SECJUR

WHITEPAPER
2026

NIS2 · ENERGIE, VERSORGUNG & NETZBETRIEB

NIS2 in der Energiebranche: Sicherheit für die Versorgung.

Strom-, Gas- und Wärmeversorgung gehören zur kritischen Infrastruktur, und ihre Digitalisierung schreitet mit der Energiewende rasant voran. Das NIS2-Umsetzungsgesetz gilt seit Dezember 2025 und erfasst weite Teile der Branche als besonders wichtige Einrichtungen. Für Netzbetreiber kommt der IT-Sicherheitskatalog der Bundesnetzagentur hinzu, der ohnehin ein zertifiziertes ISMS verlangt. Dieses Whitepaper zeigt, welche Pflichten gelten, wo die größten Schwachstellen in IT und Netzleittechnik liegen und wie sich alles mit einem Aufbau erfüllen lässt, ohne die Versorgungssicherheit zu gefährden.

NIS2 | ISO 27001 | ISO 27019 | KRITIS | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In der Energiebranche ist Sicherheit gesetzlich verankert.

DAS WICHTIGSTE IN KÜRZE

Das NIS2-Umsetzungsgesetz (NIS2UmsuCG) ist am 6. Dezember 2025 in Kraft getreten und novelliert das BSI-Gesetz. Eine Übergangsfrist gibt es nicht. Der Sektor Energie steht im Zentrum: Strom, Gas, Fernwärme, Öl und Wasserstoff zählen überwiegend zu den besonders wichtigen Einrichtungen mit den strengsten Pflichten.

Für die Branche ist NIS2 dabei nur ein Baustein eines dichten Rahmens. Der IT-Sicherheitskatalog der Bundesnetzagentur nach §11 EnWG verlangt von Strom- und Gasnetzbetreibern seit Jahren ein zertifiziertes ISMS nach ISO 27001, ergänzt um die energiespezifische ISO 27019. Hinzu kommen die KRITIS-Regulierung und, für die physische Resilienz, das KRITIS-Dachgesetz. NIS2 fügt sich hier ein und verlangt Registrierung, Risikomanagement, Meldepflichten und eine haftende Leitung. Anders als das frühere KRITIS-Recht knüpft NIS2 an Sektor und Größe an, wodurch deutlich mehr Betriebe erfasst werden.

WARUM JETZT HANDELN

Der regulatorische Rahmen verdichtet sich, und die BSI-Registrierungsfrist endete am 31. Juli 2026. Wer betroffen und im Verzug ist, holt die Registrierung umgehend nach.

Zugleich ist die Bedrohungslage real. Energieversorger zählen zu den bevorzugten Zielen von Ransomware und staatlich gesteuerten Angreifern, weil ein Ausfall sofort große Wirkung entfaltet. Das BSI stuft die Lage für kritische Infrastrukturen anhaltend als angespannt ein. Wer den Nachweis früh aufbaut, begegnet Aufsicht und Kommunen aus einer Position der Stärke.

EIN AUFBAU, MEHRERE PFLICHTEN

Die gute Nachricht: Ein ISMS nach ISO 27001, energiespezifisch um ISO 27019 ergänzt, erfüllt den IT-Sicherheitskatalog und deckt einen Großteil von NIS2 zugleich ab. Statt jede Vorschrift getrennt abzuarbeiten, entsteht ein gemeinsames Fundament, das IT und Betriebstechnik absichert, von der Verwaltung bis zur Netzleittechnik.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken in IT und Netzleittechnik, die Pflichten aus NIS2 und dem Katalog und eine Roadmap, die im Versorgungsbetrieb funktioniert. Ein klar benannter Verantwortlicher gibt dem Thema zudem ein Gesicht im Unternehmen.

NIS2 IN KRAFT

06.12.2025

Der Sektor Energie zählt überwiegend zu den besonders wichtigen Einrichtungen.

FÜR NETZBETREIBER

§11 EnWG

Der IT-Sicherheitskatalog verlangt ein zertifiziertes ISMS nach ISO 27001 und ISO 27019.

BUSSGELD

10 Mio €

Bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei besonders wichtigen Einrichtungen.

BRANCHENKONTEXT

Die Energieversorgung ist kritische Infrastruktur.

