SECJUR

WHITEPAPER
2026

NIS2 · STADTWERKE, KOMMUNALE VER- UND ENTSORGUNG

NIS2 für Ver- und Entsorgung: Daseinsvorsorge absichern.

Wasser, Abwasser, Abfall, Strom, Gas und Fernwärme sind die Lebensadern jeder Kommune. Trinkwasser, Abwasser und Energie zählen zu den Sektoren hoher Kritikalität nach NIS2, die Abfallwirtschaft zu den sonstigen kritischen Sektoren. Viele Stadtwerke sind bereits als KRITIS-Betreiber reguliert, NIS2 erweitert den Kreis über die bekannten Schwellen hinaus. Dieses Whitepaper zeigt, wer nun betroffen ist, wo die Betriebstechnik angreifbar ist und wie ein ISMS entsteht, das NIS2, KRITIS-Nachweis und Datenschutz gemeinsam trägt.

NIS2 · KRITIS · ISO 27001 · B3S · ISO 27019 · DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Für die Ver- und Entsorgung ist Sicherheit gelebte Daseinsvorsorge.

DAS WICHTIGSTE IN KÜRZE

Das NIS2-Umsetzungsgesetz gilt seit dem 6. Dezember 2025 ohne Übergangsfrist. Trinkwasser, Abwasser und Energie, also Strom, Gas und Fernwärme, zählen zu den Sektoren hoher Kritikalität nach Anlage 1, die Abfallbewirtschaftung zu den sonstigen kritischen Sektoren nach Anlage 2. Für Stadtwerke und kommunale Ver- und Entsorger heißt das: Der regulatorische Rahmen ist gesetzt und die Betroffenheit muss belastbar geklärt sein.

Viele größere Versorger sind bereits als KRITIS-Betreiber nach der BSI-Kritisverordnung reguliert und gelten damit automatisch als besonders wichtige Einrichtungen. NIS2 senkt die Eintrittsschwelle darunter: Wer 50 Beschäftigte oder 10 Millionen Euro Umsatz erreicht, fällt als wichtige Einrichtung neu unter das Gesetz. Ein ISMS nach ISO 27001 bündelt NIS2, die KRITIS-Nachweispflicht und den Datenschutz in einem System. Wer die Betroffenheit sauber dokumentiert, schafft Klarheit und schützt die Leitung vor Haftung.

WARUM JETZT HANDELN

Der Druck kommt von mehreren Seiten. Betroffene Einrichtungen mussten sich bis zum 31. Juli 2026 beim BSI registrieren, KRITIS-Betreiber weisen ihre Maßnahmen zusätzlich alle zwei Jahre nach.

Kommunale Gremien, Aufsichtsräte und Rechnungsprüfung fragen den Stand der Umsetzung inzwischen aktiv ab.

Hinzu kommt die Bedrohungslage. Angriffe auf die Betriebs- und Leittechnik von Wasserwerken, Kläranlagen und Netzen haben spürbar zugenommen, und ein Ausfall trifft nicht nur die IT, sondern die Grundversorgung der Bürgerinnen und Bürger. Wer den Nachweis früh aufbaut, begegnet Aufsicht und Öffentlichkeit aus einer Position der Stärke.

EIN AUFBAU, MEHRERE PFLICHTEN

Die gute Nachricht: Der Aufwand lohnt mehrfach. Ein einmal aufgebautes ISMS trägt die NIS2-Pflichten, den KRITIS-Nachweis, die branchenspezifischen Standards und den Datenschutz zugleich, auch im kommunalen Querverbund über Sparten und Standorte hinweg.

Die folgenden Seiten liefern die Grundlage: den Sektorkontext, die konkreten Risiken rund um Betriebstechnik und Bürgerdaten, die gesetzlichen Pflichten und eine Roadmap, die zur kommunalen Realität passt. So entsteht Sicherheit, die im Ernstfall trägt und den Betrieb absichert, statt in Doppelarbeit zu versickern.

EINSTUFUNG

Anlage 1

Trinkwasser, Abwasser und Energie zählen zu den Sektoren hoher Kritikalität.

SCHWELLE NEU

50 MA

Ab 50 Beschäftigten oder 10 Mio. Euro Umsatz greift NIS2 als wichtige Einrichtung.

EIN AUFBAU

1 ISMS

Deckt NIS2, KRITIS-Nachweis, B3S / ISO 27019 und DSGVO gemeinsam ab.

