SECJUR

NIS2 für die Logistikbranche

Warum Transport, Spedition und Logistikdienstleister zu den besonders wichtigen NIS2-Sektoren zählen, und wie Readiness gelingt.

Der Verkehrs- und Transportsektor, von Luftfahrt über Schifffahrt und Schiene bis Straßengüterverkehr, ist als **besonders wichtige bzw. wichtige Einrichtung** in der NIS2-Richtlinie gelistet. Flughäfen, Häfen, Reedereien und große Speditionen unterliegen dem **NIS2-Umsetzungsgesetz (NIS2UmsuCG)**. Besonders exponiert: vernetzte Frachtsysteme, Track-&-Trace-Plattformen, Telematik und hochintegrierte Lieferketten.

In diesen vier Situationen wird NIS2 für Logistikunternehmen konkret:

BETROFFENHEIT & EINSTUFUNG

Annex 1 und Annex 2

- Luft- und Seehäfen sowie Verkehrsverwaltungen als besonders wichtige Einrichtungen (Annex 1)
- Speditionen, Kurierdienste und Lagerlogistik als wichtige Einrichtungen (Annex 2)
- Schwelle für Annex 2: ab 50 Beschäftigte oder 10 Mio. Euro Umsatz
- Frühe Einordnung nach §28 NIS2UmsuCG ist Pflicht

TRACK & TRACE / TMS

Frachtsysteme absichern

- TMS, Sendungsverfolgung, EDI-Schnittstellen und Hafen-/Flughafen-IT sind primäre Ziele
- Ein Ausfall legt ganze Lieferketten lahm
- NIS2 fordert Angriffserkennung, Zugriffskontrolle, Notfallkonzepte
- Gilt für alle geschäftskritischen Logistiksysteme

LIEFERKETTEN & PARTNER

Das Rückgrat absichern

- Logistik ist das Rückgrat aller Lieferketten
- NIS2 fordert die Absicherung von Subunternehmern und Frachtführern
- Auch Telematik-Anbieter und IT-Dienstleister einbeziehen
- Sicherheitsanforderungen vertraglich verankern und überprüfen

GESCHÄFTSFÜHRERHAFTUNG

Chefsache mit Bußgeldrisiko

- Management haftet persönlich für Umsetzung und Überwachung (§38)
- Besonders wichtige Einrichtungen: bis 10 Mio. Euro oder 2 %
- Wichtige Einrichtungen: bis 7 Mio. Euro oder 1,4 %
- Cybersicherheit wird zur Chefsache

Annex 1 & 2

Verkehr als besonders wichtige (Häfen, Flughäfen) und wichtige Einrichtung (Spedition)

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 Meldefähigkeit, strukturiert und auf Transport, Spedition und Hafen-/Flughafenlogistik zugeschnitten.

SCHRITT 01

Betroffenheit klären

- [ ] **Einordnung** als besonders wichtige vs. wichtige Einrichtung prüfen (§28)
- [ ] **Sektorzuordnung:** Luftfahrt, Schifffahrt, Schiene, Straßenverkehr abgrenzen
- [ ] **Größenmerkmale** ab 50 MA oder 10 Mio. € Umsatz abgleichen
- [ ] **Tochtergesellschaften** und Standorte einbeziehen
- [ ] **Einstufungsergebnis** schriftlich dokumentieren

SCHRITT 02

Kritische Systeme erfassen

- [ ] **TMS, Track-&-Trace,** EDI- und Telematik-Systeme inventarisieren
- [ ] **Hafen-/Flughafen-Betriebssysteme** und Frachtabfertigung dokumentieren
- [ ] **Schnittstellen** zu Zoll, Partnern und Kunden erfassen
- [ ] **Verantwortlichkeiten** und Asset-Owner festlegen
- [ ] **Asset-Inventar** zentral und aktuell führen

SCHRITT 03

Risikoanalyse & Maßnahmen

- [ ] **Bedrohungen** für Transport-IT, Telematik und Lieferkette bewerten
- [ ] **Zugriffskontrolle,** MFA und Netzwerksegmentierung umsetzen
- [ ] **Angriffserkennung** für geschäftskritische Systeme einplanen
- [ ] **Maßnahmen** nach §30 Abs. 2 NIS2UmsuCG dokumentieren
- [ ] **Risiken** priorisieren und Verantwortliche zuordnen

SCHRITT 04

Lieferkette absichern

- [ ] **Sicherheitsanforderungen** an Frachtführer und Subunternehmer definieren
- [ ] **NIS2-konforme Klauseln** in Verträge und AVV aufnehmen
- [ ] **Fernzugänge** von Telematik- und IT-Dienstleistern absichern
- [ ] **Sicherheitsbewertung** kritischer Partner regelmäßig einplanen
- [ ] **Kritische Abhängigkeiten** dokumentieren

