SECJUR

WHITEPAPER
2026

NIS2 · MITTELSTAND & FAMILIENUNTERNEHMEN

NIS2 im Mittelstand: betroffen, auch wenn es überrascht.

Der Mittelstand sieht sich selten als Ziel strenger Cyber-Regulierung. Doch das NIS2-Umsetzungsgesetz gilt seit Dezember 2025 ohne Übergangsfrist, und über den eigenen Sektor oder die Rolle als Zulieferer sind viele mittelständische Unternehmen betroffen. Dieses Whitepaper zeigt, wann NIS2 greift, wo gewachsene IT und vernetzte Produktion angreifbar werden und wie sich die Pflichten aus §30, §32 und §38 mit schlanken Mitteln erfüllen lassen.

NIS2 | ISO 27001 | TISAX® | IEC 62443 | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Im Mittelstand ist Sicherheit zur Chefsache 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. Bundesweit fallen rund 29.500 Unternehmen in 18 Sektoren darunter, von der Energieversorgung bis zum verarbeitenden Gewerbe.

Für den Mittelstand ist entscheidend, dass Betroffenheit auf zwei Wegen entsteht: über den eigenen Sektor und über die Rolle als Zulieferer größerer, regulierter Kunden. Wer 50 Beschäftigte oder 10 Millionen Euro erreicht, ist im betroffenen Sektor eine wichtige Einrichtung. Viele unterschätzen das. Anders als beim früheren KRITIS-Recht kommt es nicht mehr auf einzelne Anlagen an, sondern auf Sektor und Größe, wodurch weit mehr Betriebe erfasst werden als bisher. Für viele Familienbetriebe ist das neu, denn Cyber-Regulierung galt lange als Thema großer Konzerne. Heute zählt jeder Betrieb, der die Schwelle erreicht. Die frühzeitige Klärung verhindert, dass aus einer Formalie ein teures Versäumnis wird.

WARUM JETZT HANDELN

Die BSI-Registrierungsfrist endete am 31. Juli 2026, über 10.000 Unternehmen waren zu diesem Termin noch nicht registriert. Wer im Verzug ist, holt die Registrierung umgehend nach.

Hinzu kommt der Druck aus dem Markt. Große Kunden geben ihre Anforderungen über die Lieferkette weiter, und Versicherer wie Banken fragen die Sicherheitslage zunehmend ab. Ein Vorfall trifft nicht nur die Technik, sondern die Substanz eines inhabergeführten Betriebs. Wer den Nachweis früh aufbaut, verhandelt mit Kunden und Versicherern aus einer Position der Stärke.

BETROFFENHEIT IN KÜRZE

Drei Fragen führen schnell zur Antwort. Gehört Ihr Betrieb zu einem der NIS2-Sektoren, etwa dem verarbeitenden Gewerbe? Erreichen Sie 50 Beschäftigte oder 10 Millionen Euro? Beliefern Sie Kunden, die selbst unter NIS2 fallen? Ein Ja genügt, um die Betroffenheit ernsthaft zu prüfen. Wer die Prüfung sauber dokumentiert, schafft Klarheit und schützt die Geschäftsführung im Zweifel vor Haftung. Wer die drei Fragen offen lässt, verschiebt die Entscheidung nur auf den ungünstigsten Moment, meist die nächste Kundenanfrage oder Prüfung.

Die folgenden Seiten liefern die Grundlage dafür: Branchenkontext, konkrete Risiken, die Pflichten aus dem Gesetz und eine Roadmap, die zu einem Betrieb mit schlanker IT passt. Sie zeigen zugleich, wie sich der Aufwand mit vorhandenen Strukturen klein halten lässt, statt ein zweites Projekt neben dem Kerngeschäft aufzubauen.

BETROFFEN

29.500

Unternehmen in 18 Sektoren fallen unter NIS2, viele mittelständische Betriebe darunter.

FRIST ABGELAUFEN

31.07.2026

Die verlängerte BSI-Registrierungsfrist endete am 31. Juli 2026, über 10.000 fehlten noch.

BUSSGELD

10 Mio €

Bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei besonders wichtigen Einrichtungen.

