SECJUR

NIS2 für Luftfahrt & Verteidigung

Warum Airlines, Flughäfen, Raumfahrt und Wehrtechnik zu den am strengsten regulierten NIS2-Sektoren zählen, und wie Readiness gelingt.

Der Luftfahrt- und Verteidigungssektor berührt gleich mehrere NIS2-Sektoren: Luftverkehr (Airlines, Flughäfen, Flugsicherung) und Weltraum gelten als **besonders wichtige Einrichtungen** (Annex 1), die Herstellung von Luft-, Raumfahrt- und Wehrtechnik als wichtige Einrichtung (Annex 2). Das **NIS2-Umsetzungsgesetz (NIS2UmsuCG)** stellt hohe Anforderungen an IT- und OT-Sicherheit. Besonders exponiert: Avionik, Flugsicherung, Satelliten-Bodenstationen und sicherheitskritische Lieferketten.

In diesen vier Situationen wird NIS2 für Aerospace & Defense konkret:

BETROFFENHEIT & EINSTUFUNG

Annex 1 und Annex 2

- Airlines, Flughäfen und Flugsicherung als besonders wichtige Einrichtungen (Annex 1)
- Betreiber von Satelliten-Bodeninfrastruktur im Sektor Weltraum
- Luft-, Raumfahrt- und Verteidigungshersteller als wichtige Einrichtungen (Annex 2)
- Frühe Einordnung nach §28 NIS2UmsuCG ist Pflicht

AVIONIK & FLUGSICHERUNG

Sicherheitskritische Systeme

- Flight-Management-Systeme, Avionik, ATM und Satelliten-Kommunikation sind hochkritisch
- Ein erfolgreicher Angriff gefährdet unmittelbar die Sicherheit
- NIS2 fordert Angriffserkennung, Segmentierung, Notfallkonzepte
- Gilt auch für sicherheitskritische Betriebssysteme

SICHERHEITSKRITISCHE LIEFERKETTE

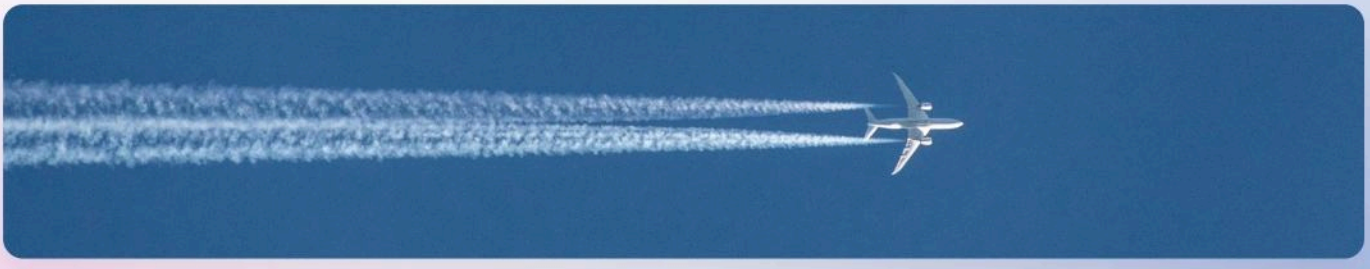
Global und mehrstufig

- Aerospace-&-Defense-Lieferketten sind mehrstufig und global
- Absicherung von Zulieferern, MRO-Betrieben und Technologiepartnern
- Anforderungen vertraglich verankern, prüfen und durchsetzen
- Auch Exportkontrolle und Geheimschutz mitdenken

LEITUNGSHAFTUNG & AUFSICHT

Strenge behördliche Prüfung

- Management haftet persönlich für Umsetzung und Überwachung (§38)
- Besonders wichtige Einrichtungen: bis 10 Mio. Euro oder 2 %
- Strenge Aufsicht (§61–62) mit Vor-Ort-Prüfungen
- Cybersicherheit wird zur Chefsache



Annex 1 & 2
Luftverkehr und Weltraum (besonders wichtig) plus Herstellung (wichtig)

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 Aufsichtsfähigkeit, strukturiert und auf Airlines, Flughäfen, Raumfahrt und Wehrtechnik zugeschnitten.

SCHRITT 01

Betroffenheit klären

- [ ] **Einordnung** als besonders wichtige vs. wichtige Einrichtung prüfen (§28)
- [ ] **Sektorzuordnung:** Luftverkehr, Weltraum, Herstellung abgrenzen
- [ ] **Schnittstellen** zu nationaler Sicherheit / Verteidigung gesondert bewerten
- [ ] **Tochtergesellschaften** und Standorte einbeziehen
- [ ] **Einstufungsergebnis** schriftlich dokumentieren

SCHRITT 02

Kritische Systeme erfassen

- [ ] **Avionik, FMS, ATM-** und Satelliten-Bodensysteme inventarisieren
- [ ] **Konstruktions-, PLM-** und Fertigungs-IT (OT) dokumentieren
- [ ] **Schnittstellen** zu Behörden, Partnern und MRO-Betrieben erfassen
- [ ] **Verantwortlichkeiten** und Asset-Owner festlegen
- [ ] **Asset-Inventar** zentral und aktuell führen

