SECJUR

WHITEPAPER
2026

NIS2 · STARTUPS & SCALE-UPS

NIS2 trifft Startups früher, als Sie denken.

Das NIS2-Umsetzungsgesetz gilt seit Dezember 2025, ohne Übergangsfrist. Viele digitale Dienste, B2B-SaaS- und Cloud-Startups fallen früher darunter, als ihre Gründerinnen und Gründer erwarten. Dieses Whitepaper zeigt, wann ein Startup betroffen ist, wo seine größten Schwachstellen liegen und wie sich die Pflichten aus §30, §32 und §38 nachweisbar erfüllen lassen, ohne das Tempo aus der Produktentwicklung zu nehmen.

NIS2 | ISO 27001 | SOC 2 | TISAX® | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Cybersicherheit ist im Startup von Tag eins Chefsache.

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, die Pflichten gelten seit dem ersten Tag. Bundesweit fallen rund 29.500 Unternehmen in 18 Sektoren darunter, von der Energieversorgung bis zu digitalen Diensten.

Für Startups ist entscheidend, dass die Richtlinie die Schwelle deutlich nach unten verschiebt. Wer in digitalen Diensten, in der IT oder in der Cloud tätig ist und die Größenmerkmale erreicht, ist reguliert, unabhängig davon, wie fertig das Produkt ist. Die Geschäftsführung billigt die Maßnahmen, überwacht sie und haftet persönlich.

Anders als beim früheren KRITIS-Recht kommt es nicht mehr auf einzelne Schwellenwerte bei Anlagen an, sondern auf Sektor und Unternehmensgröße. Dadurch geraten viele Startups erstmals in den Anwendungsbereich, oft ohne es zu bemerken.

WARUM JETZT HANDELN

Die BSI verlängerte die Registrierungsfrist auf den 31. Juli 2026. Auch zu diesem Termin waren über 10.000 der betroffenen Unternehmen noch nicht registriert. Wer die Frist versäumt hat, ist nicht aus der Pflicht, sondern im Verzug, und sollte die Registrierung umgehend nachholen.

Startups trifft die Regulierung an einer wunden Stelle. Wachstum verschiebt die Betroffenheit laufend, jede Finanzierungsrunde und jede Einstellungswelle kann die Schwelle reißen. Zugleich geben Enterprise-Kunden ihre Anforderungen über die Lieferkette weiter und verlangen den Nachweis vertraglich.

Hinzu kommt die Aufsicht. Das BSI kann bei wichtigen Einrichtungen tätig werden, sobald Hinweise auf Mängel vorliegen, und bei besonders wichtigen auch aus eigenem Antrieb prüfen. Wer vorbereitet ist, begegnet einer solchen Prüfung gelassen.

BETROFFENHEIT IN KÜRZE

Drei Fragen führen schnell zur Antwort. Gehört Ihr Produkt zu den digitalen Diensten, zur IT oder zur digitalen Infrastruktur? Erreichen Sie 50 Beschäftigte oder 10 Mio. Euro? Beliefern Sie Kunden, die selbst unter NIS2 fallen? Ein Ja genügt, um die Betroffenheit ernsthaft zu prüfen.

Wer unsicher ist, dokumentiert die Prüfung trotzdem. Eine belastbare Einschätzung schützt die Geschäftsführung und spart Zeit, wenn ein Kunde oder die Aufsicht danach fragt.

Die folgenden Seiten liefern die Grundlage dafür: Branchenkontext, konkrete Risiken, die Pflichten aus dem Gesetz und eine Roadmap, die zum Tempo eines Startups passt.

BETROFFEN

29.500

Unternehmen in 18 Sektoren fallen unter NIS2, viele digitale Geschäftsmodelle darunter.

FRIST ABGELAUFEN

31.7.26

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

Startups sind digital von Grund auf.

Kaum ein anderer Unternehmenstyp ist so vollständig in der Cloud gebaut wie ein Tech-Startup. Genau das macht ein Startup schnell und zugleich verwundbar. NIS2 ist die Antwort auf eine Bedrohungslage, die digitale Geschäftsmodelle ins Zentrum rückt.

