

NIS2 für Städtische Ver- und Entsorgung

Warum Wasserversorgung, Abwasser und Abfallwirtschaft unter NIS2 fallen, und wie Readiness gelingt.

Städtische Ver- und Entsorgungsunternehmen gehören zur kritischen Infrastruktur Deutschlands. Wasser, Abwasser und Abfallwirtschaft sind explizit im NIS2-Umsetzungsgesetz (NIS2UmsuCG) gelistet, Betreiber fallen in der Regel als **besonders wichtige Einrichtungen** unter die schärfsten Anforderungen. Das bedeutet: proaktive Überwachung durch das BSI, strenge Meldepflichten und persönliche Haftung der Geschäftsführung.

In diesen vier Situationen wird NIS2 für die Ver- und Entsorgungsbranche konkret:

KRITISCHE INFRASTRUKTUR

Anhang 1, KRITIS

- Trinkwasser, Abwasser und Abfallwirtschaft in Anhang 1 NIS2UmsuCG gelistet
- Betreiber ab 250 Beschäftigten oder 50 Mio. Euro Umsatz sind besonders wichtig
- Auch kleinere Betreiber können als wichtige Einrichtungen gelten
- Frühe, dokumentierte Einordnung ist Pflicht

OT/IT-SICHERHEIT & SCADA

Steuerungsnetze absichern

- Ver- und Entsorgungsnetze steuern kritische Prozesse über OT und SCADA
- NIS2 verlangt explizit Angriffserkennung für die Steuerungsinfrastruktur
- Veraltete Systeme und fehlende Netzwerktrennung sind die häufigsten Schwachstellen
- Gilt ausdrücklich auch für die Betriebstechnik

MELDE- & REGISTRIERUNGSPFLICHT

24 Stunden ans BSI

- Erhebliche Vorfälle innerhalb von 24 Stunden ans BSI melden
- Folgemeldung nach 72 Stunden, Abschlussbericht nach einem Monat
- Betreiber kritischer Anlagen: System zur Angriffserkennung (§31)
- Ohne vorbereiteten Meldeprozess wird der Ernstfall zum Risiko

GESCHÄFTSFÜHRER-HAFTUNG

Chefsache mit Bußgeldrisiko

- Leitungsebene muss Risikomaßnahmen genehmigen und überwachen
- Schulungspflicht für die Geschäftsführung
- Bußgelder bis 10 Mio. Euro oder 2 % des weltweiten Umsatzes
- Cybersicherheit wird zur persönlichen Verantwortung



Anhang 1

NIS2UmsuCG: Wasser, Abwasser und Abfallwirtschaft als kritische Sektoren eingestuft

24 Std.

Frühwarnung bei erheblichen Vorfällen, mehrstufige Meldepflicht bis zum Abschlussbericht

10 Mio. €

Maximales Bußgeld für besonders wichtige Einrichtungen bei Verstößen gegen NIS2

NIS2-Readiness in 6 Schritten

Eine praxiserprobte Reihenfolge für Ver- und Entsorgungsunternehmen, von der Betroffenheitsprüfung bis zur betriebssicheren Meldefähigkeit.

SCHRITT 01

Betroffenheit & Einstufung

- ☐ **Sektor prüfen:** Trinkwasser, Abwasser oder Abfallwirtschaft gemäß Anhang 1
- ☐ **Größenmerkmale** abgleichen (ab 250 MA oder 50 Mio. € Umsatz)
- ☐ **Einstufung** besonders wichtig vs. wichtig dokumentieren
- ☐ **Tochtergesellschaften** und Konzernstruktur einbeziehen
- ☐ **Ergebnis** bei Unsicherheit fachlich gegenprüfen

SCHRITT 02

Registrierung beim BSI

- ☐ **Zuständige Behörde** und Meldeweg beim BSI klären
- ☐ **Kontaktstelle (SPOC)** und Verantwortliche benennen
- ☐ **Stammdaten** der Einrichtung zusammenstellen
- ☐ **Registrierungsfrist** im Kalender verankern
- ☐ **Änderungen** laufend aktuell halten

SCHRITT 03

OT/IT-Risiken analysieren

- ☐ **Kritische Assets** in OT/SCADA und IT erfassen
- ☐ **Netzwerktrennung** zwischen IT und OT prüfen
- ☐ **Schwachstellen** in Steuerungssystemen und Fernzugriffen bewerten
- ☐ **Risiken** priorisiert dokumentieren
- ☐ **Verantwortliche** je Risiko zuordnen