Kaum ein Ausfall wirkt so unmittelbar wie der von Strom, Gas oder Wärme. Genau deshalb ist die Energiebranche reguliert wie kaum eine andere und zugleich ein bevorzugtes Ziel. Ein ISMS ist hier nicht nur Nachweis, sondern gesetzlich eingefordertes Fundament.

Fällt das Netz, steht nicht eine Firma still, *sondern eine ganze Region.*

DIE ENERGIEWENDE DIGITALISIERT DAS NETZ

Aus dem zentralen Kraftwerkspark wird ein dezentrales, digital gesteuertes System. Tausende Windräder, Solaranlagen und Speicher speisen ein, Smart Meter und Smart Grids steuern Lastflüsse in Echtzeit, Leitstellen koordinieren das Ganze. Jede neue Schnittstelle erhöht die Flexibilität und die Angriffsfläche zugleich.

Wo früher proprietäre, isolierte Steuerungstechnik lief, treffen heute IT und Betriebstechnik aufeinander. Diese Konvergenz ist der Motor der Energiewende und ihr größtes Sicherheitsthema. Mit jeder dezentralen Anlage wächst die Zahl der Punkte, die geschützt werden müssen.

EIN DICHTER PFLICHTENRAHMEN

Die Energiebranche ist mehrfach reguliert. Der IT-Sicherheitskatalog nach §11 EnWG verlangt von Netzbetreibern ein zertifiziertes ISMS nach ISO 27001 und ISO 27019. Für Energieanlagen gilt ein eigener Katalog, und über die KRITIS-Regulierung sowie NIS2 kommen weitere Pflichten hinzu.

Maßgeblich ist nicht das Selbstbild, sondern Funktion und Größe. Wer Netze betreibt oder ab den einschlägigen Schwellen Anlagen verantwortet, ist erfasst und muss die Nachweise erbringen, oft gegenüber der Bundesnetzagentur. Wer die Nachweise nicht erbringt, riskiert Anordnungen der Aufsicht bis hin zu Auflagen für den Betrieb.

EINE GEOPOLITISCHE BEDROHUNGSLAGE

Energieinfrastruktur ist ein strategisches Ziel. Neben Ransomware-Banden greifen staatlich gesteuerte Akteure gezielt Versorger an, um Druck auszuüben oder im Ernstfall zu sabotieren. Das BSI stuft die Lage für kritische Infrastrukturen anhaltend als angespannt ein, und NIS2 reagiert mit verbindlichen Mindeststandards. Ein einziger erfolgreicher Zugriff kann Schaltzustände verändern und die Versorgung unterbrechen.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als Daten: Versorgungssicherheit, Anlagensicherheit und am Ende der Schutz von Menschen. Ein erfolgreicher Angriff auf die Netzleittechnik kann Versorgungsunterbrechungen auslösen, deren Schaden weit über die IT hinausreicht.

Ein belastbarer Nachweis ist deshalb nicht nur Pflicht, sondern Schutz des eigenen Betriebs. Er sichert die Handlungsfähigkeit im Ernstfall und das Vertrauen von Aufsicht, Kommunen und Kunden. Gerade Stadtwerke tragen hier Verantwortung für die Daseinsvorsorge ihrer Kommune.

HERAUSFORDERUNGEN

Warum NIS2 in der Energie besonders fordert.

Die Anforderungen gelten unabhängig von der Branche, der Aufwand ist es nicht. Sechs Eigenheiten der Energieversorgung machen die Umsetzung anspruchsvoller als anderswo, und für jede gibt es einen pragmatischen Umgang.

IT UND BETRIEBSTECHNIK ZUGLEICH

Anders als reine Bürobetriebe müssen Energieunternehmen auch ihre Betriebstechnik absichern: Netzleittechnik, SCADA, Fernwirktechnik und Stationsautomatisierung. Diese Systeme haben lange Lebenszyklen, lassen sich nicht beliebig patchen und dürfen im Betrieb nicht einfach abgeschaltet werden. Die Risikoanalyse muss IT und OT gemeinsam betrachten, ohne die Verfügbarkeit der Steuerung zu gefährden. Genau dafür ergänzt ISO 27019 die ISO 27001 um energiespezifische Maßnahmen.