BRANCHENKONTEXT

Ver- und Entsorgung ist kritische Infrastruktur.

Kaum eine Branche ist so unmittelbar für das Gemeinwesen wie die Ver- und Entsorgung. Fällt sie aus, steht das öffentliche Leben still. Genau deshalb rückt sie ins Zentrum von NIS2. Ein ISMS macht die Absicherung dieser Systeme nachweisbar.

Wenn das Wasser stillsteht, steht die Stadt still. *Diese Verantwortung verpflichtet.*

VIER SEKTOREN, EIN AUFTRAG

Trinkwasserversorgung, Abwasserbeseitigung und die Energieversorgung mit Strom, Gas und Fernwärme zählen nach Anlage 1 zu den Sektoren hoher Kritikalität. Die Abfallbewirtschaftung gehört nach Anlage 2 zu den sonstigen kritischen Sektoren. Für kommunale Ver- und Entsorger fällt damit fast das gesamte Leistungsspektrum in den Anwendungsbereich von NIS2.

Anders als bisher hängt die Betroffenheit nicht mehr allein an den hohen KRITIS-Schwellen. NIS2 erfasst nun auch mittelgroße Versorger und Entsorger unterhalb der Versorgungsgrenzen. Ein Blick auf die eigenen Sparten und Kennzahlen zeigt schnell, welche Rolle zutrifft.

DER KOMMUNALE QUERVERBUND

Stadtwerke bündeln typischerweise mehrere Sparten unter einem Dach: Strom, Gas, Wasser, Wärme, Abfall, oft auch Nahverkehr und Telekommunikation. Damit treffen mehrere NIS2-Sektoren in einem Unternehmen zusammen, mit gemeinsamer IT, aber sehr unterschiedlicher Betriebstechnik.

Das ist Chance und Herausforderung zugleich. Ein zentral geführtes ISMS kann alle Sparten tragen, muss aber die Eigenheiten jeder Anlage abbilden. Wer den Geltungsbereich klug schneidet, sichert den Verbund mit einem System statt mit vielen Insellösungen.

KRITIS BLEIBT, NIS2 KOMMT HINZU

Größere Versorger sind bereits als KRITIS-Betreiber nach der BSI-Kritisverordnung reguliert, mit Nachweispflicht nach Paragraf 8a BSIG und branchenspezifischen Sicherheitsstandards. Diese Pflichten bestehen fort und gelten unter NIS2 als besonders wichtige Einrichtungen weiter. NIS2 ergänzt sie um eine breitere Betroffenheit und einheitliche Mindestmaßnahmen.

WAS AUF DEM SPIEL STEHT

Ein Ausfall in der Ver- und Entsorgung trifft unmittelbar Menschen: kein Trinkwasser, keine Wärme, überlaufende Kläranlagen, liegengebliebener Abfall. Der Schaden ist nicht nur wirtschaftlich, sondern eine Gefahr für die öffentliche Gesundheit und Sicherheit.

Sicherheit schützt hier die Daseinsvorsorge selbst. Ein belastbarer Nachweis sichert das Vertrauen von Bürgern, Kommune und Aufsicht und damit die Handlungsfähigkeit des Versorgers im Ernstfall. Wer die Absicherung früh belegt, muss im Krisenfall nicht erst Vertrauen zurückgewinnen.

HERAUSFORDERUNGEN

Warum die Umsetzung in der Versorgung besonders fordert.

Die NIS2-Anforderungen gelten unabhängig von der Größe des Versorgers. Der kommunale Betrieb bringt aber eigene Bedingungen mit. Sechs Eigenheiten machen die Umsetzung speziell, und für jede gibt es einen pragmatischen Umgang.

BETRIEBSTECHNIK TRIFFT IT

Wasserwerke, Kläranlagen und Netze laufen auf Prozessleit- und Fernwirktechnik, die oft jahrzehntelang im Einsatz bleibt und nicht für die Vernetzung gebaut wurde. Diese Betriebstechnik lässt sich nicht wie ein Büro-PC einfach patchen. NIS2 verlangt Sicherheit für IT und OT gemeinsam. Der Schlüssel liegt in Segmentierung, Zugriffskontrolle und Monitoring, statt in riskanten Eingriffen in den laufenden Betrieb.