Wenn die Cloud-Infrastruktur steht, steht das Produkt. *Minuten entscheiden, nicht Tage.*

CLOUD-NATIVE VON ANFANG AN

Ein Startup hat selten Altsysteme, dafür einen dichten digitalen Kern: SaaS-Stack, Public Cloud bei AWS, Google Cloud oder Azure, CI/CD-Pipelines, Code-Repositories, Multi-Tenant-Datenbanken, offene APIs und zentrale Anmeldung über Single Sign-on. Das gesamte Geschäftsmodell läuft über diese Dienste, oft rund um die Uhr und für Kunden in mehreren Ländern.

Diese Architektur ist ein Effizienzgewinn und eine Angriffsfläche zugleich. Die volle Abhängigkeit von wenigen Anbietern und wenigen Zugängen bedeutet, dass ein einziger kompromittierter Schlüssel den gesamten Betrieb öffnen kann. Es gibt kein zweites, getrenntes Netz, auf das man im Ernstfall ausweicht.

WARUM NIS2 STARTUPS ERFASST

Digitale Dienste stehen in Anlage 2 des NIS2UmsuCG, IKT-Dienstleistungsmanagement und digitale Infrastruktur in Anlage 1. Maßgeblich sind Sektor und Größe, nicht das Selbstbild. Ein B2B-SaaS-Anbieter mit 60 Beschäftigten sieht sich als junges Team, ist aber eine wichtige Einrichtung im Sinne des Gesetzes.

Wer formal unter der Schwelle bleibt, entkommt selten. Kunden im Geltungsbereich reichen ihre Pflichten über die Lieferkette weiter und verlangen den Sicherheitsnachweis vertraglich. Wer regulierte Unternehmen beliefert, liefert die Compliance gleich mit, unabhängig von der eigenen Betroffenheit.

EINE REALE BEDROHUNGSLAGE

Ransomware, Kontoübernahmen und Angriffe über Software-Abhängigkeiten zählen laut BSI zu den größten Bedrohungen für die deutsche Wirtschaft. Startups sind ein lohnendes Ziel, weil ihre Daten wertvoll, ihre Teams klein und ihre Prozesse noch jung sind. Angreifer suchen gezielt nach Organisationen, in denen niemand hauptamtlich auf Sicherheit achtet. Die Zahl automatisierter Angriffe steigt, und sie treffen kleine wie große Ziele gleichermaßen.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als einen IT-Ausfall: verlorenes Kundenvertrauen, geplatzte Deals, gefährdete Finanzierungsrunden und Folgen nach der DSGVO. Ein einziger sichtbarer Vorfall kann eine Wachstumsstory ausbremsen, die über Jahre aufgebaut wurde.

In einem Markt, in dem Sicherheit zum Kaufkriterium wird, ist ein sauberer Nachweis bares Geld. Er verkürzt Vendor-Assessments, überzeugt in der Due Diligence und macht aus Compliance ein Verkaufsargument statt einer Last.

HERAUSFORDERUNGEN

Warum NIS2 im Startup besonders fordert.

Die Anforderungen sind für alle Sektoren gleich, der Alltag eines Startups ist es nicht. Sechs Eigenheiten machen die Umsetzung anspruchsvoller als in einem etablierten Unternehmen, und für jede gibt es einen pragmatischen Umgang.

KEINE EIGENE SECURITY-FUNKTION

In vielen Startups kümmert sich der CTO oder eine Gründerin nebenbei um Sicherheit. NIS2 verlangt aber Struktur, Dokumentation und Wirksamkeitskontrolle, nicht die Heldentaten Einzelner. Werkzeuge, die führen und Nachweise erzeugen, machen hier den Unterschied und nehmen dem kleinen Team die Last der reinen Handarbeit ab. So bleibt die knappe Entwicklungszeit beim Produkt, statt in Tabellen zu versickern.

GESCHWINDIGKEIT VOR PROZESS

Startups leben von Tempo. Features gehen live, bevor Richtlinien geschrieben sind, und Nachweise entstehen selten von selbst. NIS2 verlangt Belegbarkeit, also die dokumentierte Spur hinter jeder Sicherheitsentscheidung. Der Trick liegt darin, diese Spur direkt im Arbeitsalltag entstehen zu lassen, statt sie vor jedem Audit nachzuziehen. Gut gewählte Standardprozesse bremsen die Entwicklung nicht, sie geben ihr einen verlässlichen Rahmen.