SCHRITT 04

Schutzmaßnahmen umsetzen

- ☐ **MFA, Zugriffskontrolle** und Härtung für IT und OT etablieren
- ☐ **Backup-, Patch-** und Verschlüsselungsprozesse einrichten
- ☐ **System zur Angriffserkennung (§31)** implementieren
- ☐ **Lieferanten- und Dienstleisterrisiken** vertraglich adressieren
- ☐ **Maßnahmen** als verbindliche Richtlinien dokumentieren

SCHRITT 05

Incident Response & Meldung

- ☐ **Incident-Response-Plan** inkl. OT-Szenarien definieren
- ☐ **Meldekette** für 24h-Frühwarnung und 72h-Folgemeldung aufsetzen
- ☐ **Vorlagen** für BSI-Meldungen vorbereiten
- ☐ **Krisenkommunikation** intern und extern abstimmen
- ☐ **Meldeprozess** regelmäßig testen

SCHRITT 06

Leitung & Schulung

- ☐ **Geschäftsführung** in Risikomaßnahmen einbinden und schulen
- ☐ **Billigung** und Überwachung der Maßnahmen dokumentieren
- ☐ **Awareness-Schulungen** für das Betriebspersonal etablieren
- ☐ **Jährliches Review** der Schutzmaßnahmen einplanen
- ☐ **Verbesserungen** nachhalten und dokumentieren

Häufige Stolperfallen und Quick Wins

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

STOLPERFALLE 01

OT-Systeme vergessen

- ☐ IT-Sicherheit umgesetzt, SCADA und Steuerungsnetze aber nicht
- ☐ Veraltete OT-Systeme sind oft ungepatcht und ungeschützt
- ☐ NIS2 erfasst ausdrücklich auch die Betriebstechnik
- ☐ OT von Anfang an ins Sicherheitskonzept einbeziehen

QUICK WIN 01

Netzwerktrennung sofort prüfen

- ☐ IT und OT segmentieren reduziert die Angriffsfläche sofort
- ☐ Oft mit geringem Aufwand umsetzbar
- ☐ Hohe Wirkung bei Auditoren und BSI
- ☐ Erster sichtbarer Fortschritt Richtung NIS2-Readiness

STOLPERFALLE 02

Meldeprozess fehlt

- ☐ Im Ernstfall fehlt eine vorbereitete Meldekette
- ☐ 24-Stunden-Frist wird unter Druck verpasst
- ☐ Fehlende Vorlagen erzeugen doppelten Stress
- ☐ Vorbereitete Meldekette entschärft den Ernstfall

QUICK WIN 02

Dokumentation zentralisieren

- ☐ Richtlinien und Nachweise an einem Ort bündeln
- ☐ Erleichtert spätere BSI-Prüfungen erheblich
- ☐ Verantwortliche und Review-Zyklen je Dokument festlegen
- ☐ Sofortige Übersicht über den Handlungsbedarf

STOLPERFALLE 03

Lieferkette unterschätzt

- ☐ Externe Wartungsdienstleister haben oft direkten OT-Zugriff
- ☐ Sicherheitsanforderungen nicht vertraglich verankert
- ☐ Ein Vorfall beim Dienstleister trifft den Betreiber mit
- ☐ Fernzugänge überwachen und zeitlich begrenzen

QUICK WIN 03

Früh einordnen lassen

- ☐ Betroffenheit fachlich gegenchecken lassen
- ☐ Maßnahmen nach Priorität und Wirkung sortieren
- ☐ Readiness-Roadmap realistisch aufsetzen
- ☐ Von Unsicherheit zu planbarer Readiness



Mit SECJUR zu 100 % NIS2-Compliance

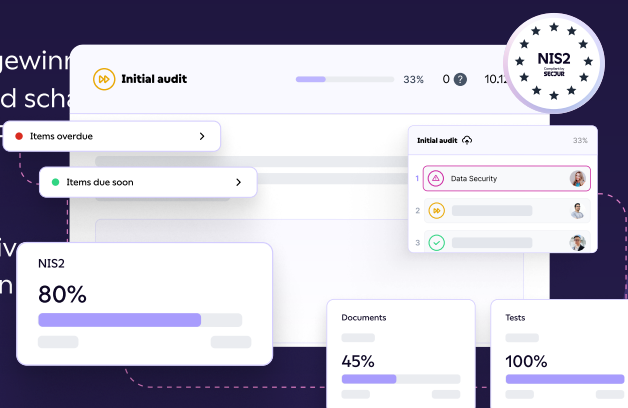
Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

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, gewinnen Transparenz über Ihren Compliance-Status und schaffen eine belastbare Grundlage für regulatorische Anforderungen und anspruchsvolle Kundenanforderungen.

Für unsere Bestandskunden bieten wir attraktive Konditionen, um frühzeitig Klarheit zu schaffen und 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



FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR



www.secjur.com