BRANCHENKONTEXT

Der Mittelstand ist digitaler, als er sich fühlt.

Auch traditionelle Betriebe steuern heute Produktion, Logistik und Vertrieb über vernetzte Systeme. Diese Digitalisierung bringt Effizienz und zugleich neue Angriffsflächen, die NIS2 in den Blick nimmt.

Ein Ransomware-Angriff legt keine Server lahm, *er stoppt die Produktion.*

GEWACHSENE IT UND VERNETZTE PRODUKTION

Ein Mittelständler steuert sein Geschäft über ERP, Warenwirtschaft und E-Mail, oft ergänzt um vernetzte Maschinen, Fertigungssteuerung und Fernwartung. Vieles ist über Jahre gewachsen, mit langlebigen Anlagen und Altsystemen, die sich nicht einfach austauschen lassen.

Diese Mischung aus Bürowelt und Produktion ist ein Effizienzgewinn und zugleich eine große Angriffsfläche. Wo IT und Maschinennetz zusammenwachsen, reicht eine offene Tür, um beide Welten zu treffen. Genau deshalb gehört die Produktion in jede Sicherheitsbetrachtung, nicht nur die Büro-IT. Wer die Produktion außen vor lässt, übersieht oft das größte Risiko. Schon ein Blick auf die Schnittstellen zwischen beiden Welten zeigt, wo die dringendsten Lücken liegen.

WARUM NIS2 DEN MITTELSTAND ERFASST

Das verarbeitende Gewerbe, Chemie, Lebensmittel, Abfallwirtschaft und weitere Branchen stehen in den Anlagen des NIS2UmsuCG. Maßgeblich sind Sektor und Größe, nicht das Selbstbild. Ein Zulieferer mit 120 Beschäftigten fühlt sich als Familienbetrieb, ist aber eine wichtige Einrichtung im Sinne des Gesetzes.

Wer formal unter der Schwelle bleibt, entkommt selten. Große Kunden reichen ihre Pflichten über die Lieferkette weiter und verlangen den Sicherheitsnachweis vertraglich. Wer den Nachweis nicht erbringt, riskiert einen Auftrag, den der Betrieb über Jahre aufgebaut hat. Die Einstufung hängt dabei nicht am Selbstbild, sondern an nachprüfbaren Zahlen zu Sektor, Beschäftigten und Umsatz.

ZULIEFERER IM FADENKREUZ

Der Mittelstand ist das Rückgrat kritischer Lieferketten. Genau das macht ihn interessant: Angreifer nutzen den kleineren, schlechter geschützten Partner als Einfallstor zum großen Kunden. Die Lieferkettensicherheit nach §30 schlägt damit direkt auf den Mittelständler durch. Der eigene Sicherheitsnachweis wird so zur Eintrittskarte in wichtige Aufträge. Wer ihn früh vorweist, verschafft sich einen Vorsprung, bevor der große Kunde ihn überhaupt einfordert.

WAS AUF DEM SPIEL STEHT

Es geht um Produktionsausfälle, Vertragsstrafen, verlorene Aufträge und um Reputation. In einem inhabergeführten Betrieb trifft ein schwerer Vorfall die Substanz, nicht nur eine Quartalszahl.

In einem Markt, in dem große Kunden Sicherheit zur Bedingung machen, ist ein sauberer Nachweis bares Geld. Er sichert Aufträge und macht aus einer Pflicht einen Vorsprung gegenüber dem Wettbewerb. In einem Familienbetrieb steht damit oft das Lebenswerk auf dem Spiel, nicht nur eine einzelne Kennzahl. Sicherheit ist hier Schutz des Lebenswerks. Wer früh vorsorgt, gibt dieses Lebenswerk gesichert an die nächste Generation weiter.

HERAUSFORDERUNGEN

Warum NIS2 im Mittelstand besonders fordert.

Die Anforderungen sind für alle gleich, die Ausgangslage im Mittelstand ist es nicht. Sechs Eigenheiten machen die Umsetzung anspruchsvoll, und für jede gibt es einen pragmatischen Umgang.

