SECJUR

WHITEPAPER
2026

NIS2 · LEBENSMITTEL, PRODUKTION & HANDEL

NIS2 in der Lebensmittelbranche: Sicherheit bis ins Regal.

Die Lebensmittelbranche ist hochautomatisiert und eng mit dem Handel verzahnt. Genau das macht sie verwundbar: Ein IT-Ausfall stoppt die Produktion, und verderbliche Ware wartet nicht. Das NIS2-Umsetzungsgesetz gilt seit Dezember 2025 und erfasst Produktion, Verarbeitung und Vertrieb von Lebensmitteln ab bestimmten Schwellen. Zugleich verlangt der Handel von seinen Lieferanten zunehmend nachweisbare Sicherheit. Dieses Whitepaper zeigt, welche Pflichten gelten, wo die größten Schwachstellen in IT und Produktionstechnik liegen und wie ein ISMS entsteht, das zur Branche passt.

NIS2 | ISO 27001 | IFS | ISO 9001 | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In der Lebensmittelbranche schützt Sicherheit die Lieferfähigkeit.

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. Bundesweit fallen rund 29.500 Unternehmen in 18 Sektoren darunter, und der Sektor Lebensmittel gehört ausdrücklich dazu.

NIS2 erfasst die Produktion, Verarbeitung und den Vertrieb von Lebensmitteln ab den Schwellen von 50 Beschäftigten oder 10 Millionen Euro. Die meisten Betriebe gelten damit als wichtige Einrichtungen, große Hersteller als besonders wichtige. Maßgeblich sind Sektor und Größe, nicht das Selbstbild. Für viele Familien- und Mittelstandsbetriebe der Branche ist das neu, weil Cyber-Regulierung lange als Thema anderer galt. Wer die Prüfung sauber dokumentiert, schafft Klarheit und schützt die Geschäftsführung im Zweifel vor Haftung.

WARUM JETZT HANDELN

Der Druck kommt von zwei Seiten. Der Lebensmitteleinzelhandel gibt seine Sicherheitsanforderungen über die Lieferkette weiter und verlangt den Nachweis vertraglich, ähnlich wie es IFS und BRC für die Lebensmittelsicherheit längst tun. Parallel läuft die NIS2-Pflicht mit Registrierung und Meldewegen.

Hinzu kommt die Bedrohungslage. Ransomware zählt zu den größten Risiken für die Wirtschaft, und in der Lebensmittelproduktion wird ein Stillstand sofort teuer, weil verderbliche Ware und enge Lieferfenster keinen Aufschub dulden. Ein Vorfall trifft hier nicht nur die IT, sondern sofort die Lieferfähigkeit an den Handel.

EIN AUFBAU, ZWEI ERGEBNISSE

Die gute Nachricht: Ein ISMS nach ISO 27001 deckt einen Großteil der NIS2-Pflichten ab, etwa Risikomanagement, Lieferkettensicherheit und Notfallvorsorge. Zugleich beantwortet es die Sicherheitsfragebögen des Handels. Die aus IFS und BRC bekannte Audit-Kultur ist dabei ein echter Vorsprung, weil Dokumentation und Korrekturmaßnahmen längst vertraut sind.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken in IT und Produktionstechnik, die Pflichten aus dem Gesetz und eine Roadmap, die zum Betrieb passt statt zum Konzern. So bleibt die knappe Kapazität an der Produktion, statt in Formularen zu versickern.

BETROFFEN

29.500

Unternehmen in 18 Sektoren fallen unter NIS2, der Sektor Lebensmittel 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 Lebensmittelbranche läuft auf Termin und Vertrauen.

Vom Wareneingang bis ins Regal ist die Lebensmittelproduktion ein eng getakteter, digital gesteuerter Prozess. Verderbliche Ware und feste Lieferfenster lassen keinen Stillstand zu, und der Handel verlangt von seinen Lieferanten nachweisbare Sicherheit.

