SECJUR

WHITEPAPER
2026

NIS2 · LOGISTIK, TRANSPORT & LAGER

NIS2 in der Logistik: Sicherheit, die den Warenfluss schützt.

Kaum eine Branche ist so vernetzt und so zeitkritisch wie die Logistik. Ein Stillstand in der IT legt heute den physischen Warenfluss lahm, und Verlader prüfen ihre Dienstleister immer genauer. Das NIS2-Umsetzungsgesetz erfasst weite Teile des Verkehrssektors, und über die Lieferkette regulierter Kunden werden viele weitere Betriebe gebunden. Dieses Whitepaper zeigt, welche Pflichten gelten, wo die größten Schwachstellen zwischen IT und Betriebstechnik liegen und wie ein ISMS entsteht, ohne den laufenden Betrieb auszubremsen.

NIS2 · ISO 27001 · TISAX® · ISO 9001 · DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Sicherheit ist in der Logistik zum Auftragskriterium geworden.

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 Verkehrssektor, von Straße und Schiene über Luft- bis zur Schifffahrt, sowie Post- und Kurierdienste zählen ausdrücklich zu den erfassten Bereichen.

Für Logistiker entsteht die Betroffenheit auf zwei Wegen: über den eigenen Sektor und über die Rolle als Dienstleister regulierter Verlader. Wer 50 Beschäftigte oder 10 Millionen Euro erreicht, ist im erfassten Sektor eine wichtige Einrichtung, große Betriebe sind besonders wichtig. Maßgeblich sind Sektor und Größe, nicht das Selbstbild. Ein ISMS nach ISO 27001 deckt einen Großteil dieser Pflichten gleich mit ab. Anders als das frühere KRITIS-Recht knüpft NIS2 an Sektor und Größe an, wodurch deutlich mehr Betriebe erfasst werden. Wer die Prüfung sauber dokumentiert, schützt die Geschäftsführung im Zweifel vor Haftung.

WARUM JETZT HANDELN

Der Druck kommt von zwei Seiten. Verlader und Industriekunden geben ihre eigenen Sicherheitsanforderungen über die Lieferkette weiter und verlangen den Nachweis vertraglich.

Parallel läuft die NIS2-Pflicht, die BSI-Registrierungsfrist endete am 31. Juli 2026.

Hinzu kommt die Bedrohungslage. Ransomware zählt zu den größten Risiken für die deutsche Wirtschaft, und Logistik ist ein lohnendes Ziel, weil Stillstand sofort teuer wird und der Warenfluss keinen Puffer kennt. Ein Vorfall trifft hier nicht nur die IT, sondern sofort Termine und Verlader. Wer den Nachweis früh aufbaut, begegnet Auftraggebern und Aufsicht aus einer Position der Stärke.

EIN AUFBAU, ZWEI ERGEBNISSE

Die gute Nachricht: Ein ISMS nach ISO 27001 erfüllt einen Großteil der NIS2-Pflichten, etwa Risikomanagement, Lieferkettensicherheit und Notfallvorsorge. Zugleich beantwortet es die Sicherheitsfragebögen der Verlader mit einem Dokument. Der Standard ist dabei verhältnismäßig und passt zu Größe und Risiko des Betriebs, nicht zum Konzernmaßstab.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken zwischen IT und Betriebstechnik, die Pflichten aus dem Gesetz und eine Roadmap, die im laufenden Betrieb funktioniert. So bleibt die knappe IT-Kapazität beim Tagesgeschäft, statt in Formularen zu versickern. Ein klar benannter Verantwortlicher gibt dem Thema zudem ein Gesicht im Betrieb.

BETROFFEN

29.500

Unternehmen in 18 Sektoren fallen unter NIS2, der Verkehrssektor gehört dazu.