SCHRITT 05

Vorfallsmanagement & Meldung

- [ ] **Incident-Response-Prozess** für Transport- und Hafen-IT aufbauen
- [ ] **24-Stunden-Meldekette** an BSI/Behörde einrichten und testen
- [ ] **Meldevorlagen** für Erst- (24 h), Folge- (72 h) und Abschlussbericht
- [ ] **Business-Continuity-Plan** für Logistikausfälle erstellen
- [ ] **Verantwortliche** für den Ernstfall benennen

SCHRITT 06

Leitung & Schulung

- [ ] **Geschäftsführung** in Risikomaßnahmen einbinden und schulen (§38)
- [ ] **Billigung** und Überwachung der Sicherheitsmaßnahmen dokumentieren
- [ ] **Awareness-Schulungen** für Disposition, IT und Lager einplanen
- [ ] **Wirksamkeit** regelmäßig überprüfen
- [ ] **Reviews** und Nachbesserungen fest verankern

SECJUR

Häufige Stolperfallen und Quick Wins

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

STOLPERFALLE 01

Telematik als blinder Fleck

- [ ] **Fahrzeug-Telematik** und IoT-Sensorik nicht als Angriffsfläche erkannt
- [ ] **Track-&-Trace-Plattformen** ohne Sicherheitskonzept betrieben
- [ ] **Keine Angriffserkennung** für vernetzte Flotten
- [ ] **Telematik** von Anfang an ins Sicherheitskonzept aufnehmen

QUICK WIN 01

Netzwerksegmentierung

- [ ] **Betriebs-IT** von Office- und Gäste-Netzen sofort trennen
- [ ] **Günstige Maßnahme** mit hoher Schutzwirkung
- [ ] **Angriffsfläche** wird erheblich und schnell reduziert
- [ ] **Erster sichtbarer Fortschritt** Richtung NIS2-Readiness

STOLPERFALLE 02

Partner-Kette unterschätzt

- [ ] **Subunternehmer und Frachtführer** ohne Sicherheitsanforderungen
- [ ] **EDI-Schnittstellen** zu Kunden und Zoll ungeprüft
- [ ] **Ein Angriff** über einen Partner trifft den gesamten Betrieb
- [ ] **Keine Übersicht** über kritische Partner und Zugänge

QUICK WIN 02

ISO 27001 nutzen

- [ ] **Bestehendes ISMS** ist direkt auf NIS2 anrechenbar
- [ ] **Gap-Analyse** zeigt konkrete Ergänzungsbedarfe
- [ ] **Ein Rahmenwerk** für NIS2 und Informationssicherheit
- [ ] **Vorhandene Nachweise** gezielt wiederverwenden

STOLPERFALLE 03

Ausfall nicht geprobt

- [ ] **Kein getesteter Notfallplan** für IT-Ausfall in der Disposition
- [ ] **Ransomware** legt Sendungsverfolgung und Abfertigung lahm
- [ ] **Manuelle Rückfallprozesse** seit Jahren nicht aktualisiert
- [ ] **Ernstfall** regelmäßig üben, bevor er eintritt

QUICK WIN 03

Meldeprozess als 1-Seiter

- [ ] **Meldevorlage** für die Behörde in rund zwei Stunden erstellbar
- [ ] **Eskalationskette** auf einer A4-Seite festhalten
- [ ] **Im Ernstfall** enorm stressreduzierend
- [ ] **Von Unsicherheit** zu handlungsfähiger Meldekette

SECJUR

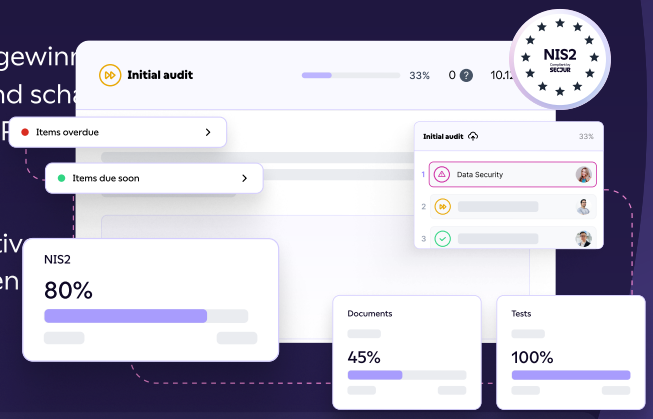
Mit SECJUR zu 100 % NIS2-Compliance

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