SCHLANKE IT, OFT AUSGELAGERT

Sicherheit ist im Mittelstand häufig Nebenaufgabe einer kleinen IT-Abteilung oder eines externen Dienstleisters. NIS2 verlangt aber Struktur, Dokumentation und Nachweise. Werkzeuge, die führen und Belege erzeugen, machen hier den Unterschied. So bleibt die knappe IT-Kapazität beim Kerngeschäft, statt in Formularen zu versickern. Ein klar benannter Verantwortlicher gibt dem Thema zudem ein Gesicht im Betrieb. Ein externer Dienstleister bleibt dabei eingebunden, die Verantwortung für die Nachweise bleibt aber im Haus.

GEWACHSENE ALTSYSTEME

Maschinen und Software laufen oft über viele Jahre und lassen sich nicht einfach aktualisieren. Sicherheit muss um den Bestand herum gebaut werden, mit Segmentierung und kompensierenden Maßnahmen statt mit dem Austausch alles Alten. Oft genügt es, ein Altsystem vom übrigen Netz zu trennen, statt es sofort zu ersetzen. So bleibt die Produktion verfügbar, während die Sicherheit Schritt für Schritt wächst.

IT TRIFFT OT

Produktionsnetze waren nie für das Internet gedacht. Fernwartung und Vernetzung öffnen sie trotzdem. Die Absicherung dieser Betriebstechnik ist für viele Betriebe Neuland und gehört früh auf die Agenda. Eine klare Trennung von Büro- und Produktionsnetz ist dabei der wirksamste erste Schritt. Schon ein einfaches Netzsegment vor der Fertigung verhindert, dass ein Vorfall im Büro sofort die Produktion erreicht. Wer die Übergänge kontrolliert, behält die Maschinen im Blick, ohne sie neu beschaffen zu müssen.

FACHKRÄFTEMANGEL

Security-Wissen ist knapp und teuer, und der Mittelstand konkurriert mit Konzernen um dieselben Fachkräfte. Umso wichtiger sind klare Prozesse und Partner, die Wissen gezielt zuliefern, statt eine ganze Abteilung aufzubauen. Ein verlässlicher Partner ersetzt so das teure, schwer zu findende Fachpersonal im eigenen Haus.

BEGRENZTE BUDGETS, KLARE PRIORITÄTEN

Das Prinzip der Verhältnismäßigkeit erlaubt, Maßnahmen an Größe und Risiko auszurichten. Wer mit den wirksamsten Hebeln beginnt, schützt das Wichtigste zuerst und verteilt den Rest planbar über die Zeit. Große Kunden fordern zugleich ein hohes Niveau, das sich mit klaren Prioritäten Schritt für Schritt erreichen lässt.

UNTERSCHÄTZTE BETROFFENHEIT

Das Gefühl, zu klein oder unwichtig zu sein, verzögert den Start. Dabei genügt eine dokumentierte Prüfung, um Klarheit zu schaffen und die Geschäftsführung abzusichern. Der frühe Start zahlt sich aus, weil Aufträge und Versicherungsschutz zunehmend an einen Nachweis geknüpft sind. Wer wartet, riskiert, im entscheidenden Moment ohne Nachweis dazustehen. Ein früher, schlanker Aufbau ist günstiger als die Hektik unter Zeitdruck. Schon eine knappe, dokumentierte Selbsteinschätzung nimmt dem Thema den Schrecken.

BEDROHUNGSLAGE & RISIKEN

Wo der Mittelstand konkret angreifbar ist.

Die Risiken sind selten abstrakt. Sie hängen an Maschinen, Zugängen und Menschen, die ein kleines Team kaum lückenlos überwacht. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE STOPPT DIE PRODUKTION

Der häufigste Ernstfall. Werden ERP oder Fertigungssteuerung verschlüsselt, steht der Betrieb still, Lieferungen und Umsatz fallen sofort aus. Getestete, vom Netz getrennte Backups und ein geübter Wiederanlauf entscheiden über Stunden oder Wochen. Wer den Ernstfall nie geübt hat, verliert im Angriff die wertvollste Zeit. Ein aktueller Notfallplan legt vorab fest, wer im Ernstfall was entscheidet. Ein zweiter, getrennter Datenstand verkürzt den Wiederanlauf erheblich. Die Zahlung eines Lösegelds ist dabei keine Lösung, denn sie garantiert keine Wiederherstellung und lädt neue Angriffe ein.