FRIST ABGELAUFEN

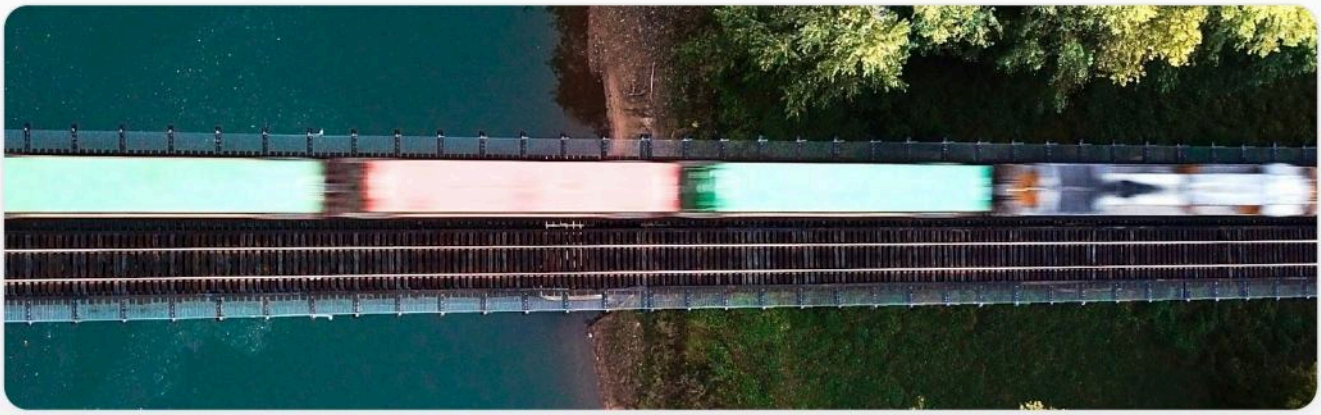
31.07.2026

Die verlängerte BSI-Registrierungsfrist endete am 31. Juli 2026, viele fehlten noch.

BUSSGELD

10 Mio €

Bis zu 10 Mio. Euro bei besonders wichtigen, bis zu 7 Mio. bei wichtigen Einrichtungen.



BRANCHENKONTEXT

Die Logistik ist das Nervensystem der Wirtschaft.

Kaum eine Branche ist so vernetzt und so zeitkritisch wie die Logistik. Genau das macht sie für Angreifer attraktiv und für Auftraggeber zum Prüffall. NIS2 und der Markt verlangen deshalb nachweisbare Sicherheit.

Steht das Transportmanagementsystem, steht der Warenfluss. *Stunden entscheiden, nicht Tage.*

ZWANZIG JAHRE DIGITALISIERUNG

Was früher Telefon, Fax und Papierfrachtbrief war, läuft heute über vernetzte Systeme. Transportmanagement, Lagerverwaltung, Telematik in der Flotte, automatisierte Hochregallager, Sendungsverfolgung und elektronischer Datenaustausch bilden eine durchgehende digitale Kette vom Auftrag bis zur Auslieferung.

Hinzu kommen Zollanbindungen wie ATLAS und Buchungsplattformen. Jede dieser Schnittstellen ist Effizienzgewinn und Angriffsfläche zugleich. Was den Betrieb schnell macht, macht ihn auch verwundbar. Schon ein Blick auf die Übergänge zwischen TMS und Betriebstechnik zeigt, wo die dringendsten Lücken liegen.

AUFTRAGGEBER PRÜFEN GENAUER

Große Verlader und Industriekunden kaufen Logistik nicht mehr ohne Prüfung. Bevor ein Konzern einen Dienstleister in seine Lieferkette lässt, durchläuft dieser eine Lieferantenprüfung mit langen Sicherheitsfragebögen. Ein ISMS beantwortet einen Großteil davon mit einem einzigen Nachweis.

Ohne Nachweis wird aus der Ausschreibung ein Prüfmarathon, und manche Vergabe ist von vornherein verloren. Mit Nachweis steht der Betrieb auf der Auswahlliste, statt vorab auszuscheiden. Sicherheit wird so vom Kostenposten zum Vertriebsargument. Wer den Nachweis früh vorlegt, bleibt im Vergabeprozess ein bevorzugter Partner.

