SECJUR

NIS2 für die Energiebranche

Warum Energieversorger und Netzbetreiber besonders im Fokus stehen, und wie NIS2-Readiness strukturiert gelingt.

Die Energiebranche gehört zu den kritischsten Sektoren unter NIS2. Strom-, Gas- und Wärmeversorger sowie Netzbetreiber sind als **besonders wichtige Einrichtungen** eingestuft und unterliegen den strengsten Anforderungen des NIS2-Umsetzungsgesetzes (NIS2UmsuCG). Hinzu kommen branchenspezifische Vorgaben aus dem Energiewirtschaftsgesetz (§§ 5c–5e EnWG). Wer OT-Systeme, SCADA-Infrastruktur oder kritische Netzleittechnik betreibt, muss **jetzt handeln.**

In diesen vier Situationen wird NIS2 für Energieunternehmen konkret:

BETROFFENHEIT & EINSTUFUNG

Automatisch im Fokus

- Energieversorger und Netzbetreiber gelten als besonders wichtige Einrichtungen
- Einstufung unabhängig von der Unternehmensgröße
- Auch Tochtergesellschaften und kleinere Verteilnetze betroffen
- Frühe Einordnung nach §28 NIS2UmsuCG ist Pflicht

OT/SCADA-SICHERHEIT

Betriebstechnik absichern

- Steuerungssysteme (OT) und SCADA sind besonders exponiert
- NIS2 fordert Angriffserkennung, Segmentierung, Schwachstellenmanagement
- Gilt auch für Betriebstechnik, nicht nur klassische IT
- Veraltete Legacy-Systeme ohne Patch-Support sind das größte Risiko

MELDEPFLICHTEN & BSI

24-Stunden-Frist

- Erhebliche Vorfälle innerhalb von 24 Stunden melden
- KRITIS-Betreiber: zusätzliche BSI-Registrierungspflicht
- Verpflichtende Prüfung alle drei Jahre
- Ohne vorbereiteten Meldeprozess wird der Ernstfall zur Katastrophe

LEITUNGSHAFTUNG

Chefsache mit Bußgeldrisiko

- Management haftet persönlich für Umsetzung und Überwachung
- Cybersicherheitstraining ist Pflicht
- Bußgelder bis 10 Mio. Euro oder 2 % des globalen Jahresumsatzes
- Rechtsgrundlage: §65 NIS2UmsuCG

Annex 1

Energiesektor als besonders wichtige Einrichtung, höchste NIS2-Pflichtklasse

24 h

Frist für die Erstmeldung erheblicher Sicherheitsvorfälle an die Behörde

bis 10 Mio. €

Maximales Bußgeld für besonders wichtige Einrichtungen bei Verstößen

SECJUR

NIS2-Readiness in 6 Schritten

Von der Betroffenheitsprüfung bis zur KRITIS-Auditfähigkeit, strukturiert und branchenspezifisch für Energieunternehmen.

SCHRITT 01

Betroffenheit & Einstufung

- [ ] **Einstufung** als besonders wichtige vs. wichtige Einrichtung prüfen (§28)
- [ ] **EnWG §§5c–5e** als branchenspezifische Regelungen berücksichtigen
- [ ] **Tochtergesellschaften** und Betriebseinheiten einbeziehen
- [ ] **BSI-Registrierungspflicht** für KRITIS-Betreiber klären
- [ ] **Einordnung** dokumentieren und laufend aktuell halten

SCHRITT 02

OT/IT-Asset-Inventar

- [ ] **Kritische OT-Systeme,** SCADA und Netzleittechnik erfassen
- [ ] **Schnittstellen** zwischen IT- und OT-Netz dokumentieren
- [ ] **Legacy-Systeme** ohne Patch-Support identifizieren
- [ ] **Verantwortlichkeiten** für OT-Assets festlegen
- [ ] **Asset-Inventar** zentral und nachvollziehbar führen

SCHRITT 03

Risikoanalyse & Maßnahmen

- [ ] **Bedrohungen** für OT/SCADA und IT-Infrastruktur bewerten
- [ ] **Netzwerksegmentierung** und Zugriffskontrolle prüfen
- [ ] **Angriffserkennung** (IDS/IPS) für OT-Umgebungen einplanen
- [ ] **Maßnahmen** nach §30 Abs. 2 NIS2UmsuCG dokumentieren
- [ ] **Risiken** priorisieren und Verantwortliche zuordnen

SCHRITT 04

Business Continuity

- [ ] **Backup-** und Notfallwiederherstellungspläne für kritische Systeme
- [ ] **Krisenszenarien** (Stromausfall, Cyberangriff) testen
- [ ] **Redundanzen** in Leit- und Steuerungstechnik sicherstellen
- [ ] **Wiederherstellungszeit** (RTO/RPO) für Kernsysteme definieren
- [ ] **Pläne** regelmäßig üben und aktualisieren

SCHRITT 05

Vorfallsmanagement & Meldung

- [ ] **Incident-Response-Prozess** für IT und OT aufbauen
- [ ] **24-Stunden-Meldekette** an BSI/Behörde einrichten
- [ ] **Meldevorlagen** für Erst- (24 h), Folge- (72 h) und Abschlussbericht
- [ ] **Verantwortliche** für Vorfallsreaktion benennen und schulen
- [ ] **Meldeprozess** regelmäßig testen