WACHSTUM REISST DIE SCHWELLEN

Die Betroffenheit ist kein fester Zustand. Was heute nicht greift, kann nach der nächsten Finanzierungsrunde und einer Einstellungswelle gelten. Wer die Prüfung früh dokumentiert, erspart sich später Hektik unter Zeitdruck und muss die Grundlagen nicht mitten in der Skalierung nachrüsten. Ein früh aufgesetztes ISMS wächst mit, ohne dass jemand von vorn beginnt.

VOLLE CLOUD-ABHÄNGIGKEIT

Das Prinzip der geteilten Verantwortung wird oft missverstanden. Der Cloud-Anbieter sichert die Infrastruktur, nicht Ihre Konfiguration, Ihre Zugänge und Ihre Daten. Genau diese Übergabepunkte, von falsch gesetzten Rechten bis zu offenen Speicher-Buckets, verdienen in der Risikoanalyse besondere Aufmerksamkeit. Die meisten Cloud-Vorfälle gehen nicht auf den Anbieter zurück, sondern auf eine Fehlkonfiguration im eigenen Konto.

BEGRENZTE MITTEL

Startups arbeiten mit knappen Kassen, das Budget für Sicherheit ist selten üppig. Hier hilft das Prinzip der Verhältnismäßigkeit: Maßnahmen müssen zur Größe und zum Risiko passen, nicht zum Konzernmaßstab. Zugleich fordern Enterprise-Kunden ein hohes Schutzniveau, oft schon vor dem ersten Vertrag. Der Ausweg liegt darin, zuerst die wenigen Maßnahmen mit der größten Wirkung umzusetzen und den Rest geplant nachzuziehen.

VERTEILTE TEAMS UND EIGENE GERÄTE

Viele Startups arbeiten remote und mit privaten Geräten. Homeoffice-Netze, ungepatchte Laptops und schnell eingeführte Tools erweitern die Angriffsfläche über das Büro hinaus. Klare Regeln für Geräte, Zugänge und genutzte Dienste halten diese Fläche beherrschbar, ohne die Flexibilität zu nehmen, die ein junges Team braucht.

BEDROHUNGSLAGE & RISIKEN

Wo Startups konkret angreifbar sind.

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

1 · KONTOÜBERNAHME UND GELEAKTE ZUGANGSDATEN

Der häufigste Ernstfall. API-Schlüssel und Tokens landen versehentlich im Code-Repository, und ohne Multifaktor-Authentifizierung genügt ein geleaktes Passwort. Ein einziger Zugang öffnet dann den Vollzugriff auf die Produktivumgebung. Multifaktor-Authentifizierung und ein sauberes Secrets-Management schließen diese Tür fast vollständig. Auch inaktive Konten ehemaliger Teammitglieder und großzügig vergebene Admin-Rechte gehören regelmäßig auf den Prüfstand.

2 · RANSOMWARE LEGT DAS PRODUKT LAHM

Wird die Infrastruktur verschlüsselt oder das Cloud-Konto gesperrt, steht der SaaS-Betrieb sofort still. Anders als ein Ausfall im Backoffice trifft das die Kunden unmittelbar und kostet auf der Stelle Vertrauen. Getestete Backups entscheiden über Stunden oder Tage, und nur ein geübter Wiederanlauf hält vertragliche Verfügbarkeitszusagen ein. Ein Offline- oder unveränderliches Backup ist dabei der Unterschied zwischen einem schlechten Tag und einem existenzbedrohenden Vorfall.