DIE NIS2-VERBINDUNG

Der Verkehrssektor fällt weitgehend unter NIS2. Wer ein ISMS nach ISO 27001 betreibt, erfüllt damit einen Großteil der gesetzlichen Pflichten, etwa Risikomanagement, Lieferkettensicherheit und Notfallvorsorge. Ein Aufbau, zwei Ergebnisse. Auch wer knapp unter den Schwellen bleibt, wird über die Kette regulierter Verlader gebunden.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als IT-Ausfall: gerissene Liefertermine, Vertragsstrafen, abwandernde Verlader und ein beschädigter Ruf. In einem Markt, der von Zuverlässigkeit lebt, ist Sicherheit längst ein Wettbewerbsfaktor.

Ein sauberer Nachweis sichert deshalb Aufträge und hält Verlader. Er macht aus einer Pflicht einen Vorsprung gegenüber Wettbewerbern, die den Nachweis erst noch aufbauen müssen. Ein einziger längerer Stillstand kann eine ganze Tourenplanung durcheinanderbringen.

HERAUSFORDERUNGEN

Warum NIS2 in der Logistik besonders fordert.

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

ZEITKRITIKALITÄT OHNE PUFFER

Ein Maschinenbauer kann die Produktion drei Tage anhalten. Ein Logistiker kann das nicht. Fällt das TMS oder WMS aus, stoppen Disposition, Kommissionierung und Verladung sofort, Just-in-time-Zusagen platzen innerhalb von Stunden. Für das ISMS heißt das: kurze Wiederanlaufzeiten betriebsnaher Systeme, getestete Backups und ein belastbarer Notfallplan. Genau diese Vorsorge verlangt auch NIS2. Ein zweiter, getrennter Datenstand verkürzt den Wiederanlauf erheblich.

GEWACHSENE IT- UND OT-LANDSCHAFT

Neben klassischer IT steuern operative Systeme den physischen Betrieb: Telematik, Lagerautomatik, Tor- und Rampensteuerung, Scanner und Förderanlagen. Vieles ist über Jahre gewachsen, läuft auf älteren Ständen und war nie für offene Vernetzung gedacht. Diese Übergänge zwischen OT und IT sind der wunde Punkt der Branche und verdienen in der Risikoanalyse besondere Aufmerksamkeit. Eine klare Trennung von Büro- und Betriebsnetz ist dabei der wirksamste erste Schritt.

TIEFE SUBUNTERNEHMER-NETZE

Speditionen arbeiten mit Frachtführern, Lagerpartnern, Zollagenten und IT-Dienstleistern. Jeder Zugang ist ein möglicher Einstiegspunkt. NIS2 und die Norm verlangen Sicherheit in der Lieferantenbeziehung, also Anforderungen an Dienstleister und deren Nachweis. In einem fragmentierten Markt ist das dauerhafte Arbeit, aber genau hier liegt der größte Hebel. Ein aktuelles Verzeichnis aller Partner und Zugänge macht die Kette überhaupt erst überblickbar.

DÜNNE MARGEN, SAISONSPITZEN

Die Branche arbeitet mit knappen Margen, Budget für Sicherheit ist selten üppig. Hier hilft das Prinzip der Verhältnismäßigkeit: Maßnahmen passen zu Größe und Risiko, nicht zum Konzernmaßstab. Zugleich treffen Angriffe in Spitzenzeiten besonders hart, wenn alles unter Volllast läuft und das Team weniger wachsam ist.

DÜNNE IT-DECKE

Viele Betriebe haben kleine IT-Teams ohne eigene Sicherheitsfunktion, und der Fachkräftemangel verschärft das. NIS2 verlangt aber Struktur, Dokumentation und Wirksamkeitskontrolle, nicht Heldentaten Einzelner. Werkzeuge, die führen und dokumentieren, machen hier den Unterschied. Ein verlässlicher Partner ersetzt so das teure, schwer zu findende Fachpersonal im eigenen Haus.

PHYSISCHE STANDORTE ABSICHERN

Lager, Umschlagplätze und Höfe sind über den Zutritt selbst ein Angriffsziel. NIS2 denkt physische und digitale Sicherheit zusammen: Zutrittskontrolle, Videoüberwachung und klare Zonen schützen Ware und Systeme gleichermaßen, gerade an Standorten mit hoher Personalfluktuation.

