unternehmen
Frequenz	alle drei Jahre	Stichproben	Stichproben	Anlass bezogen
Empfänger	BSI	BBK	BSI	BSI

Tabelle: eigene Zusammenstellung nach Referentenentwürfen, Stand Dezember 2023 *Quelle: www.openkritis.de*

Wesentliche Anforderungen von NIS2

- 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**
- Betriebserhaltung (BCM)
- Cyberhygiene und **Security-Schulungen (Schulungen auch für Leitungsebene)**
- Sicherheit der **Lieferkette**
- **Unterrichtungs- und Meldepflichten** an Behörden

Diese Punkte sind nicht wirklich neu aber oft nicht vollständig umgesetzt oder nicht nach dem „Stand der Technik“. 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.

Schon bei **wichtigen** Einrichtungen sind die Bußgelder nach §60 (6) wie folgt festgelegt :

Höhe	Verstöße
7 Mio. EUR oder 1,4 % Umsatz	• Vorkehrungen zur Cybersicherheit nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen
500.000 EUR	• Nachweise über Erfüllung der Anforderungen werden nicht oder nicht rechtzeitig erbracht • Registrierung wird nicht oder nicht rechtzeitig vorgenommen oder erforderliche Stelle nicht oder nicht rechtzeitig informiert • Informationen zur Bewältigung einer Störung werden nicht herausgegeben • Hinweis: Nachweiserbringung nach §34 (1) oder §39 (2) 1 und Informationsherausgabe nach $40 (4) 1 eigentlich nicht relevant für wichtige Betreiber. • Registrierungspflicht bereits über allgemeine Bußgelder geregelt
100.000 EUR	• Änderungen notwendiger Angaben werden nicht fristgerecht übermittelt • Verbindlichen Anweisungen zur Umsetzung der Gesetzesanforderungen nach §65 (1) 2 wird nicht nachgekommen • Anweisungen zur Veröffentlichung von Verstößen nach §65 (3) wird nicht nachgekommen

Quelle: www.openkritis.de

Umsetzung von NIS2: „Fast Path“

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

- Erstellung eines normgerechten **ISMS** (InformationSicherheitsManagementSystem)
- **Schwachstellen-Management** (Analyse, Behebung, Härtungen und Konfigurationen)
- Nutzung von **SSO** (SingleSignOn) 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 Informationssicherheitsbeauftragten (ISB) und einer Datenschutzmanager- Position (DSM)
- **Training** der **Mitarbeiter** und aller **Führungskräfte** (Training ist nicht an Mitarbeiter delegierbar)
- **Lieferkette:** Verträge mit „Partnern“ zum Thema „Cybersecurity“
- **Reporting** (Prozesse) von Vorfällen inkl. „Beinahevorfall“ an Behörden – auch von nur „wichtigen“ Unternehmen

Wenn Sie schon nach ISO 27000 oder VdS 10000 zertifiziert sind, haben Sie typischerweise schon einige der obigen Punkte abgedeckt. Trotzdem zeigt die Praxis vieler Unternehmen, dass noch erhebliche Lücken existieren.

CAIRO als IT Compliance & Security Beratungsfirma kann diese schnell schließen. Typischerweise starten wir mit einem CAIRO CyberRisikoCheck (CRC) und einem CAIRO CyberSecurity-Check (CSC) für die Planung der notwendigen Schutz-Maßnahmen. Beide Überprüfungen sind BSI-konform. Der CSC beinhaltet eine NIS2 GAP-Analyse.

Wir liefern ebenso spezielle Lösungen für die Schwachstellenbehebung wie auch fertige ISMS-Baukästen/Bausteine im Bereich der Dokumentation, der Verfahren und Tools, die Ihnen helfen, schnell gesetzeskonform zu werden.

Die NIS2 Compliance Beratung ist Teil unseres Security & Compliance Portfolios von normgerechten Security-Prüfungen, über das Schwachstellen-Management bis zum sicheren IT-Betrieb mit modernen Lösungen, CAIRO Security Managed Service oder Security Awareness Trainings.

CAIRO ist VdS 10000 zertifiziert für ein Informationssicherheits-Management System (ISMS).

Tel.: +49 (0)621 86 75 10

Mail: info@cairo.ag

Web: www.cairo.ag

CAIRO

secure • digital • IT-infrastructures

Kontakt