VERSORGUNGSSICHERHEIT HAT VORRANG

In der IT gilt oft Vertraulichkeit zuerst. In der Netzleittechnik steht die Verfügbarkeit an erster Stelle, denn die Versorgung darf nicht abreißen. Eine Sicherheitsmaßnahme, die ein Steuerungssystem destabilisiert, ist keine Option. Maßnahmen müssen so gewählt werden, dass sie schützen, ohne den Betrieb zu stören. Wiederanlaufpläne und Redundanzen sind hier besonders wichtig, damit die Steuerung verfügbar bleibt.

GEWACHSENE, LANGLEBIGE ANLAGEN

Komponenten im Netz sind oft Jahrzehnte im Einsatz und stammen aus einer Zeit, in der Cybersicherheit keine Rolle spielte. Sie lassen sich selten ersetzen und kaum aktualisieren. Kompensierende Maßnahmen wie Netzsegmentierung und strenge Zugänge schützen dort, wo ein Update nicht möglich ist. Ein vom übrigen Netz getrenntes Altsystem bleibt beherrschbar, auch ohne aktuellen Patch.

DEZENTRALE ANLAGEN UND SMART METER

Mit der Energiewende verteilt sich die Erzeugung auf unzählige Standorte, von der Trafostation bis zur PV-Anlage. Jeder Fernzugang und jedes intelligente Messsystem ist ein möglicher Einstieg. Diese verteilte Angriffsfläche konsequent zu verwalten, ist eine Daueraufgabe. Ein zentrales Verzeichnis aller Fernzugänge schafft den Überblick, den verteilte Anlagen schnell verlieren.

NACHWEIS GEGENÜBER DER AUFSICHT

Anders als bei einer rein freiwilligen Zertifizierung prüfen hier die Bundesnetzagentur und das BSI. Zertifikat und Dokumentation müssen jederzeit belastbar vorliegen. Ein gut geführtes ISMS mit lückenlosem Nachweis ist deshalb kein Selbstzweck, sondern Pflichterfüllung. Wer die Dokumentation laufend pflegt, besteht die nächste Prüfung ohne Hektik.

FACHKRÄFTE UND ZEIT

Security-Wissen für IT und OT zugleich ist knapp, und Stadtwerke wie kleinere Versorger konkurrieren mit Konzernen um dieselben Fachkräfte. Klare Prozesse, Vorlagen und ein verlässlicher Partner ersetzen den Aufbau einer eigenen Abteilung und halten die knappe Kapazität beim Versorgungsbetrieb. So wächst die Sicherheit Schritt für Schritt, ohne den Betrieb zu überlasten.

BEDROHUNGSLAGE & RISIKEN

Wo die Energiebranche konkret angreifbar ist.

Die Risiken sind selten abstrakt. Sie hängen an der Netzleittechnik, an einer wachsenden Zahl dezentraler Anlagen und an einer Bedrohungslage, die auch staatliche Akteure umfasst. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · ANGRIFF AUF DIE NETZLEITTECHNIK

Der gefährlichste Ernstfall. Gelingt es Angreifern, in Leitstellen oder Fernwirktechnik einzudringen, können sie im schlimmsten Fall Schaltzustände manipulieren und die Versorgung unterbrechen. Strikte Trennung von IT und OT, Netzsegmentierung und überwachte Zugänge sind hier die entscheidenden Schutzlinien, ergänzt um die Maßnahmen der ISO 27019. Eine kontinuierliche Überwachung der Leitsysteme erkennt Manipulationen, bevor sie wirken. Die Trennung von IT und OT verhindert, dass ein Angriff aus dem Büro die Steuerung erreicht.

2 · RANSOMWARE LEGT DEN BETRIEB LAHM

Auch ohne direkten Zugriff auf die Steuerung trifft Ransomware die Verwaltungs- und Abrechnungssysteme und kann den Betrieb empfindlich stören. Verschlüsselte Leitsysteme oder Kundendatenbanken bedeuten Stillstand und Meldepflicht. Getestete, vom Netz getrennte Backups und ein eingeübter Notfallplan entscheiden über die Dauer des Ausfalls. Ein zweiter, getrennter Datenstand verkürzt den Wiederanlauf erheblich. Wer den Ernstfall nie geübt hat, verliert im Angriff die wertvollste Zeit.

3 · STAATLICH GESTEUERTE ANGREIFER

Energieversorger sind ein strategisches Ziel. Hoch entwickelte Angreifer nisten sich oft monatelang unbemerkt ein, um im Ernstfall handlungsfähig zu sein. Dagegen helfen kontinuierliche Überwachung, Angriffserkennung und ein geübter Vorfallprozess, wie ihn auch NIS2 mit der Meldepflicht an das BSI verlangt. Eine lückenlose Protokollierung macht solche stillen Zugriffe überhaupt erst sichtbar. Die Meldung verschafft im Ernstfall zugleich Zugang zu Lagebild und Unterstützung.