2 · ANGRIFF ÜBER DIE FERNWARTUNG

Offene Fernzugänge zu Maschinen und Anlagen sind ein beliebtes Einfallstor. Ohne Absicherung und Netztrennung wird der Wartungszugang zum Generalschlüssel für Büro und Produktion. Verschlüsselte Verbindungen, feste Zugriffszeiten und Protokollierung machen die Fernwartung wieder beherrschbar. Jeder Zugang gehört auf das Nötigste beschränkt und nach der Wartung wieder geschlossen. Ein Verzeichnis aller aktiven Zugänge schafft den Überblick, den ein kleines Team im Alltag schnell verliert. Ein fester Rhythmus zur Prüfung dieser Zugänge hält das Verzeichnis aktuell.

3 · ÜBER DIE LIEFERKETTE ZUM GROSSEN KUNDEN

Angreifer nehmen den Mittelständler als Weg zum OEM. Kompromittierte Zugänge und EDI-Verbindungen tragen den Angriff weiter. Genau hier setzt die Lieferkettensicherheit nach §30 an. Wer seine Zugänge zu Kundensystemen absichert, schützt sich selbst und den großen Kunden zugleich. Große Kunden prüfen diese Absicherung inzwischen aktiv und machen sie zur Bedingung für den nächsten Auftrag. Ein Betrieb, der seine Schnittstellen sauber führt, besteht solche Prüfungen ohne Hektik. So wird der Sicherheitsnachweis vom lästigen Formular zum Argument im Vertrieb.

4 · CEO-FRAUD UND PHISHING

In Betrieben mit kurzen Wegen wirken gefälschte Anweisungen der Geschäftsführung besonders gut. Ein Vier-Augen-Prinzip bei Zahlungen und regelmäßige Sensibilisierung stoppen die meisten Versuche. Eine kurze, wiederkehrende Schulung hält die Belegschaft für solche Maschen wach. Klare Freigabewege nehmen Betrügern zusätzlich die Angriffsfläche. Zahlungen sollten nie allein auf Zuruf freigegeben werden. Auch gefälschte Rechnungen und geänderte Bankverbindungen gehören zu dieser Masche und lassen sich durch einen kurzen Rückruf entlarven.

5 · DATENDIEBSTAHL UND BETRIEBSSPIONAGE

Konstruktionsdaten, Rezepturen und Kundenlisten sind wertvoll. Ihr Abfluss trifft die Wettbewerbsfähigkeit und ist zugleich ein DSGVO-Vorfall. Verschlüsselung und enge Zugriffsrechte begrenzen den Schaden. Wer weiß, wo die wertvollsten Daten liegen, kann sie zuerst und am stärksten schützen. Oft fällt der Abfluss erst spät auf, wenn Wettbewerber plötzlich mit ähnlichen Produkten am Markt sind. Eine Protokollierung der Zugriffe macht ungewöhnliche Muster früh sichtbar.

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 bei Umsatz und Bilanzsumme erreicht. Besonders wichtig ist, wer ab 250 Beschäftigte oder mehr als 50 Mio. Euro Umsatz erreicht. Maßgeblich ist die Zugehörigkeit zu einem NIS2-Sektor, etwa dem verarbeitenden Gewerbe. 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. So bleibt die Einstufung jederzeit belastbar. Im Zweifel hilft eine kurze rechtliche Einschätzung. Die Registrierung selbst ist in wenigen Schritten erledigt, die saubere Begründung der Einstufung kostet mehr Sorgfalt als Zeit.