Verderbliche Ware kennt keine Geduld. *Steht die Produktion, ist die Charge verloren.*

AUTOMATISIERT VON DER LINIE BIS ZUM ERP

Moderne Lebensmittelbetriebe steuern ihre Produktion über vernetzte Systeme: ERP und Warenwirtschaft, Manufacturing-Execution-Systeme, Abfüll- und Verpackungsanlagen, Kühl- und Lagertechnik sowie die elektronische Anbindung an den Handel über EDI. Rückverfolgbarkeit verlangt zudem lückenlose Daten von der Charge bis zur Auslieferung.

Diese durchgehende Digitalisierung schafft Effizienz und Angriffsfläche zugleich. Wo IT und Produktionstechnik zusammentreffen, entstehen die kritischen Punkte, die NIS2 in den Blick nimmt. Schon ein Blick auf die Übergänge zwischen Linie und ERP zeigt, wo die dringendsten Lücken liegen.

DER HANDEL GIBT DEN TAKT VOR

Der Lebensmitteleinzelhandel ist mächtig und anspruchsvoll. Wer als Lieferant gelistet bleiben will, muss liefern, was der Handel fordert, und das umfasst zunehmend Informationssicherheit. Sicherheitsfragebögen und Lieferantenprüfungen sind aus dem Qualitätsbereich längst bekannt und greifen nun auch auf die IT über.

Ein ISMS beantwortet einen Großteil dieser Anforderungen mit einem einzigen Nachweis. Statt jeden Fragebogen einzeln zu bearbeiten, legt der Hersteller das anerkannte Dokument vor und bleibt verlässlicher Partner. Wer den Nachweis früh vorlegt, verschafft sich einen Vorsprung in der nächsten Listungsrunde.

DIE NIS2-VERBINDUNG

NIS2 erfasst die Produktion, Verarbeitung und den Vertrieb von Lebensmitteln ab bestimmten Schwellen. Wer ein ISMS nach ISO 27001 betreibt, erfüllt damit einen Großteil der NIS2-Pflichten, etwa Risikomanagement, Lieferkettensicherheit und Notfallvorsorge. Ein Aufbau, zwei Ergebnisse.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als IT: verlorene Chargen, gerissene Liefertermine, Vertragsstrafen und ausgelistete Produkte. Hinzu kommen wertvolle Rezepturen und die Integrität der Rückverfolgbarkeit, die für die Lebensmittelsicherheit unverzichtbar ist.

Sicherheit schützt hier das Kerngeschäft. Ein sauberer Nachweis sichert Listungen und Lieferfähigkeit und macht aus einer Pflicht einen Vorsprung gegenüber Wettbewerbern. Ein einziger längerer Stillstand kann eine ganze Saisonplanung durcheinanderbringen.

HERAUSFORDERUNGEN

Warum NIS2 in der Lebensmittelbranche besonders fordert.

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

ZEITKRITIKALITÄT UND VERDERBLICHE WARE

Anders als in vielen Industrien lässt sich ein Produktionsstopp nicht einfach nachholen. Steht die Linie, verdirbt Ware, Kühlketten reißen, und feste Lieferfenster des Handels platzen. Der Druck zur schnellen Wiederherstellung ist enorm. Für das ISMS heißt das: kurze Wiederanlaufzeiten, getestete Backups und ein belastbarer Notfallplan. Genau diese Vorsorge verlangt auch NIS2. Ein zweiter, getrennter Datenstand verkürzt den Wiederanlauf spürbar.

IT TRIFFT PRODUKTIONSTECHNIK

Neben klassischer IT steuern operative Systeme den Betrieb: MES, Abfüllanlagen, Kühl- und Fördertechnik. Vieles ist über Jahre gewachsen, läuft auf älteren Ständen und darf im Betrieb nicht einfach unterbrochen werden. Diese Übergänge verdienen in der Risikoanalyse besondere Aufmerksamkeit. Kompensierende Maßnahmen wie Netzsegmentierung schützen, wo ein Update nicht möglich ist. Eine klare Trennung von Büro- und Produktionsnetz ist dabei der wirksamste erste Schritt.