4 · ANGRIFFE ÜBER DIE LIEFERKETTE

Steuerungstechnik, Wartungsdienstleister und Fernwartungszugänge sind ein beliebter Umweg ins Netz. Ein kompromittierter Hersteller oder ein manipuliertes Update wird zum Einfallstor. Lieferantensteuerung mit klaren Anforderungen und abgesicherte Fernwartung sind deshalb zentral, unter NIS2 wie unter dem IT-Sicherheitskatalog. Ein aktuelles Verzeichnis aller Wartungszugänge ist die Grundlage, um die Kette zu überblicken. Feste Zeitfenster und Mehrfaktor-Anmeldung begrenzen, was über einen Fernzugang möglich ist.

5 · VERTEILTE ANLAGEN UND FERNZUGÄNGE

Trafostationen, PV- und Windparks sowie intelligente Messsysteme sind oft nur leicht gesichert und über Fernzugänge erreichbar. Jeder dieser Punkte ist ein möglicher Einstieg in größere Systeme. Starke Authentifizierung, Verschlüsselung und lückenlose Protokollierung begrenzen dieses Risiko. Wer weiß, welche Anlagen erreichbar sind, kann sie zuerst und am stärksten absichern.

REGULATORISCHE PFLICHTEN

Was NIS2 und der Katalog konkret verlangen.

NIS2 steht in der Energie neben dem IT-Sicherheitskatalog, der KRITIS-Regulierung und ISO 27019. Fünf Bausteine muss jedes betroffene Unternehmen kennen: Betroffenheit (§28), Risikomanagement (§30), Meldepflichten (§32), Leitungspflichten (§38) und Sanktionen (§65).

§28 · BETROFFENHEIT UND REGISTRIERUNG

Der Sektor Energie zählt überwiegend zu den besonders wichtigen Einrichtungen, mit den strengsten Pflichten und der schärfsten Aufsicht. Maßgeblich sind Funktion und Größe, nicht das Selbstbild. Die Registrierung läuft über das Unternehmenskonto und das BSI-Portal, zusätzlich zum benannten Ansprechpartner IT-Sicherheit, den der IT-Sicherheitskatalog gegenüber der Bundesnetzagentur fordert. Im Zweifel schafft eine kurze, dokumentierte Einstufung Klarheit und Sicherheit für die Leitung.

§30 · DIE TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Verlangt werden angemessene Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, Zugriffskontrolle, Kryptografie und Multifaktor-Authentifizierung. Netzleittechnik und Betriebstechnik gehören ausdrücklich dazu. Wer bereits nach ISO 27001 und ISO 27019 zertifiziert ist, hat den Großteil abgedeckt und setzt NIS2 als Erweiterung um, nicht als zweites Projekt. Entscheidend ist, dass jede Maßnahme nicht nur existiert, sondern nachweisbar gelebt und regelmäßig überprüft wird.

§32 · MELDEFRISTEN

Bei einem erheblichen Sicherheitsvorfall gilt eine gestufte Meldepflicht an das BSI: Frühwarnung binnen 24 Stunden, Meldung mit erster Bewertung binnen 72 Stunden, Abschlussbericht binnen eines Monats. Gerade bei einem Vorfall in der Netzleittechnik zählt jede Stunde, und die Uhr läuft ab Kenntnis. Nur ein vorab geübter Prozess hält diese Fristen. Ein vorbereitetes Meldeformular und klare Zuständigkeiten sparen im Ernstfall wertvolle Minuten.

§38 · LEITUNG HAFTET PERSÖNLICH

Die Geschäftsführung muss die Maßnahmen billigen, ihre Umsetzung überwachen und sich schulen lassen. Wer den Netzbetrieb verantwortet, haftet persönlich für die Umsetzung. Die Verantwortung ist nicht delegierbar, auch nicht an den externen Dienstleister. Das dokumentierte Engagement der Leitung ist im Ernstfall zugleich ein Nachweis gelebter Sorgfalt. Regelmäßige, kurze Schulungen der Leitung sind ausdrücklich Teil dieser Pflicht.