§30 · DIE ZEHN MASSNAHMEN

Verlangt werden angemessene und wirksame technische und organisatorische Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, sichere Beschaffung, Wirksamkeitskontrolle, Schulungen, Kryptografie, Zugriffskontrolle und Multifaktor-Authentifizierung. Produktion und Betriebstechnik gehören ausdrücklich dazu. Wer bereits ein ISMS nach ISO 27001 oder ein TISAX-Label betreibt, hat den Großteil abgedeckt. NIS2 lässt sich dann als Erweiterung des Bestehenden umsetzen, 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. Ohne vorab geübten Prozess sind diese Fristen kaum zu halten. Die Uhr läuft ab Kenntnis des Vorfalls, und die erste Meldung darf zunächst unvollständig sein. Wichtiger als Vollständigkeit ist Schnelligkeit, denn die Frühwarnung soll dem BSI ein frühes Lagebild geben. Ein vorbereitetes Meldeformular spart 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 Inhaber wird Cybersicherheit damit zur Führungsaufgabe. Regelmäßige, kurze Schulungen der Leitung sind ausdrücklich Teil dieser Pflicht. Im Ernstfall ist das dokumentierte Engagement der Leitung zugleich ein Nachweis gelebter Sorgfalt. Wer als Geschäftsführer nachweisen kann, dass er sich gekümmert hat, senkt zugleich sein persönliches Haftungsrisiko.

§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: Ein Mittelständler schuldet ein Schutzniveau, das zu seiner Größe und seinem Risiko passt, nicht das eines Konzerns. 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 priorisiert nach Risiko und Frist 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 den Großteil von §30 ab. *NIS2 wird damit zur Erweiterung, nicht zum Neustart.*

1 · BETROFFENHEIT FESTSTELLEN

Sektor und Schwellenwerte prüfen, auch die Rolle als Zulieferer, und die Einstufung dokumentieren. Diese Bewertung ist die Grundlage für alles Weitere und gehört in die Unterlagen der Geschäftsführung. In Grenzfällen lohnt eine kurze rechtliche Einschätzung, bevor die weiteren Schritte starten.

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 · ASSETS UND RISIKEN ERFASSEN

Ein Inventar aufbauen, das Büro-IT und Produktion umfasst, von Servern über Maschinen bis zu Fernwartungszugängen. Risiken bewerten, Lücken sichtbar machen und nach Wirkung auf den Betrieb priorisieren. Ein gepflegtes Inventar ist danach die Grundlage jeder Wiederholung der Risikobeurteilung.

4 · MASSNAHMEN UMSETZEN

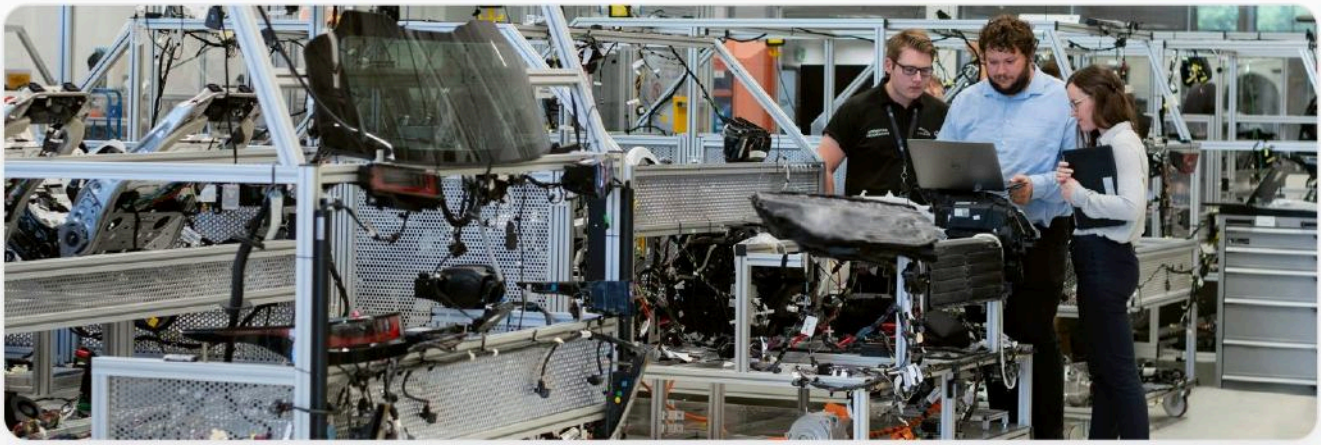
Mit den wirksamsten Hebeln beginnen: Multifaktor-Authentifizierung, Backup, Trennung von Büro- und Produktionsnetz, abgesicherte Fernwartung, Sensibilisierung und Anforderungen an Dienstleister. Jede Maßnahme so dokumentieren, dass sie im Audit Bestand hat. Vieles davon lässt sich in vorhandenen Systemen direkt aktivieren und zentral vorgeben. So wirkt jede Maßnahme sofort im ganzen Betrieb. Zentrale Vorgaben verhindern, dass jede Abteilung eigene Wege geht.