VERFÜGBARKEIT HAT VORRANG

In der Versorgung darf nichts stillstehen. Eine Anlage lässt sich nicht für ein Sicherheitsupdate abschalten, und jede Maßnahme muss den unterbrechungsfreien Betrieb berücksichtigen. Das unterscheidet die Branche von der klassischen Büro-IT. Ein ISMS, das die Verfügbarkeit als obersten Schutzwert versteht, findet den richtigen Rhythmus für Wartungs- und Wartungsfenster.

KOMMUNALE STRUKTUREN

Stadtwerke stehen zwischen kommunaler Trägerschaft, Aufsichtsrat und wirtschaftlichem Betrieb. Entscheidungen brauchen Gremienbeschlüsse, Budgets sind an Haushalte gebunden, und die Verwaltung ist oft eng getaktet. NIS2 verlangt dennoch klare Verantwortung und Tempo. Eine früh eingebundene Leitung und ein klarer Fahrplan halten das Thema aus dem politischen Klein-Klein heraus.

DÜNNE IT-SICHERHEITSDECKE

Viele kommunale Versorger haben eine IT-Abteilung, aber selten eine eigene OT-Sicherheitsfunktion. NIS2 und die branchenspezifischen Standards verlangen Struktur, Dokumentation und Wirksamkeitskontrolle, nicht Heldentaten Einzelner. Werkzeuge, die durch die Anforderungen führen und dokumentieren, ersetzen hier ein Stück weit das fehlende Spezialwissen.

LIEFERANTEN UND DIENSTLEISTER

Anlagenbauer, Fernwartung und IT-Dienstleister haben oft tiefen Zugriff auf die Betriebstechnik. NIS2 macht die Lieferkette ausdrücklich zur Pflicht. Wer seine Dienstleister vertraglich bindet, Fernzugänge absichert und Nachweise einfordert, schließt ein häufig unterschätztes Einfallstor.

NACHWEIS FÜR ZWEI RAHMEN

KRITIS-Betreiber kennen die Nachweispflicht bereits, für neu betroffene Einrichtungen ist sie neu. Statt KRITIS-Nachweis, NIS2-Maßnahmen und branchenspezifische Standards getrennt zu führen, lohnt sich ein gemeinsames System. Ein ISMS bündelt die Anforderungen und macht jeden Nachweis nur einmal erforderlich. So sinkt der Aufwand, und die Prüfungen von KRITIS und NIS2 lassen sich aufeinander abstimmen.

BEDROHUNGSLAGE & RISIKEN

Wo die Ver- und Entsorgung konkret angreifbar ist.

Die Risiken sind in der Versorgung selten abstrakt. Sie hängen an vernetzter Betriebstechnik, an langen Anlagenlebenszyklen und an einer Infrastruktur, die nicht ausfallen darf. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · ANGRIFF AUF DIE LEITTECHNIK

Der schwerste Ernstfall. Werden Prozessleit- oder Fernwirksysteme manipuliert, drohen Fehldosierungen im Wasserwerk, Störungen in der Kläranlage oder Ausfälle im Netz. Solche Angriffe zielen unmittelbar auf die physische Versorgung und die öffentliche Gesundheit. Segmentierung zwischen IT und OT, strenge Zugriffskontrolle und ein Monitoring der Leittechnik sind hier unverzichtbar. Wer den Ernstfall nie geübt hat, verliert im Angriff die wertvollste Zeit. Ein aktueller Notfallplan legt vorab fest, wer im Stillstand was entscheidet.

2 · RANSOMWARE LEGT DEN BETRIEB LAHM

Werden Verwaltungs- und Abrechnungssysteme verschlüsselt, stehen Abrechnung, Disposition und Kundenservice still, im schlimmsten Fall greift der Angriff auf die Steuerung über. Versorger gelten Angreifern als lohnendes Ziel, weil ein Ausfall der Grundversorgung enormen Druck erzeugt. Getestete Backups und ein eingeübter Notfallplan entscheiden, wie schnell der Betrieb zurückkehrt. Getrennte Sicherungen der Betriebs- und der Bürodaten verhindern, dass ein Angriff beides zugleich trifft.