§65 · SANKTIONEN UND VERHÄLTNISMÄSSIGKEIT

Verstöße kosten bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei besonders wichtigen Einrichtungen. Hinzu treten Anordnungen der Aufsicht bis hin zu Auflagen für den Betrieb. 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 plant, wird selbst bei einem Vorfall milder bewertet als ein untätiger Betrieb.

UMSETZUNG IN DER PRAXIS

In sechs Schritten mit Augenmaß NIS2-konform.

Die Umsetzung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt vorhandene Strukturen, statt bei null zu beginnen. Realistisch sind je nach Reife und Anlagenlandschaft einige Monate bis zum auditbereiten Stand.

Ein ISMS erfüllt den IT-Sicherheitskatalog und einen Großteil von NIS2 zugleich. *Ein Aufbau, mehrere Pflichten.*

1 · BETROFFENHEIT UND GELTUNGSBEREICH

Feststellen, ob das Unternehmen als besonders wichtige Einrichtung unter NIS2 fällt und welche Kataloge zusätzlich greifen. Den Scope auf die regulierten Bereiche schneiden: Netzbetrieb, Leitstellen, zugehörige IT und OT. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und entscheidend für die Prüfung durch die Aufsicht.

2 · FÜHRUNG, LEITLINIE, ANSPRECHPARTNER

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, stellt Ressourcen bereit und benennt den Ansprechpartner IT-Sicherheit, den der IT-Sicherheitskatalog gegenüber der Bundesnetzagentur fordert. Registrierung und Kontaktstellen für das BSI gehören ebenfalls in diesen Schritt.

3 · RISIKEN IN IT UND OT ANALYSIEREN

Assets erfassen, von der Verwaltung über Leitstellen bis zur Fernwirktechnik. Risiken gemeinsam für IT und Betriebstechnik bewerten, Verfügbarkeit besonders gewichten und die Erklärung zur Anwendbarkeit mit Annex A und ISO 27019 erstellen. Eine gute Analyse macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

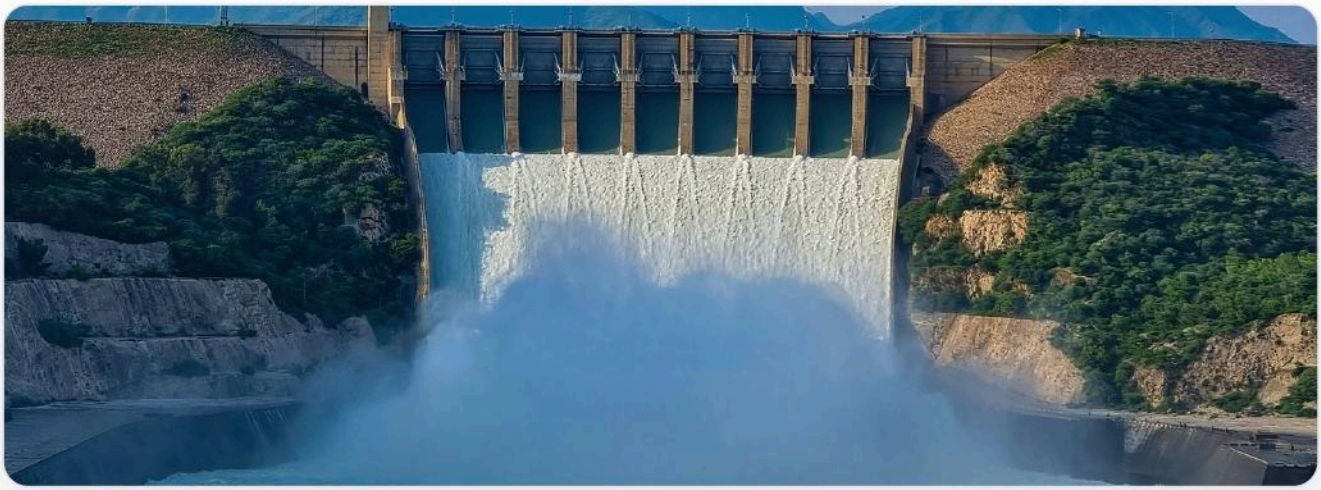
Mit den wirksamsten Hebeln beginnen: Netzsegmentierung, Zugriffs- und Fernwartungskontrolle, Backup und Angriffserkennung. Jede Maßnahme so festhalten, dass sie im Audit und vor der Aufsicht Bestand hat. In der OT gilt: schützen, ohne die Verfügbarkeit der Steuerung zu gefährden. So wirkt jede Maßnahme sofort im ganzen Betrieb.