DÜNNE MARGEN, HOHE VOLUMINA

Die Branche arbeitet mit knappen Margen und großen Mengen. Budget für Sicherheit ist selten üppig. Hier hilft das Prinzip der Verhältnismäßigkeit: Maßnahmen richten sich nach Größe und Risiko, nicht nach Konzernmaßstab. So bleibt die Investition überschaubar und der Nutzen, vermiedene Ausfälle und gehaltene Listungen, messbar.

AUDIT-KULTUR ALS VORSPRUNG

Anders als viele Branchen kennt die Lebensmittelproduktion strenge Audits längst, etwa nach IFS oder BRC. Dokumentation, Rückverfolgbarkeit und Korrekturmaßnahmen sind vertraut. Diese Kultur lässt sich auf das ISMS übertragen und verkürzt den Weg zur NIS2-Konformität spürbar. Wer die Nachweise laufend pflegt, besteht die nächste Prüfung ohne Hektik.

DÜNNE IT-DECKE

Viele Hersteller 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.

BETROFFENHEIT ÜBER DIE KETTE

Auch wer knapp unter den Schwellen bleibt, entkommt selten. Große Handels- und Industriekunden reichen ihre NIS2-Pflichten über die Lieferkette weiter und verlangen den Nachweis vertraglich. Der eigene Sicherheitsnachweis wird so zur Bedingung für die nächste Listung.

BEDROHUNGSLAGE & RISIKEN

Wo die Lebensmittelbranche konkret angreifbar ist.

Die Risiken sind selten abstrakt. Sie hängen an einer eng getakteten, automatisierten Produktion, an wertvollen Rezepturen und an der engen Anbindung an den Handel. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE STOPPT DIE PRODUKTION

Der häufigste und teuerste Ernstfall. Werden ERP, MES oder Steuerungssysteme verschlüsselt, steht die Linie. Verderbliche Ware verdirbt, Kühlketten sind gefährdet, und feste Lieferfenster des Handels reißen. Getestete, vom Netz getrennte Backups und ein eingeübter Notfallplan entscheiden, ob der Stillstand Stunden oder Tage dauert, und damit über den Schaden. 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 Zulieferer, Logistiker oder IT-Dienstleister wird zum Einfallstor. Genau hier setzt die Lieferkettensicherheit nach §30 an, mit Mindestanforderungen und deren Überprüfung. Der Handel fordert denselben Nachweis zunehmend auch vom Hersteller selbst ein. Ein aktuelles Verzeichnis aller Zulieferer und Zugänge ist die Grundlage, um die Kette zu überblicken. Wer seine Schnittstellen sauber führt, besteht die Prüfungen des Handels ohne Hektik.

3 · MANIPULATION DER PRODUKTIONSTECHNIK

Werden MES, Rezeptursteuerung oder Kühltechnik manipuliert, drohen nicht nur Ausfälle, sondern im Extremfall Risiken für die Lebensmittelsicherheit, etwa durch veränderte Mischungsverhältnisse oder unterbrochene Kühlung. Die Trennung von IT und OT sowie strenge Zugänge sind hier zentral und schützen zugleich Mensch und Marke. Eine kontinuierliche Überwachung erkennt Manipulationen, bevor sie die Ware erreichen. Im Zweifel schützt ein sicherer Rückfallmodus Mensch und Produkt.

4 · DIEBSTAHL VON REZEPTUREN UND DATEN

Rezepturen, Verfahren und Konditionen mit dem Handel sind das Kapital vieler Hersteller. Werden sie abgegriffen, ist der Wettbewerbsvorsprung dahin. Verschlüsselung und strenge Zugriffskontrolle schützen dieses Wissen vor Abfluss, und eine Protokollierung macht ungewöhnliche Zugriffe früh sichtbar. Wer weiß, wo die wertvollsten Rezepturdaten liegen, kann sie zuerst und am stärksten schützen.

5 · INTEGRITÄT DER RÜCKVERFOLGBARKEIT

Rückverfolgbarkeit ist gesetzlich gefordert und für Rückrufe überlebenswichtig. Werden Chargen- und Herkunftsdaten verfälscht oder gelöscht, ist im Ernstfall kein sauberer Rückruf möglich. Schutz der Datenintegrität, Protokollierung und Backups sichern diese Nachweiskette. Getrennte, unveränderbare Sicherungen der Chargendaten sichern den Rückruf auch nach einem Angriff.