3 · ANGRIFF ÜBER DIE LIEFERKETTE

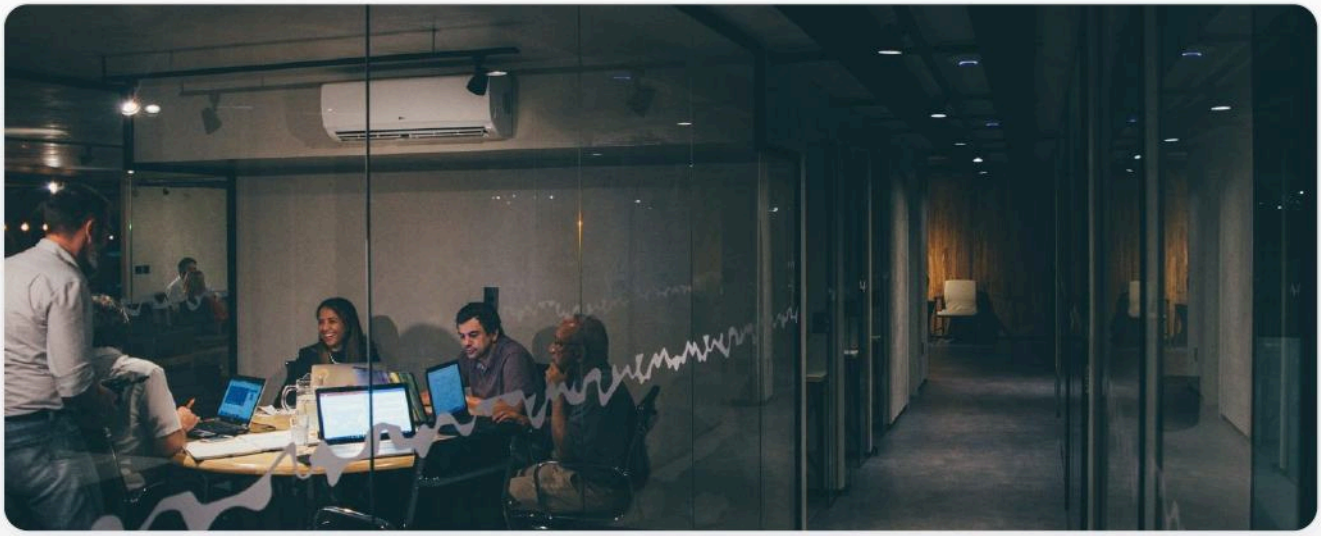
Startups bauen auf offenen Bibliotheken. Ein manipuliertes npm- oder pip-Paket oder eine kompromittierte CI/CD-Pipeline schleust Schadcode direkt in das Produkt und damit zu jedem Kunden. Genau hier setzt die Lieferkettensicherheit nach §30 an, von der Prüfung der Abhängigkeiten bis zur Absicherung der Build-Umgebung. Eine aktuelle Übersicht der eingesetzten Komponenten macht sichtbar, welche neue Schwachstelle das eigene Produkt gerade betrifft.

4 · DATENABFLUSS AUS DER DATENBANK

Kundendaten mehrerer Mandanten liegen dicht beieinander. Ein Fehler in der Zugriffslogik oder ein erbeuteter Datenbankzugang legt Daten quer über Kunden hinweg offen. Das ist zugleich ein DSGVO-Vorfall und ein Deal-Killer im Vertrieb. Verschlüsselung, strikte Mandantentrennung und enge Rechte begrenzen den Schaden, bevor er entsteht. Regelmäßige Prüfungen der Zugriffsrechte verhindern, dass alte Berechtigungen unbemerkt bestehen bleiben.

5 · PHISHING UND SOCIAL ENGINEERING

Im kleinen Team fehlt die Distanz. Gefälschte Rechnungen, vorgetäuschte Anweisungen der Geschäftsführung und gezielte Phishing-Mails wirken, wo niemand für Sicherheit zuständig ist. Ohne Sensibilisierung ist dieser Weg schwer zu schließen. Kurze, regelmäßige Schulungen und eine klare Meldekultur senken das Risiko spürbar. Eine einfache Regel für Zahlungsfreigaben im Vier-Augen-Prinzip stoppt zusätzlich die meisten Betrugsversuche.



REGULATORISCHE PFLICHTEN

Was das Gesetz konkret verlangt.

Fünf Paragraphen bilden den Kern, den jedes betroffene Startup 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. Bei Beteiligungen kann die Betroffenheit über die Gruppe entstehen, was gerade für VC-finanzierte Startups zählt. Die Registrierung läuft über das Unternehmenskonto und das BSI-Portal, die Einstufung nimmt das Unternehmen selbst vor. Sie sollte schriftlich begründet und bei jeder Änderung der Größe oder des Geschäftsmodells aktualisiert werden.

§30 · DIE ZEHN MASSNAHMEN

Verlangt werden angemessene und wirksame technische und organisatorische Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, sichere Entwicklung, Wirksamkeitskontrolle, Schulungen, Kryptografie, Zugriffskontrolle und Multifaktor-Authentifizierung. Wer bereits ein ISMS nach ISO 27001 oder ein SOC-2-Programm betreibt, hat den Großteil davon abgedeckt. Der Grundsatz der Verhältnismäßigkeit erlaubt, Tiefe und Umfang der Maßnahmen an Größe und Risiko des Startups auszurichten.