5 · MELDE- UND NOTFALLPROZESSE AUFBAUEN

Die 24-Stunden-Meldekette an das BSI einrichten, Zuständigkeiten klären und den Notfallplan testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen. Eine Übung pro Jahr zeigt, wo der Ablauf zwischen Netzleittechnik und Verwaltung noch hakt.

6 · PRÜFEN, NACHWEISEN, VERBESSERN

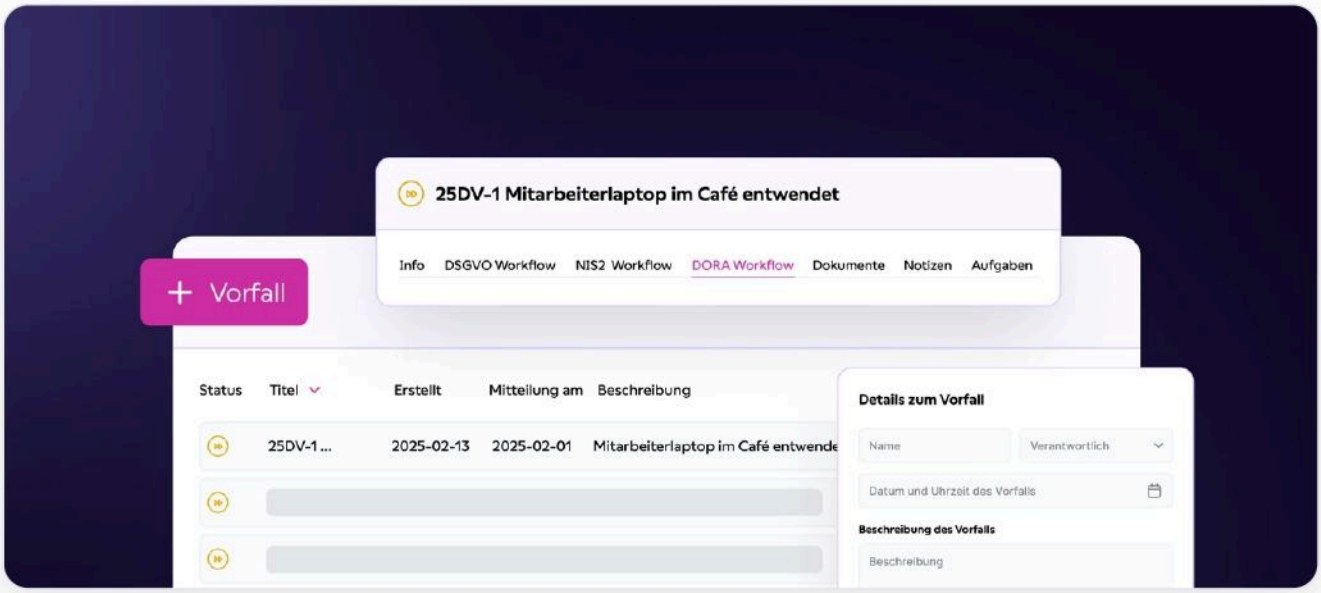
Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Genau diese Schleife erwarten Zertifizierer und Aufsicht gleichermaßen. Wer sie einmal vollständig durchläuft, ist zugleich reif für das Zertifizierungsaudit und den Nachweis gegenüber der Bundesnetzagentur.



WIE SECJUR ES EINFACH MACHT

Vom Pflichtenrahmen zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) führt Energieunternehmen durch NIS2 und den IT-Sicherheitskatalog zugleich: Risiken in IT und OT, Maßnahmen, Meldeprozess und Nachweise an einem Ort, mehrere Frameworks parallel. Statt monatelanger 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

Eine Risikoanalyse, die Verwaltung und Netzleittechnik zusammen denkt, mit Vorlagen aus ISO 27001 und der energiespezifischen ISO 27019.

Vorfall & Meldung

Strukturiertes Incident-Management mit der 24-Stunden-Meldekette an das BSI, inklusive Fristenverfolgung (24h / 72h / 1 Monat) und Bericht.