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 Sektor Lebensmittel umfasst Produktion, Verarbeitung und Vertrieb. Die Registrierung läuft über das Unternehmenskonto und das BSI-Portal, die Einstufung nimmt der Betrieb selbst vor. Sie sollte schriftlich begründet und bei jeder Änderung von Größe oder Geschäftsmodell aktualisiert werden. 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. Produktions- und Kühltechnik gehören ausdrücklich dazu. Wer bereits ein ISMS nach ISO 27001 oder eine gelebte IFS-/BRC-Struktur hat, bringt vieles mit 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 die Produktion 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. Aus dem Qualitätsmanagement ist diese Leitungsverantwortung vielen Betrieben bereits vertraut. 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, 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 aus dem Qualitätsmanagement, statt bei null zu beginnen. Realistisch führt der Weg in wenigen Monaten zu einem auditbereiten Stand.

Wer IFS und BRC kennt, kennt die Audit-Logik. *NIS2 und ISO 27001 bauen darauf auf.*

1 · BETROFFENHEIT UND GELTUNGSBEREICH

Sektor und Schwellenwerte prüfen, auch die Rolle als Zulieferer, und die Einstufung dokumentieren. Den Scope eng schneiden: welcher Standort, welche Produktion, welche Systeme. 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 ERP und MES über Kühl- und Abfülltechnik bis zur Anbindung an den Handel. Risiken bewerten, Verfügbarkeit und Datenintegrität besonders gewichten und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Mit den wirksamsten Hebeln beginnen: Backup, Zugriffskontrolle, Netztrennung von Produktion und IT sowie 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 jede Abteilung 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 Produktion und Verwaltung noch hakt.

