SECJUR

NIS2 für die Lebensmittelbranche

Warum Hersteller, Verarbeiter und Händler ins Visier der NIS2-Aufsicht geraten, und wie Readiness gelingt.

Die Lebensmittelbranche ist als **wichtige Einrichtung** in Annex 2 der NIS2-Richtlinie gelistet. Hersteller, Verarbeiter und Händler ab 50 Beschäftigten oder 10 Mio. Euro Umsatz sind betroffen. In Deutschland setzt das **NIS2-Umsetzungsgesetz (NIS2UmsuCG)** verbindliche Anforderungen an IT-Sicherheit, Risikomanagement und Managementhaftung. Besonders exponiert: Lieferketten, Produktionssteuerung und Qualitätssicherung.

In diesen vier Situationen wird NIS2 für Lebensmittelunternehmen konkret:

BETROFFENHEIT & EINSTUFUNG

Annex 2, wichtige Einrichtung

- Lebensmittelunternehmen fallen unter Annex 2 als wichtige Einrichtungen
- Schwelle: ab 50 Beschäftigte oder 10 Mio. Euro Umsatz und Bilanzsumme
- Auch Tochtergesellschaften und Lohnhersteller können erfasst sein
- Frühe Einordnung nach §28 NIS2UmsuCG vermeidet Überraschungen

LIEFERKETTENSICHERHEIT

Zulieferer absichern

- Lebensmittelproduzenten hängen in komplexen Zulieferernetzwerken
- NIS2 fordert ausdrücklich die Absicherung der Lieferkette
- Anforderungen an Dienstleister, ERP-Schnittstellen, Logistikpartner
- Vertraglich verankern und regelmäßig überprüfen

PRODUKTIONSSCHUTZ & OT

Produktion nicht stilllegen

- Automatisierte Linien, SCADA und MES sind attraktive Angriffsziele
- Ein Cyberangriff kann den Betrieb stilllegen und Rückrufe auslösen
- NIS2 fordert Angriffserkennung, Segmentierung, Notfallwiederherstellung
- Gilt ausdrücklich auch für OT-Systeme

GESCHÄFTSFÜHRERHAFTUNG

Chefsache mit Bußgeldrisiko

- Management haftet persönlich für Umsetzung und Überwachung (§38)
- Pflichtschulung, Billigung und Überwachung sind gesetzlich verankert
- Bußgelder bis 7 Mio. Euro oder 1,4 % des globalen Umsatzes
- Cybersicherheit wird zur Chefsache

Annex 2
Lebensmittelsektor als wichtige Einrichtung, NIS2-Pflichten ab 50 MA oder 10 Mio. € Umsatz

24 h
Frist für die Erstmeldung erheblicher Sicherheitsvorfälle an die Behörde

bis 7 Mio. €
Maximales Bußgeld für wichtige Einrichtungen bei Verstößen gegen NIS2UmsuCG

SECJUR

NIS2-Readiness in 6 Schritten

Von der Betroffenheitsprüfung bis zur Meldefähigkeit, strukturiert und auf die Lebensmittelbranche zugeschnitten.

SCHRITT 01

Betroffenheit klären

- [ ] **Einordnung** als wichtige Einrichtung nach Annex 2 prüfen (§28)
- [ ] **Größenmerkmale:** ab 50 MA oder 10 Mio. € Umsatz und Bilanzsumme
- [ ] **Tochtergesellschaften,** Lohnhersteller und Konzernstruktur einbeziehen
- [ ] **Einstufungsergebnis** schriftlich dokumentieren
- [ ] **Einordnung** bei Unsicherheit fachlich gegenprüfen

SCHRITT 02

Kritische Assets erfassen

- [ ] **ERP-, MES- und SCADA-Systeme** in der Produktion inventarisieren
- [ ] **Schnittstellen** zu Logistik, Handel und Lieferanten dokumentieren
- [ ] **Kritische Prozesse** (Produktion, QS, Rückverfolgung) identifizieren
- [ ] **Verantwortlichkeiten** und Asset-Owner festlegen
- [ ] **Asset-Inventar** zentral und aktuell führen

SCHRITT 03

Risikoanalyse & Maßnahmen

- [ ] **Bedrohungen** für Produktion, Lieferkette und IT-Systeme bewerten
- [ ] **Zugriffskontrolle,** MFA und Netzwerksegmentierung implementieren
- [ ] **Patch-Management** und Schwachstellenscans etablieren
- [ ] **Maßnahmen** nach §30 Abs. 2 NIS2UmsuCG dokumentieren
- [ ] **Risiken** priorisieren und Verantwortliche zuordnen

SCHRITT 04

Lieferkette absichern

- [ ] **Sicherheitsanforderungen** an Dienstleister und Lieferanten definieren
- [ ] **NIS2-konforme Klauseln** in Verträge und AVV aufnehmen
- [ ] **Fernwartungszugänge** von IT-Dienstleistern absichern und protokollieren
- [ ] **Sicherheitsbewertung** kritischer Lieferanten regelmäßig einplanen
- [ ] **Kritische Abhängigkeiten** dokumentieren