3 · FERNWARTUNG UND LIEFERKETTE

Anlagenbauer und Dienstleister warten Steuerungen häufig aus der Ferne. Ein kompromittierter Fernzugang oder eine manipulierte Softwarelieferung öffnet Angreifern direkt den Weg in die Betriebstechnik. Abgesicherte Fernzugänge mit Mehrfaktor-Anmeldung, protokollierte Zugriffe und vertraglich gebundene Dienstleister schließen dieses Einfallstor. Wer weiß, wer wann auf welche Anlage zugreift, erkennt ungewöhnliche Zugriffe früh.

4 · BÜRGER- UND VERBRAUCHSDATEN

Versorger verwalten Zähler-, Verbrauchs- und Abrechnungsdaten großer Teile der Bevölkerung. Ein Abfluss dieser Daten ist ein Verstoß gegen die DSGVO und beschädigt das Vertrauen der Bürgerinnen und Bürger. Verschlüsselung, rollenbasierte Zugriffskontrolle und eine Protokollierung der Zugriffe schützen diese Bestände. Wer weiß, wo die sensibelsten Daten liegen, kann sie zuerst und am stärksten schützen.

5 · PHYSISCHE UND HYBRIDE ANGRIFFE

Anlagen der Ver- und Entsorgung sind räumlich weit verteilt, von der Pumpstation bis zum Umspannwerk. Unbefugter Zutritt, Sabotage oder eine Kombination aus physischem und digitalem Angriff sind reale Szenarien. Zutrittskontrolle, Überwachung entlegener Standorte und eine enge Verzahnung von physischer und IT-Sicherheit gehören deshalb zusammen. Das KRITIS-Dachgesetz verstärkt diese Pflicht zur physischen Resilienz zusätzlich. Wer physische und digitale Meldewege zusammenführt, erkennt einen kombinierten Angriff schneller als jede Einzeldisziplin für sich.

REGULATORISCHE PFLICHTEN

Was NIS2 und KRITIS konkret verlangen.

Ein Rahmen, mehrere Ebenen. NIS2 setzt einheitliche Mindestmaßnahmen, die KRITIS-Regulierung und die branchenspezifischen Standards ergänzen sie. Fünf Bausteine muss jeder Versorger kennen: Betroffenheit (§28), Risikomanagement (§30), Meldepflichten (§32), Leitungspflichten (§38) und Sanktionen (§65).

§28 · BETROFFENHEIT UND REGISTRIERUNG

Ob ein Versorger unter NIS2 fällt, hängt von Sektor und Größe ab. KRITIS-Betreiber gelten automatisch als besonders wichtige Einrichtungen. Darunter greifen die Schwellen: ab 250 Beschäftigten oder 50 Millionen Euro Umsatz als besonders wichtig, ab 50 Beschäftigten oder 10 Millionen Euro als wichtig. Betroffene Einrichtungen registrieren sich über das BSI-Portal, KRITIS-Betreiber benennen zusätzlich eine Kontaktstelle. Wer die Prüfung dokumentiert, schafft Klarheit über die eigene Rolle.

§30 · DIE TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Verlangt werden angemessene Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, Zugriffskontrolle, Kryptografie und Mehrfaktor-Authentifizierung. In der Versorgung erstrecken sich diese Pflichten ausdrücklich auf die Betriebs- und Leittechnik, nicht nur auf die Büro-IT. Branchenspezifische Standards wie der B3S für Wasser und Abwasser oder die ISO 27019 für die Energieversorgung konkretisieren, was angemessen ist. Entscheidend ist, dass jede Maßnahme nachweisbar gelebt und regelmäßig überprüft wird. Ein regelmäßiger Soll-Ist-Abgleich hält die Maßnahmen auf dem Stand der Technik.

§32 · MELDEFRISTEN

Für betroffene Einrichtungen gilt eine gestufte Meldepflicht an das BSI: eine Erstmeldung binnen 24 Stunden, eine Meldung binnen 72 Stunden und ein Abschlussbericht binnen eines Monats. Bei Datenpannen greift parallel die 72-Stunden-Meldung an die Datenschutzaufsicht. Nur ein vorab geübter Prozess hält diese Fristen. Ein vorbereitetes Meldeformular und klare Zuständigkeiten sparen im Ernstfall wertvolle Minuten.

§38 · LEITUNG TRÄGT DIE VERANTWORTUNG

Geschäftsführung und Werkleitung müssen die Maßnahmen billigen, ihre Umsetzung überwachen und sich schulen lassen. Die Verantwortung ist nicht delegierbar, auch nicht an den externen IT-Dienstleister oder Anlagenbauer. Im kommunalen Umfeld gehört der Aufsichtsrat eingebunden. Das dokumentierte Engagement der Leitung ist im Ernstfall ein Nachweis gelebter Sorgfalt.