5 · MELDEPROZESS AUFBAUEN

Die 24-Stunden-Meldekette einrichten, Zuständigkeiten klären, den Notfallplan testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen. Eine kurze Übung pro Jahr zeigt, wo der Ablauf zwischen den Bereichen noch hakt. Kurze Wege im Betrieb helfen, die Fristen zu halten.

6 · LEITUNG UND DIENSTLEISTER STEUERN

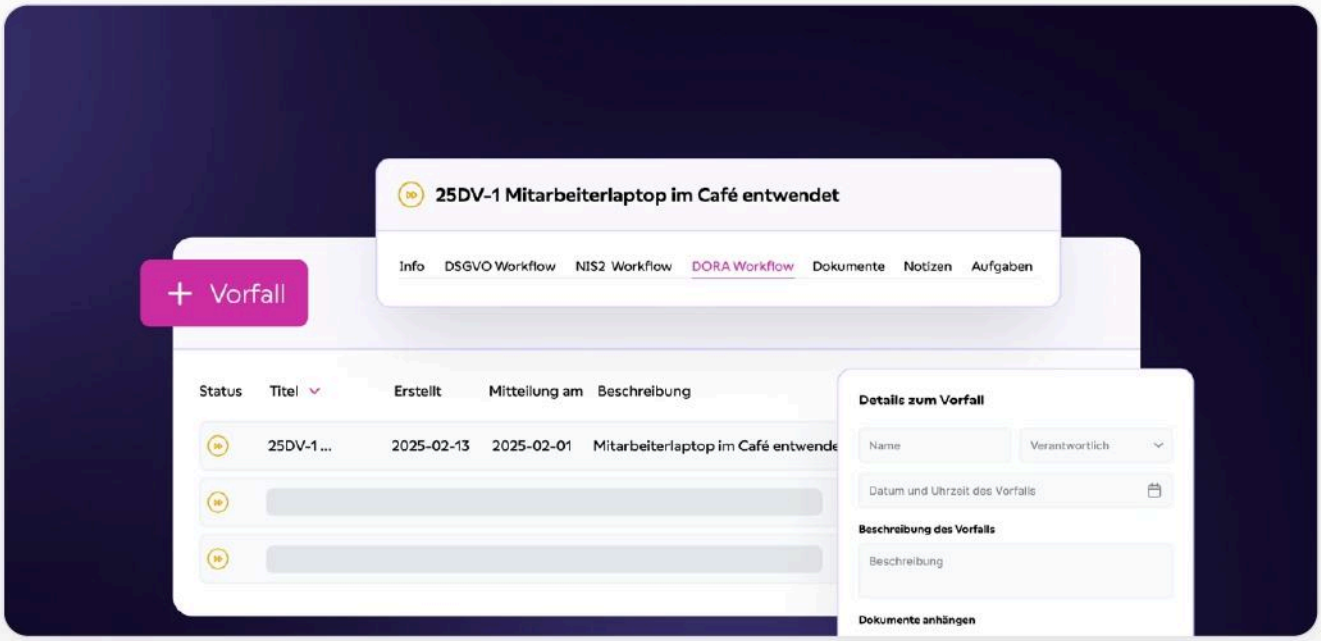
Die Geschäftsführung schulen, Billigung und Überwachung dokumentieren, den externen IT-Partner klar beauftragen und einen Audit-Trail führen. NIS2 ist kein Projekt mit Enddatum, sondern ein dauerhafter Prozess. Wer das verankert, ist zugleich reif für die ISO-27001-Zertifizierung. Der Aufwand von heute trägt so gleich mehrere Nachweise von morgen. Ein fester Jahresrhythmus hält Registrierung, Risiken und Nachweise ohne Hektik aktuell.