BEDROHUNGSLAGE & RISIKEN

Wo die Logistik konkret angreifbar ist.

Die Risiken sind selten abstrakt. Sie hängen an konkreten Systemen und an einem Netz aus Partnern, das ein einzelner Betrieb kaum allein kontrolliert. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE STOPPT DEN WARENFLUSS

Der häufigste Ernstfall. Wird das TMS oder WMS verschlüsselt, lässt sich nicht mehr disponieren, kommissionieren oder verladen. Der Betrieb fällt auf manuellen Notbetrieb zurück, Sendungen stauen sich, Termine reißen. Getestete, vom Netz getrennte Backups und ein eingeübter Notfallplan entscheiden, ob der Stillstand Stunden oder Tage dauert. Wer den Ernstfall nie geübt hat, verliert im Angriff die wertvollste Zeit. Ein aktueller Notfallplan legt vorab fest, wer im Stillstand was entscheidet.

2 · ANGRIFFE ÜBER DIE LIEFERKETTE

Angreifer nutzen den schwächsten Partner als Tür. Ein kompromittierter Frachtführer, Lagerpartner oder Software-Dienstleister wird zum Einfallstor in das eigene Netz. Genau hier setzt die Lieferkettensicherheit nach §30 an, mit Mindestanforderungen und deren Überprüfung. Verlader fordern diesen Nachweis zunehmend selbst ein. Ein aktuelles Verzeichnis aller Frachtführer und Zugänge ist die Grundlage, um die Kette zu überblicken. Wer seine Schnittstellen sauber führt, besteht die Prüfungen der Verlader ohne Hektik.

3 · OT- UND TELEMATIK-KOMPROMITTIERUNG

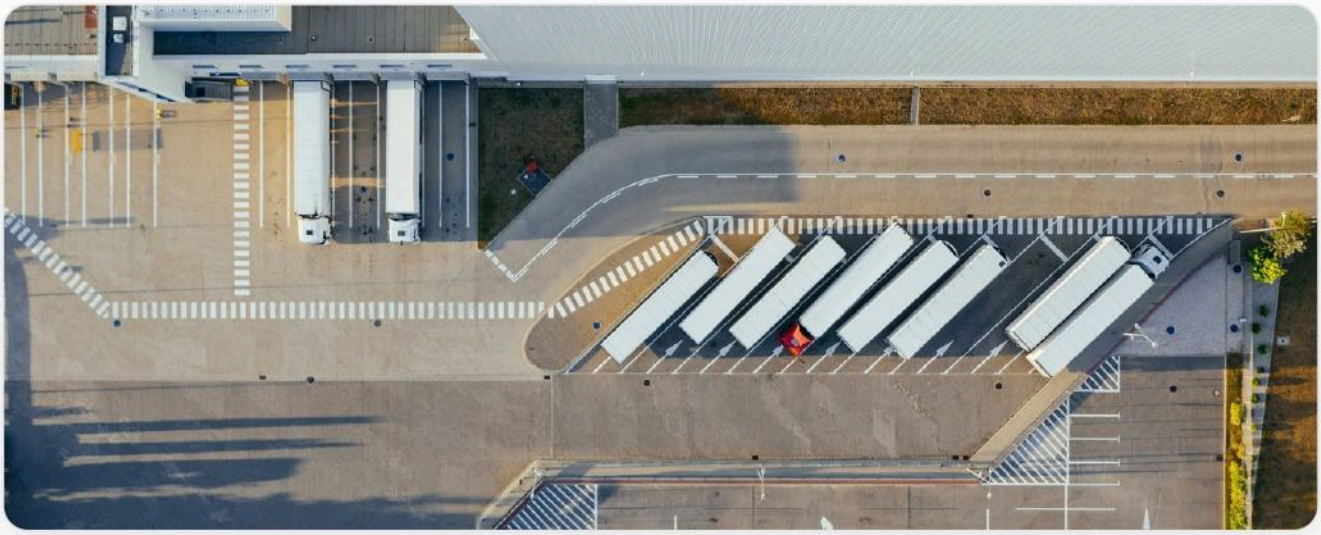
Flotten-Telematik, Lagerautomatik und Steueranlagen sind angreifbar, wenn sie offen vernetzt und selten gepatcht sind. Manipulierte Standortdaten oder lahmgelegte Förderanlagen wirken unmittelbar auf den physischen Betrieb. Solche Anlagen lassen sich selten einfach neu starten, ohne den Betrieb zu unterbrechen. Eine kontinuierliche Überwachung erkennt Manipulationen, bevor sie den Betrieb erreichen. Feste Zugriffszeiten und lückenlose Protokollierung machen die Fernwartung wieder beherrschbar.