§65 · SANKTIONEN UND VERHÄLTNISMÄSSIGKEIT

Für besonders wichtige Einrichtungen drohen Bußgelder bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes, für wichtige Einrichtungen bis zu 7 Millionen Euro oder 1,4 Prozent. Schwerer wiegt in der Versorgung oft der öffentliche Vertrauensverlust nach einem Ausfall. Zugleich gilt die Verhältnismäßigkeit: geschuldet ist ein Schutzniveau, das zu Größe und Risiko passt. Ein dokumentierter, gelebter Prozess ist im Prüffall die beste Verteidigung. Wer Lücken kennt und ihre Behebung plant, wird selbst bei einem Vorfall milder bewertet als ein untätiger Betreiber.

UMSETZUNG IN DER PRAXIS

In sechs Schritten zu einem belastbaren Nachweis.

Die Umsetzung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt vorhandene KRITIS- und Datenschutzstrukturen, statt bei null zu beginnen. Realistisch führt der Weg in wenigen Monaten zu einem auditbereiten Stand.

Wer den KRITIS-Nachweis schon kennt, hat das Fundament gelegt. *NIS2 und ISO 27001 bauen darauf auf.*

1 · BETROFFENHEIT UND GELTUNGSBEREICH

Prüfen, welche Sparten unter NIS2 fallen und ob eine KRITIS-Einstufung besteht, und den Scope klar schneiden: welche Sparten, welche Anlagen, welche Standorte, welche IT- und OT-Systeme. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und der wirksamste Hebel, um Aufwand und Kosten niedrig zu halten.

2 · FÜHRUNG UND LEITLINIE

Geschäftsführung und Werkleitung verabschieden die Sicherheitsleitlinie, benennen eine verantwortliche Person und stellen Ressourcen bereit. Im kommunalen Umfeld gehört der Aufsichtsrat eingebunden. Betroffene Einrichtungen nehmen die Registrierung beim BSI vor, KRITIS-Betreiber benennen ihre Kontaktstelle.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von den Leitsystemen der Wasserwerke und Kläranlagen über die Netzsteuerung bis zu Abrechnung und Bürgerdaten. Risiken für IT und OT gemeinsam bewerten, die Verfügbarkeit besonders gewichten und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse trennt das Kritische vom Nebensächlichen und macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Mit den wirksamsten Hebeln beginnen: Segmentierung von IT und OT, Zugriffskontrolle, Mehrfaktor-Anmeldung, abgesicherte Fernwartung und Backup. Jede Maßnahme so festhalten, dass sie im Audit Bestand hat. Eingriffe in die Leittechnik werden dabei so geplant, dass die Versorgung nicht unterbrochen wird.

5 · MELDE- UND NOTFALLPROZESS

Die Meldeketten für NIS2 und für Datenpannen einrichten, Zuständigkeiten klären und den Notfallplan an einer realistischen Anlagenstörung testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen und die Versorgung. Eine Übung pro Jahr zeigt, wo es noch hakt.