WIE SECJUR ES EINFACH MACHT

Vom Gesetzestext zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) bündelt die NIS2-Umsetzung an einem Ort: Risiken, Maßnahmen, Meldeprozess und Nachweise. Gerade Betriebe ohne eigene Security-Abteilung arbeiten in einer geführten Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Unternehmen berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Risiko & Maßnahmen

Geführte Risikoanalyse und ein Modul, das die zehn Maßnahmen nach §30 nachvollziehbar dokumentiert, priorisiert und für die Leitung aufbereitet.

Vorfall & Meldung

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

Lieferanten & Nachweise

Lieferantenbewertung, revisionssichere Dokumentation und voller Audit-Trail für die Aufsicht und das nächste Kundenaudit.

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 und 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 der Betrieb die wirksamsten Maßnahmen zuerst ab und verteilt den Rest planbar über die folgenden Wochen. Der Fortschritt bleibt dabei jederzeit sichtbar, für die IT ebenso wie für die Geschäftsführung.

EIN AUFBAU, MEHRERE ERGEBNISSE

Weil sich NIS2, ISO 27001 und TISAX weitgehend überschneiden, deckt das DCO mehrere Anforderungen zugleich ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass der Nachweis aktuell bleibt, ohne dass jemand Tabellen pflegt.

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

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

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

Mittelständische Betriebe, Zulieferer und familiengeführte Unternehmen erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem Mittelstand:

„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 DEM MITTELSTAND UND DER INDUSTRIE

MESSER Gases for Life · PETER KÖLLN · Nordzucker · SWT STAHLWERK THÜRINGEN · FEDDERSEN · oetinger aluminium

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 DER MITTELSTAND SECJUR WÄHLT

Der Reiz liegt in der Machbarkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die zu einem Betrieb mit schlanker IT passen. Das Team bleibt beim Kerngeschäft, die Compliance entsteht parallel.

Nachweise wachsen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass Geschäftsführung, IT und externer Dienstleister 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 wenn keine eigene Sicherheitsabteilung existiert.

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 erledigtes Gesetz, sondern ein Betrieb, der seine Risiken kennt und seine Lieferkette im Griff hat. Genau das sichert Aufträge und überzeugt große Kunden in ihren Sicherheitsprüfungen.

Weil dieselbe Struktur NIS2 und die gängigen Zertifikate gemeinsam bedient, senkt sie den Aufwand und hält den Betrieb auch nach dem nächsten Wachstumsschritt nachweisbar konform.

Ein sauberer Nachweis wirkt weit über die Aufsicht hinaus. Er verkürzt die Sicherheitsprüfungen großer Kunden, entkräftet Einwände in Ausschreibungen und verschafft einen Vorsprung gegenüber Wettbewerbern, die den Nachweis erst noch aufbauen müssen.

Und der Aufwand bleibt einmalig. Was heute für NIS2 entsteht, trägt morgen die ISO-27001-Zertifizierung, das TISAX-Label und die nächste Kundenanfrage. Sicherheit wird so zum festen Bestandteil der Art, wie der Betrieb arbeitet.

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.

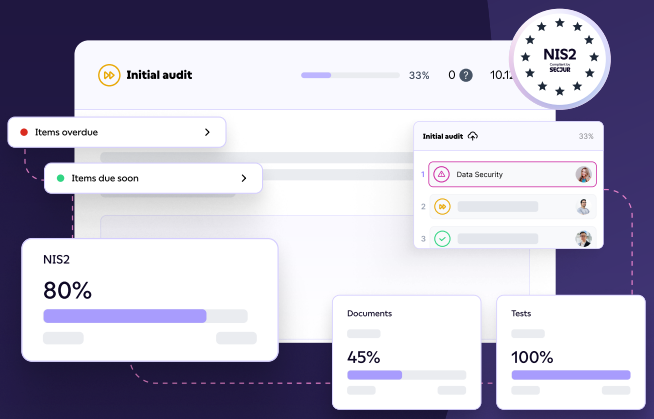
Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- 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