SCHRITT 06

Leitung & Auditfähigkeit

- [ ] **Management** in Risikomaßnahmen einbinden und schulen (§38)
- [ ] **KRITIS-Audit** alle 3 Jahre vorbereiten (§39 NIS2UmsuCG)
- [ ] **Nachweise,** Richtlinien und Logs zentral ablegen
- [ ] **Maßnahmeneffektivität** jährlich überprüfen
- [ ] **Kontinuierliche Verbesserung** fest verankern

SECJUR

Häufige Stolperfallen und Quick Wins

Was Energieunternehmen bei NIS2 typischerweise unterschätzen, und womit sich schnell Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

OT als blinder Fleck

- [ ] **NIS2-Anforderungen** nur auf klassische IT-Systeme angewendet
- [ ] **SCADA und Leitstellen** ohne eigenes Sicherheitskonzept betrieben
- [ ] **OT-spezifische Angriffserkennung** fehlt komplett
- [ ] **Betriebstechnik** von Anfang an mitdenken, nicht nachrüsten

QUICK WIN 01

IT/OT-Segmentierung

- [ ] **Netzwerktrennung** zwischen Büro-IT und Leitstelle sofort umsetzen
- [ ] **Günstige Maßnahme** mit hoher Schutzwirkung
- [ ] **Angriffsfläche** wird erheblich und schnell reduziert
- [ ] **Erster sichtbarer Fortschritt** Richtung NIS2-Readiness

STOLPERFALLE 02

Lieferkette unterschätzt

- [ ] **Dienstleister** und Systemlieferanten ohne Sicherheitsanforderungen
- [ ] **Fernwartungszugänge** nicht ausreichend abgesichert
- [ ] **Vertraglich** keine NIS2-konformen Anforderungen verankert
- [ ] **Keine Übersicht** über kritische Abhängigkeiten

QUICK WIN 02

Synergien mit ISO 27001

- [ ] **Bestehendes ISMS** ist direkt auf NIS2 anrechenbar
- [ ] **Gap-Analyse** zeigt konkrete Ergänzungsbedarfe
- [ ] **Ein Rahmenwerk** für beide Welten statt Doppelaufwand
- [ ] **Bestehende Controls** gezielt auf NIS2 mappen

STOLPERFALLE 03

Zu späte Management-Einbindung

- [ ] **Cybersicherheit** als rein technisches Thema behandelt
- [ ] **Leitungsebene** nicht in Risikomaßnahmen eingebunden
- [ ] **Persönliche Haftung** nach §38 NIS2UmsuCG ignoriert
- [ ] **Frühe Einbindung** schützt Unternehmen und Leitung

QUICK WIN 03

Meldeprozess als Checkliste

- [ ] **Meldevorlage** für das BSI in rund zwei Stunden erstellt
- [ ] **Verantwortlichkeiten** auf einer A4-Seite festhalten
- [ ] **Im Ernstfall** enorm stressreduzierend
- [ ] **Von Unsicherheit** zu handlungsfähiger Meldekette

SECJUR

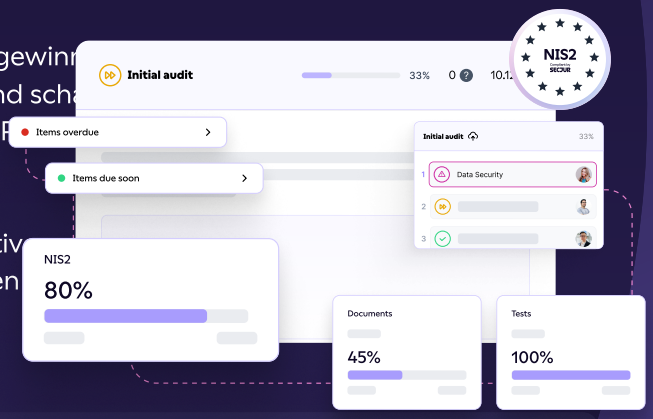
Mit SECJUR zu 100 % NIS2-Compliance

Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- Aufbau und Betrieb eines NIS2-konformen ISMS inkl. Risiko- und Incident-Management
- Klare Verantwortlichkeiten, Dokumentation und Nachweise für Behörden
- Profitieren Sie von der dedizierten Erfahrung unserer TÜV-geprüften Expert:innen

Reduzieren Sie manuellen Aufwand deutlich, gewinn
Transparenz über Ihren Compliance-Status und sch
eine belastbare Grundlage für regulatorische
und anspruchsvolle Kundenanforderungen.



Für unsere Bestandskunden bieten wir attraktiv
Konditionen, um frühzeitig Klarheit zu schaffen
NIS2-Readiness planbar umzusetzen.

→ **Jetzt informieren**

Mit SECJUR zu Informationssicherheitszertifizierungen:

Dank SECJUR konnten wir schnell ein hochwertiges ISMS aufbauen, wie uns auch in den Zertifizierungsaudits bestätigt wurde. Unser zugewiesener Berater hat uns stets kompetent unterstützt – als wäre er ein Teil der Firma. Freuen uns auf die weitere Zusammenarbeit!

Stefan Gregori
Chief Information Security Officer

CONSOLINNO energy

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

1KOMMA5° · Stadtwerke Kamp-Lintfort · Consolinno Energy · Stadtwerke Nienburg Energie · Changing Cities · CUBOS

www.secjur.com