4 · DIEBSTAHL SENSIBLER DATEN

Sendungsdaten, Zolldokumente, Tarife und Kundendaten fließen permanent zwischen Systemen und über EDI-Schnittstellen. Ein Abfluss ist nicht nur ein DSGVO-Vorfall, sondern kostet Vertrauen bei Verladern und kann Wettbewerber begünstigen. Verschlüsselung und Zugriffskontrolle sind hier die zentralen Hebel. Eine Protokollierung der Zugriffe macht ungewöhnliche Muster früh sichtbar. Wer weiß, wo die sensibelsten Daten liegen, kann sie zuerst und am stärksten schützen.

5 · FRACHTBETRUG UND SCHWACHE ZUGÄNGE

Überlastangriffe auf Track-and-Trace-Portale legen den Kundenkontakt lahm. Frachtbetrug mit gefälschten Lieferadressen, untergeschobenen Aufträgen oder manipulierten Rechnungen verursacht direkten Schaden. Multifaktor-Authentifizierung und saubere Rechtevergabe verhindern einen Großteil davon und kosten wenig. Ein Vier-Augen-Prinzip bei Zahlungen und Adressänderungen stoppt die meisten Betrugsversuche.



REGULATORISCHE PFLICHTEN

Was das Gesetz konkret verlangt.

Fünf Paragraphen bilden den Kern, den jeder betroffene Betrieb kennen muss: Betroffenheit (§28), Risikomanagement (§30), Meldepflichten (§32), Leitungspflichten (§38) und Sanktionen (§65).

§28 · BETROFFENHEIT UND REGISTRIERUNG

Wichtige Einrichtung ist, wer ab 50 Beschäftigte oder mehr als 10 Mio. Euro erreicht, besonders wichtig ab 250 Beschäftigte oder mehr als 50 Mio. Euro. Der Verkehrssektor umfasst Straße, Schiene, Luft und Wasser, hinzu kommen Post- und Kurierdienste. Die Registrierung läuft über das Unternehmenskonto und das BSI-Portal, die Einstufung nimmt der Betrieb selbst vor und begründet sie schriftlich. Im Zweifel hilft eine kurze rechtliche Einschätzung. Wer wartet, riskiert, im entscheidenden Moment ohne Nachweis dazustehen.

§30 · DIE TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Verlangt werden angemessene Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, Zugriffskontrolle, Kryptografie und Multifaktor-Authentifizierung. Betriebs- und Lagertechnik gehören ausdrücklich dazu. Wer bereits ein ISMS nach ISO 27001 betreibt, 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. Steht der Warenfluss still, 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. Die Verantwortung ist nicht delegierbar, auch nicht an den externen IT-Dienstleister. Für die Leitung wird Cybersicherheit damit zur Führungsaufgabe. Das dokumentierte Engagement 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, bis zu 7 Mio. Euro oder 1,4 % bei wichtigen Einrichtungen. 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 führt der Weg in wenigen Monaten zu einem auditbereiten Stand.

Ein ISMS nach ISO 27001 deckt zugleich einen Großteil von NIS2 ab. *Ein Aufbau, zwei Ergebnisse.*

1 · BETROFFENHEIT UND GELTUNGSBEREICH

Sektor und Schwellenwerte prüfen, auch die Rolle als Dienstleister regulierter Verlader, und die Einstufung dokumentieren. Den Scope eng schneiden: welche Standorte, welche Systeme, welche Prozesse. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und der wirksamste Hebel, um den Aufwand niedrig zu halten.