SCHRITT 03

Risikoanalyse & Maßnahmen

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

SCHRITT 04

Lieferkette & Exportkontrolle

- [ ] **Sicherheitsanforderungen** an Zulieferer und MRO-Betriebe definieren
- [ ] **NIS2-konforme Klauseln** in Verträge und AVV aufnehmen
- [ ] **Exportkontroll- und Geheimschutzauflagen** mit IT-Sicherheit verzahnen
- [ ] **Sicherheitsbewertung** kritischer Partner regelmäßig einplanen
- [ ] **Kritische Abhängigkeiten** dokumentieren

SCHRITT 05

Vorfallsmanagement & Meldung

- [ ] **Incident-Response-Prozess** für Avionik- und Betriebs-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 sicherheitskritische Systeme erstellen
- [ ] **Verantwortliche** für den Ernstfall benennen

SCHRITT 06

Leitung & Aufsicht

- [ ] **Geschäftsführung** in Risikomaßnahmen einbinden und schulen (§38)
- [ ] **Vor-Ort-Prüfungen** der Aufsichtsbehörde vorbereiten (§61–62)
- [ ] **Awareness-Schulungen** für Technik, IT und Engineering einplanen
- [ ] **Wirksamkeitsreviews** und interne Audits verankern
- [ ] **Kontinuierliche Verbesserung** fest verankern

SECJUR

Häufige Stolperfallen und Quick Wins

Was Aerospace-&-Defense-Unternehmen bei NIS2 typischerweise unterschätzen, und womit sich schnell Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

Avionik/OT als blinder Fleck

- [ ] **Avionik und Prüfstände** nicht als IT-Assets behandelt
- [ ] **Engineering- und Fertigungs-OT** ohne Sicherheitskonzept
- [ ] **Keine Angriffserkennung** für sicherheitskritische Systeme
- [ ] **Betriebstechnik** von Anfang an mitdenken, nicht nachrüsten

QUICK WIN 01

Netzwerksegmentierung

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

STOLPERFALLE 02

Compliance-Silos

- [ ] **NIS2, Exportkontrolle und Geheimschutz** getrennt behandelt
- [ ] **Doppelter Aufwand** statt integriertem Managementsystem
- [ ] **Lücken** an den Schnittstellen der Regelwerke
- [ ] **Regelwerke** in ein gemeinsames System zusammenführen

QUICK WIN 02

ISO 27001 / EN 9100 nutzen

- [ ] **Bestehendes ISMS** ist direkt auf NIS2 anrechenbar
- [ ] **EN 9100** (Aerospace-QM) als Brücke zur Risikosteuerung
- [ ] **Gap-Analyse** zeigt konkrete Ergänzungsbedarfe
- [ ] **Doppelaufwand** vermeiden, Rahmenwerke kombinieren

STOLPERFALLE 03

Lieferkette unterschätzt

- [ ] **Mehrstufige Zulieferer** ohne Sicherheitsanforderungen
- [ ] **MRO- und Technologiepartner** als Einfallstor ignoriert
- [ ] **Ein Angriff** über die Kette trifft sicherheitskritische Produkte
- [ ] **Keine Übersicht** über kritische Abhängigkeiten

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

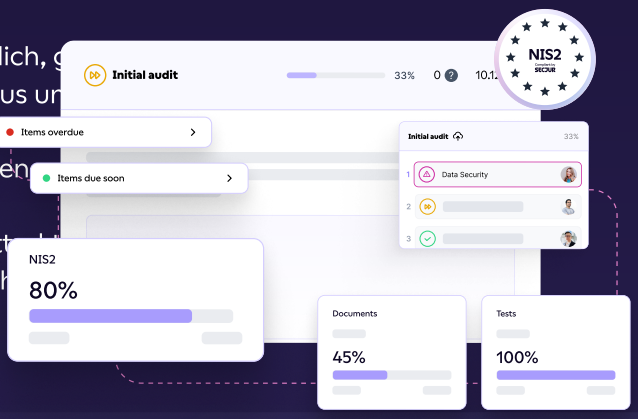
Mit SECJUR zu 100 % NIS2-Compliance

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, g
Transparenz über Ihren Compliance-Status ur
eine belastbare Grundlage für regulator
und anspruchsvolle Kundenanforderungen



Für unsere Bestandskunden bieten wir att
Konditionen, um frühzeitig Klarheit zu sch
NIS2-Readiness planbar umzusetzen.

→ **Jetzt informieren**

Mit SECJUR zu Informationssicherheitszertifizierungen:

“Wir konnten wie geplant neue OEM-Projekte erlangen und so den Unternehmensumsatz steigern. Die Plattform ist super hilfreich und unsere Ansprechpartnerin unterstützt uns stets kompetent.”

Steffen Brureiner
Projektleiter IT

KLEINER STANZTECHNIK
CoCREATE THE FUTURE

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

STAHLWERK THÜRINGEN · OTTO DÖRNER · oetinger aluminium · FEDDERSEN GRUPPE · STEYRMOTORS

www.secjur.com