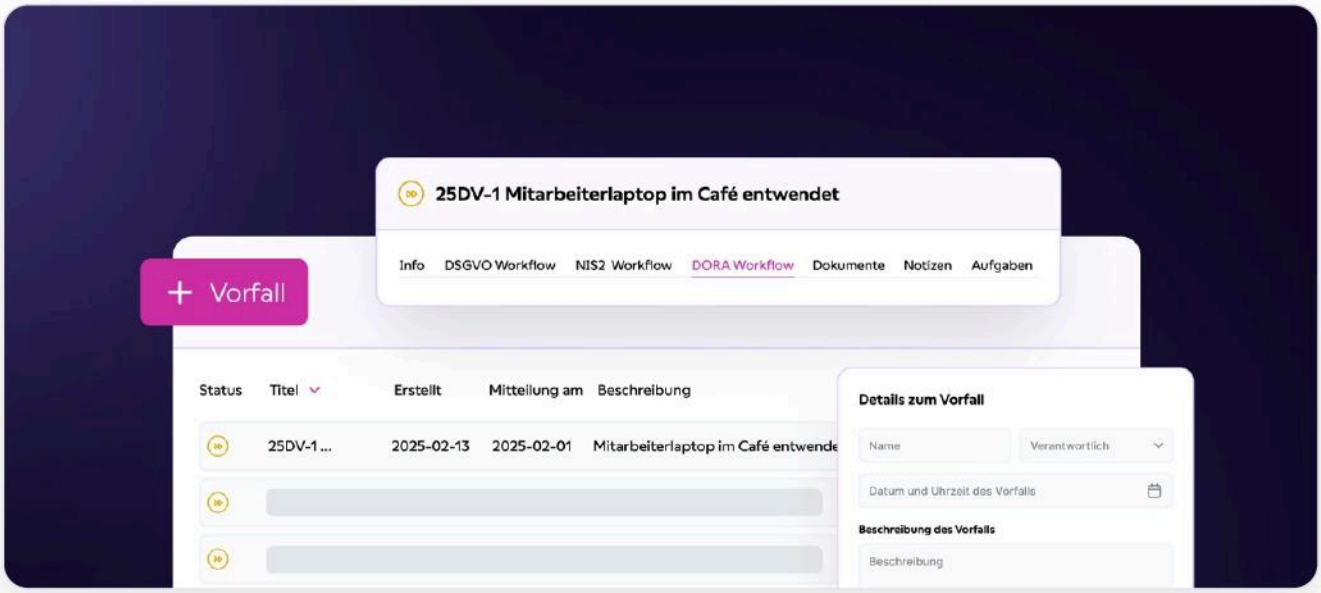
6 · PRÜFEN, NACHWEISEN, VERBESSERN

Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Wer den KRITIS-Nachweis bereits führt, kennt diese Logik. Wer die Schleife einmal vollständig durchläuft, ist zugleich reif für die ISO-27001-Zertifizierung und erfüllt den NIS2- und KRITIS-Nachweis aus demselben Aufbau. Der Aufwand von heute trägt so gleich mehrere Nachweise von morgen.

WIE SECJUR ES EINFACH MACHT

Vom Pflichtenrahmen zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) führt Stadtwerke und kommunale Ver- und Entsorger durch NIS2, KRITIS-Nachweis und Datenschutz zugleich: Risiken, Maßnahmen, Meldeprozess und Nachweise an einem Ort, mehrere Frameworks parallel. Statt teurer Beratung arbeiten Sie in einer Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Teams berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



IT und OT gemeinsam

Module für Segmentierung, Zugriffskontrolle und die Absicherung der Betriebs- und Leittechnik in Wasser, Abwasser, Abfall und Energie.

Querverbund im Blick

Ein zentral geführtes ISMS über alle Sparten und Standorte, das die Eigenheiten jeder Anlage abbildet statt Insellösungen zu erzeugen.

Mehrere Pflichten

NIS2, KRITIS-Nachweis, B3S / ISO 27019 und ISO 27001 laufen auf einem ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt mehrfach.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank. Sie legen den Geltungsbereich über die Sparten fest, das DCO führt durch jede Anforderung, und wo eine Expertin für OT-Sicherheit nötig ist, schalten wir sie zu. Sie entscheiden, das System dokumentiert im Hintergrund. So entsteht ein auditbereiter Nachweis in Wochen statt in Quartalen, ohne den Betrieb zu bremsen.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Assets und bestehende KRITIS- und Datenschutzmaßnahmen ab und leitet daraus die offenen Punkte ab. Jeder Schritt ist mit einer Vorlage hinterlegt, sodass niemand vor einem leeren Blatt sitzt.

Wo es schnell gehen muss, arbeitet das Team die wirksamsten Maßnahmen zuerst ab und verteilt den Rest planbar. Der Fortschritt bleibt für Leitung und Gremien jederzeit sichtbar.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2, KRITIS-Regulierung, branchenspezifische Standards und ISO 27001 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass IT und Betrieb an einer Quelle arbeiten statt an parallelen Tabellen.

Für einen Versorger heißt das weniger Doppelarbeit. Der KRITIS-Nachweis und der NIS2-Nachweis entstehen aus demselben Aufbau, statt in getrennten Projekten geführt zu werden.