SCHRITT 05

Vorfallsmanagement & Meldung

- [ ] **Incident-Response-Prozess** für IT und OT/Produktion aufbauen
- [ ] **24-Stunden-Meldekette** an BSI/Behörde einrichten und testen
- [ ] **Meldevorlagen** für Erst- (24 h), Folge- (72 h) und Abschlussbericht
- [ ] **Business-Continuity-Plan** für Produktionsausfälle 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 Produktion und IT einplanen
- [ ] **Wirksamkeit** regelmäßig überprüfen
- [ ] **Reviews** und Nachbesserungen fest verankern

SECJUR

Häufige Stolperfallen und Quick Wins

Was Lebensmittelunternehmen bei NIS2 häufig unterschätzen, und womit sich schnell Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

»Wir sind kein Tech-Unternehmen«

- [ ] **NIS2** gilt branchenübergreifend, auch für Produzenten und Händler
- [ ] **Digitale Produktionssteuerung** und ERP erhöhen die Angriffsfläche
- [ ] **Betroffenheit** früh prüfen statt auf die Behördenanfrage warten
- [ ] **Auch analoge Betriebe** haben längst kritische IT

QUICK WIN 01

Betroffenheitsprüfung in 1 h

- [ ] **Sektorcheck** und Größenmerkmale in unter einer Stunde klärbar
- [ ] **Ergebnis** schriftlich festhalten, schützt vor späteren Vorwürfen
- [ ] **Sofortiger Überblick** über den Handlungsbedarf
- [ ] **Klare Basis** für alle weiteren Schritte

STOLPERFALLE 02

Lieferkette nicht berücksichtigt

- [ ] **Zulieferer und Logistikpartner** als Einfallstor unterschätzt
- [ ] **Keine vertraglichen** Sicherheitsanforderungen an IT-Dienstleister
- [ ] **Ein Angriff** über die Lieferkette trifft den Betrieb genauso hart
- [ ] **Keine Übersicht** über kritische Abhängigkeiten

QUICK WIN 02

ISO 22301 / ISO 9001 nutzen

- [ ] **Bestehende QM- und BCM-Prozesse** direkt auf NIS2 anrechenbar
- [ ] **Gap-Analyse** zeigt konkrete Ergänzungsbedarfe
- [ ] **Ein Rahmenwerk** für mehrere Standards statt Doppelaufwand
- [ ] **Vorhandene Nachweise** gezielt wiederverwenden

STOLPERFALLE 03

Produktion und IT getrennt gedacht

- [ ] **OT/SCADA-Systeme** nicht ins Sicherheitskonzept einbezogen
- [ ] **Kein Notfallplan** für Produktionsausfall durch Cyberangriff
- [ ] **IT/OT-Segmentierung** als wichtigste Schutzmaßnahme vernachlässigt
- [ ] **Produktion und IT** gehören in ein gemeinsames Konzept

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.

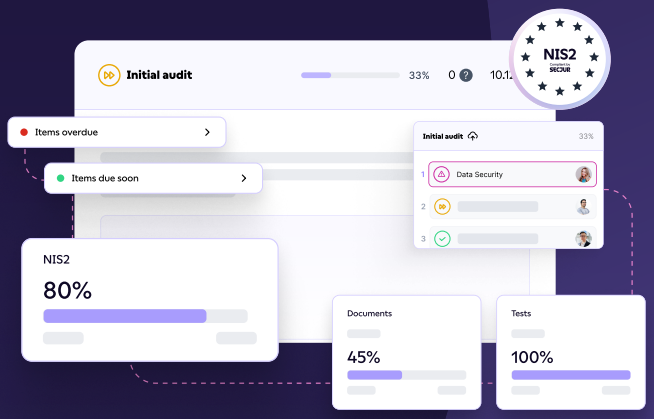
Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- 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, gewinnen Transparenz über Ihren Compliance-Status und schaffen eine belastbare Grundlage für regulatorische Prüfungen und anspruchsvolle Kundenanforderungen.

Für unsere Bestandskunden bieten wir attraktive Konditionen, um frühzeitig Klarheit zu schaffen und NIS2-Readiness planbar umzusetzen.

→ **Jetzt informieren**



Mit SECJUR zur automatisierten Compliance

"Mit SECJUR lassen sich alle NIS2-Anforderungen auf einer Plattform umsetzen. Dadurch konnten wir binnen einer Woche ein zentrales, skalierbares Richtliniensystem für die NIS2"

Dipl. Ing. Michael Dohr
Manager IT Security

Nordzucker

FRUCHTHOF NORTHEIM · FRUCHTHANSA · PETER KÖLLN · Trolli · yfood · demeter

www.secjur.com