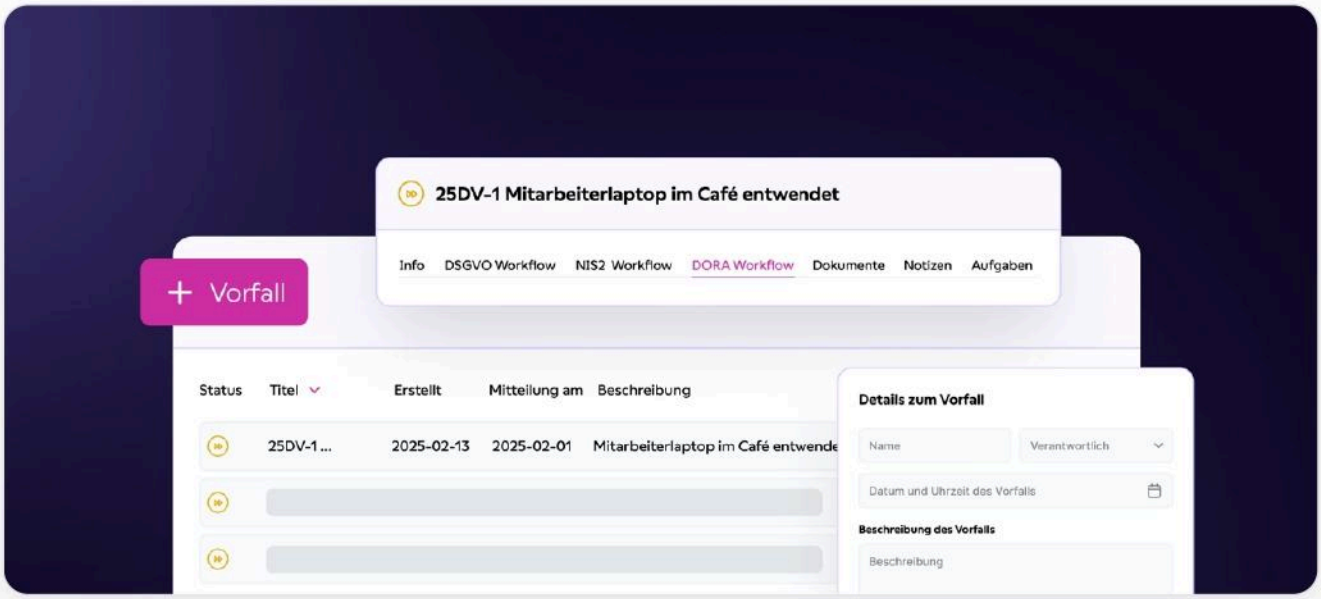
6 · PRÜFEN, NACHWEISEN, VERBESSERN

Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Für Betriebe mit IFS- oder BRC-Erfahrung ist diese Schleife vertrautes Terrain. Wer sie einmal vollständig durchläuft, ist zugleich reif für die ISO-27001-Zertifizierung und den nächsten Handelsnachweis. 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 Lebensmittelbetriebe durch die NIS2-Umsetzung: Risiken in IT und Produktionstechnik, 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 Produktion

Eine Risikoanalyse, die Verwaltung und Produktionstechnik zusammen denkt, mit Vorlagen, die zum Lebensmittelbetrieb 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.

Handel & Nachweise

Lieferantensteuerung und ein Nachweis, der die Sicherheitsfragebögen des Handels 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 die Produktion stehen bleibt.

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

EINE BEKANNTE AUDIT-KULTUR ZAHLT SICH AUS

Weil sich NIS2, ISO 27001 und die Erwartungen aus IFS und BRC weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus ERP, MES und Co., sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegt.

Für einen Hersteller heißt das weniger Doppelarbeit. Der NIS2-Nachweis lässt sich mit wenigen Ergänzungen zur ISO-27001-Zertifizierung ausbauen, statt jedes Mal von vorn zu beginnen.

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

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

Lebensmittelhersteller, Getränkeproduzenten, Logistiker und Industrieunternehmen erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Lebensmittelbranche:

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

Dipl.-Ing. Michael Dohr
Manager IT Security, Nordzucker

REFERENZEN AUS LEBENSMITTEL, INDUSTRIE UND HANDEL

PETER KÖLLN · Trolli · Nordzucker · yfood · demeter · STERNWYWIOL Gruppe

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 LEBENSMITTELBETRIEBE SECJUR WÄHLEN

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

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

Wo Fachwissen 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 Herstellern.

Und die Plattform denkt in der Realität eines Produktionsbetriebs. Sie priorisiert die Maßnahmen mit der größten Wirkung und macht auf einen Blick sichtbar, was noch offen ist, damit die Umsetzung planbar bleibt.

MEHR ALS EINE PFLICHTÜBUNG

Am Ende steht nicht nur ein erfülltes Gesetz, sondern ein Betrieb, der seine Produktion absichert, seine Rezepturen schützt und in der nächsten Lieferantenprüfung des Handels souverän auftritt. Genau das sichert Listungen und Lieferfähigkeit.

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

Weil derselbe Unterbau NIS2, ISO 27001 und die Erwartungen aus IFS und BRC zugleich trägt, zahlt eine bekannte Audit-Kultur direkt auf die Zertifizierung ein, statt getrennt abgearbeitet zu werden.

So wird aus einer Pflicht ein dauerhafter Schutz von Charge, Liefertermin und Ruf, der mit jeder neuen Anlage und jedem Handelspartner 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.

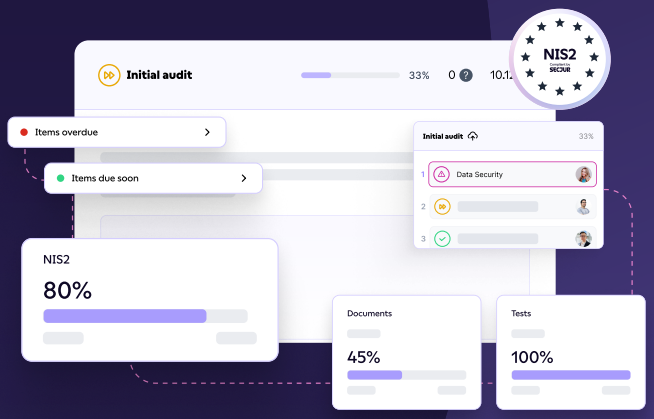
Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- 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, 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