2 · BEIM BSI REGISTRIEREN

Unternehmenskonto anlegen, im BSI-Portal registrieren, Kontaktstellen benennen. Wer die Frist versäumt hat, holt den Schritt umgehend nach, um Bußgelder zu vermeiden. Die benannte Kontaktstelle ist zugleich der Draht zum BSI im Ernstfall.

3 · RISIKEN IN IT UND OT ANALYSIEREN

Assets erfassen, von TMS und WMS über Telematik bis zu den OT/IT-Übergängen. Risiken bewerten, Lücken sichtbar machen und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse trennt das Wichtige vom Nebensächlichen und macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Mit den wirksamsten Hebeln beginnen: Backup, Zugriffskontrolle, Multifaktor-Anmeldung und Lieferantenanforderungen. Jede Maßnahme so festhalten, dass sie im Audit Bestand hat. Vieles lässt sich in vorhandenen Systemen direkt aktivieren, sodass jede Maßnahme sofort im ganzen Betrieb wirkt. Zentrale Vorgaben verhindern, dass jeder Standort eigene Wege geht.

5 · MELDEPROZESS 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 Disposition und IT noch hakt.

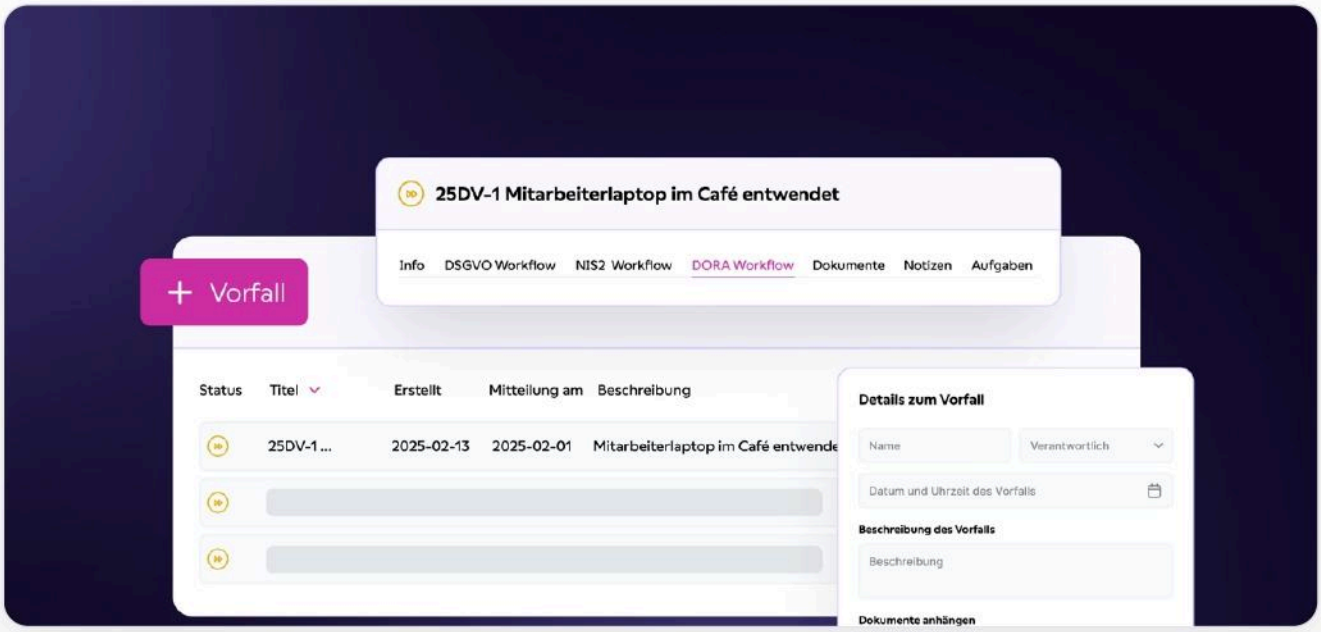
6 · PRÜFEN, NACHWEISEN, VERBESSERN

Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Genau diese Schleife will der Auditor sehen: nicht Perfektion, sondern einen gelebten Kreislauf. Wer sie einmal vollständig durchläuft, ist zugleich reif für die ISO-27001-Zertifizierung. 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 Logistikbetriebe durch die NIS2-Umsetzung: Risiken in IT und Betriebstechnik, 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 Betrieb