Mehrere Pflichten

NIS2, IT-Sicherheitskatalog, ISO 27001 und ISO 27019 laufen auf einem ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt mehrfach.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank. Sie legen den Geltungsbereich fest, das DCO führt durch jede Anforderung, und wo eine Expertin nötig ist, schalten wir sie zu. Sie entscheiden, das System dokumentiert im Hintergrund. So entsteht ein auditbereiter Nachweis in Wochen statt in Quartalen, ohne dass der Versorgungsbetrieb stehen bleibt.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Assets in IT und OT sowie bestehende Maßnahmen 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 jederzeit sichtbar, für die IT ebenso wie für die Leitstelle.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2, der IT-Sicherheitskatalog, ISO 27001 und ISO 27019 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegt.

Für einen Versorger heißt das weniger Doppelarbeit. Der NIS2-Nachweis und die Zertifizierung nach ISO 27001 und ISO 27019 entstehen aus demselben Aufbau, statt in getrennten Projekten.

Und weil die Belege aktuell bleiben, ist das Unternehmen für das nächste Überwachungsaudit oder die nächste Prüfung der Bundesnetzagentur vorbereitet, ohne kurzfristig Unterlagen zusammensuchen zu müssen. Aus einer Pflicht wird so ein dauerhafter Schutz der Versorgung.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

Energieversorger, Netzbetreiber, Stadtwerke und Industrieunternehmen erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Energiebranche:

„Dank SECJUR konnten wir schnell ein *hochwertiges ISMS* aufbauen, wie uns die Zertifizierungsaudits bestätigt haben. Unser Berater hat uns stets kompetent unterstützt, als wäre er Teil der Firma."

Stefan Gregori
Chief Information Security Officer, Consolinno Energy

REFERENZEN AUS ENERGIE, VERSORGUNG UND INDUSTRIE

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

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 ENERGIEUNTERNEHMEN SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit und in der Branchentiefe. Statt monatelanger Beratung führt ein klarer Pfad durch NIS2, ISO 27001 und ISO 27019, mit Vorlagen, die IT und Netzleittechnik gemeinsam denken. Das Team bleibt beim Betrieb, das ISMS entsteht parallel.

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

Wo Fachwissen für IT und OT 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 Stadtwerken und kleineren Versorgern.

Und die Plattform denkt in der Realität eines Versorgungsbetriebs. Sie priorisiert die Maßnahmen mit der größten Wirkung und schützt, ohne die Verfügbarkeit der Steuerung zu gefährden.

MEHR ALS EINE PFLICHTÜBUNG

Am Ende steht nicht nur der Nachweis gegenüber der Bundesnetzagentur, sondern ein Versorger, der seine Risiken in IT und OT kennt und im Ernstfall handlungsfähig bleibt. Genau das schützt die Versorgung.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Betriebsvorteil. Audits der Aufsicht verlieren ihren Schrecken, Störungen werden schneller beherrscht, und Netzleittechnik wie Verwaltung ziehen an einem Strang.

Weil derselbe Unterbau NIS2, den IT-Sicherheitskatalog und die ISO-Zertifizierung zugleich trägt, sinkt der Aufwand, statt sich zu verdoppeln. Ein Aufbau bedient die Aufsicht, die Zertifizierung und das nächste Kundenaudit.

So wird aus einer Pflicht ein dauerhafter Schutz der Versorgungssicherheit, der mit jeder neuen dezentralen Anlage und jedem Smart Meter an Bedeutung gewinnt.

SECJUR

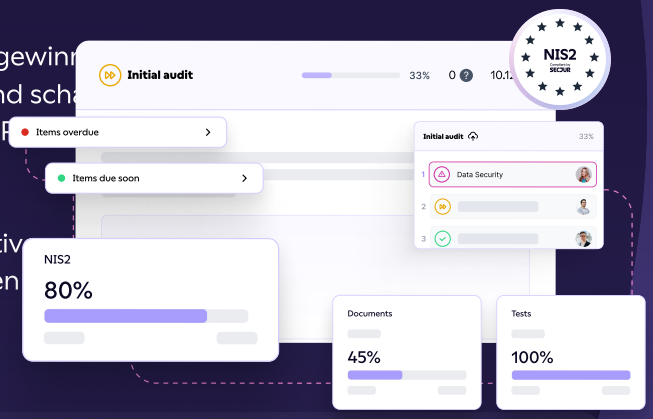
Mit SECJUR zu 100 % NIS2-Compliance

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