Und weil die Belege aktuell bleiben, ist das Unternehmen für die nächste Prüfung durch Aufsicht oder Auditor vorbereitet, ohne kurzfristig Unterlagen zusammensuchen zu müssen. Aus einer Pflicht wird so ein dauerhafter Nachweis der Versorgungssicherheit.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

Stadtwerke, kommunale Versorger, Entsorger und Energieunternehmen erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der kommunalen Versorgung:

ISMS-Aufbau für die Stadtwerke *Kamp-Lintfort & Nienburg/Weser.*

Die Stadtwerke Kamp-Lintfort und die Stadtwerke Nienburg/Weser haben frühzeitig erkannt, dass Informationssicherheit nicht nur eine regulatorische Pflicht ist, sondern auch ein entscheidender Wettbewerbsfaktor für die Energieversorgung von morgen.

Mit SECJUR fiel die Wahl auf eine automatisierte, praxisnahe Lösung, die von erfahrenen Experten eng begleitet wird. Ziel war es, ein vollumfängliches ISMS nach ISO 27001 aufzubauen und die Stadtwerke zugleich für die seit Dezember 2025 geltenden NIS2-Anforderungen aufzustellen.

Mit dem ISMS demonstrieren die Stadtwerke Kamp-Lintfort und Nienburg/Weser beispielhaft, wie kommunale Versorger heute schon Verantwortung für die Informationssicherheit übernehmen und sich mit SECJUR zukunftssicher aufstellen.

REFERENZEN AUS STADTWERKEN, VERSORGUNG UND ENERGIE

1KOMMA5° · Stadtwerke Cottbus Heizkraftwerksgesellschaft · Stadtwerke Nienburg Energie · Otto Dörner · Stadtwerke Kamp-Lintfort

AUDIT-ERFOLG
100%
Erfolgsquote in bisherigen Zertifizierungsaudits.

ZEITERSPARNIS
50%
Weniger Aufwand gegenüber klassischer Beratung.

INTEGRATIONEN
60+
Native API-Anbindungen, von Microsoft 365 bis GitHub.

STANDARDS
10+
Frameworks parallel abgedeckt, ohne Doppelarbeit.

WARUM KOMMUNALE VERSORGER SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit und in der Bündelung. Statt teurer Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die zur kommunalen Realität passen. Das Team bleibt beim Betrieb, das ISMS entsteht parallel.

Nachweise entstehen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass IT und Betrieb an einer Quelle arbeiten statt an parallelen Tabellen.

Wo Spezialwissen zur OT-Sicherheit fehlt, schalten sich Expertinnen und Experten gezielt zu, statt ein dauerhaftes Beratungsmandat zu verlangen. Das hält die Kosten im Rahmen und die Kontrolle im Haus, gerade bei kommunaler Trägerschaft.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Versorger, der seine Anlagen, seine Netze und die Daten seiner Bürgerinnen und Bürger schützt und gegenüber Aufsicht und Kommune souverän auftritt. Genau das sichert die Daseinsvorsorge.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Betriebsvorteil. Nachweise gegenüber Aufsicht und Auditor sind schneller erbracht, Prüffragen verlieren ihren Schrecken, und die Versorgung bleibt auch unter Druck handlungsfähig.

Weil dieselbe Struktur die KRITIS-Nachweispflicht, die branchenspezifischen Standards und die NIS2-Anforderungen gemeinsam bedient, deckt ein Projekt mehrere Anforderungen ab. Das senkt den Aufwand und hält das Unternehmen auch nach dem Audit jederzeit nachweisfähig.

SECJUR

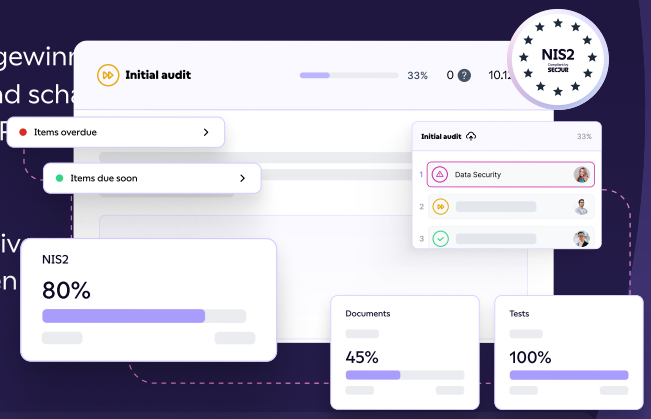
Mit SECJUR zu 100 % NIS2-Compliance

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