Eine Risikoanalyse, die Disposition, Lager und Betriebstechnik zusammen denkt, mit Vorlagen, die zum Logistikbetrieb passen statt zum Konzern.

Vorfall & Meldung

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

Lieferkette & Nachweise

Lieferantensteuerung und ein Nachweis, der die Sicherheitsfragebögen der Verlader und die NIS2-Pflichten gemeinsam bedient.

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 Betrieb stehen bleibt.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Assets in IT und Betrieb 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 Disposition.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2 und ISO 27001 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 Logistiker heißt das weniger Doppelarbeit. Der NIS2-Nachweis und die ISO-27001-Zertifizierung entstehen aus demselben Aufbau, statt in getrennten Projekten.

Und weil die Belege aktuell bleiben, ist der Betrieb für die nächste Ausschreibung oder Lieferantenprüfung vorbereitet, ohne kurzfristig Unterlagen zusammensuchen zu müssen. Aus einer Pflicht wird so ein dauerhafter Vorteil.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

Speditionen, Transport- und Lagerbetriebe, Kurierdienste und Industrieunternehmen erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Logistik:

„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 LOGISTIK UND ANGRENZENDEN BRANCHEN

OTTO DÖRNER · SVG · orbit · bm bahndienste · HADAG

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 LOGISTIKER SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die zum Betrieb passen statt zum Konzern. Das Team bleibt beim Tagesgeschäft, das ISMS entsteht parallel.

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

Und die Plattform denkt in der Realität eines Logistikbetriebs. Sie priorisiert die Maßnahmen mit der größten Wirkung und schützt, ohne den Warenfluss zu unterbrechen.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur der Nachweis, sondern ein Betrieb, der seine Risiken kennt, seine Lieferkette im Griff hat und in der nächsten Ausschreibung souverän auftritt. Genau das gewinnt Aufträge und hält Verlader.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Vorteil. Sicherheitsfragebögen sind in Stunden beantwortet, Audits verlieren ihren Schrecken, und Verlader sehen belegt, dass ihre Ware zuverlässig fließt.

Weil dieselbe Struktur ISO 27001 und die NIS2-Pflichten gemeinsam bedient, deckt ein Projekt mehrere Anforderungen ab. Das senkt den Aufwand und hält den Betrieb auch nach dem Audit jederzeit nachweisfähig.

So wird aus einer Pflicht ein dauerhafter Schutz von Warenfluss, Terminen und Ruf, der mit jeder neuen Anbindung und jedem Verlader an Bedeutung gewinnt.

SECJUR

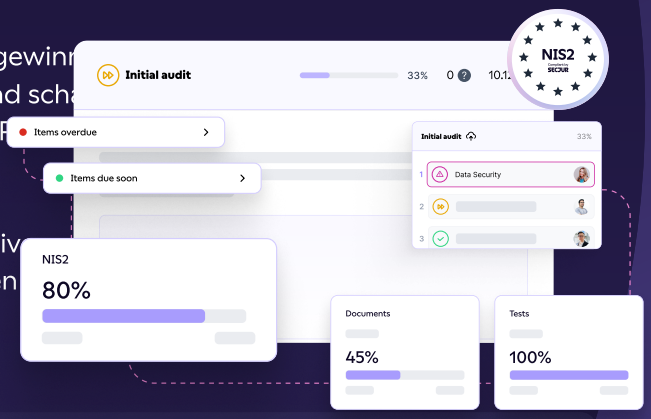
Mit SECJUR zu 100 % NIS2-Compliance

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