§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, nicht ab dem Moment, in dem alle Fakten vorliegen. Die erste Meldung darf unvollständig sein, entscheidend ist, dass sie fristgerecht beim BSI eingeht.

§38 · LEITUNG HAFTET PERSÖNLICH

Die Geschäftsführung muss die Maßnahmen billigen, ihre Umsetzung überwachen und sich schulen lassen. Die Verantwortung ist nicht delegierbar, die Haftung persönlich. Für Gründerinnen und Gründer wird Cybersicherheit damit zur Führungsaufgabe, die sich nicht an die IT allein abgeben lässt. Regelmäßige, kurze Schulungen der Leitung sind ausdrücklich Teil dieser Pflicht und im Ernstfall ein Nachweis gelebter Sorgfalt.

§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 junges Team schuldet nicht das Schutzniveau eines Konzerns, sondern eines, das zu seiner Größe und seinem Risiko passt. Neben dem Bußgeld wiegt oft der Reputationsschaden schwerer, gerade wenn Kunden und Investoren mitlesen.

UMSETZUNG IN DER PRAXIS

In sechs Schritten nachweisbar 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, 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, damit die Einstufung auch vor der Aufsicht Bestand hat.

2 · BEIM BSI REGISTRIEREN

Unternehmenskonto anlegen, im BSI-Portal registrieren, Kontaktstellen benennen. Wer die Frist vom 31. Juli 2026 versäumt hat, holt diesen Schritt umgehend nach, um Bußgelder zu vermeiden. Die benannte Stelle ist zugleich der Draht zum BSI, wenn ein Vorfall gemeldet werden muss. Ohne diese Registrierung bleibt das Unternehmen für die Aufsicht unsichtbar, was im Ernstfall negativ auffällt.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von Cloud-Konten über Repositories und CI/CD bis zu den Datenflüssen und Secrets. Bedrohungen bewerten, Lücken sichtbar machen und nach Wirkung auf das Produkt priorisieren. Eine saubere Analyse trennt das Wichtige vom Nebensächlichen und macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

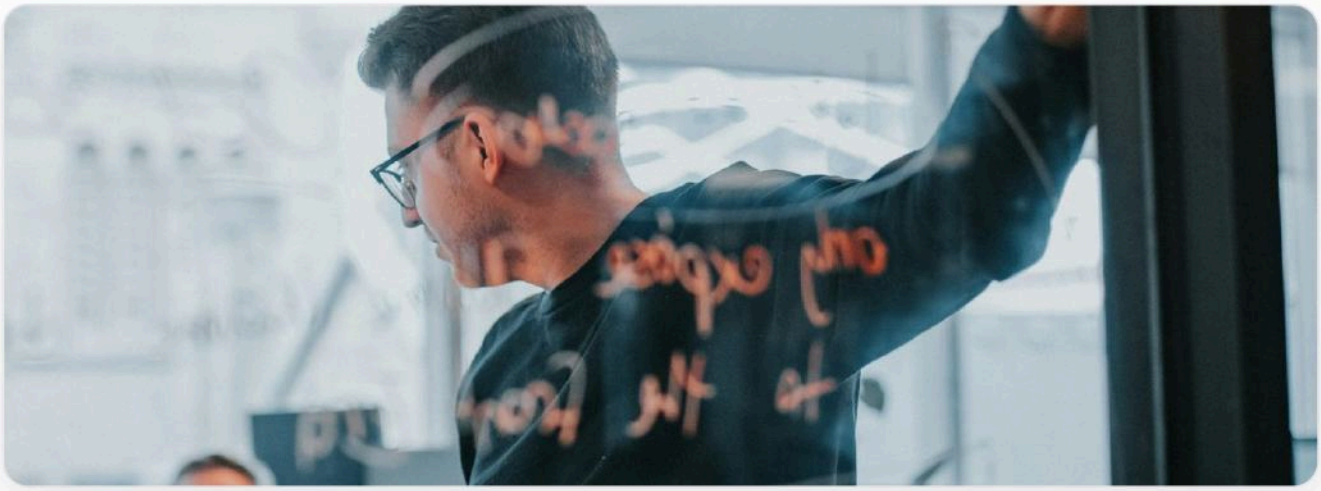
Mit den wirksamsten Hebeln beginnen: Multifaktor-Authentifizierung, Backup, Zugriffskontrolle, sauberes Secrets-Management und Anforderungen an Dienstleister. Jede Maßnahme so dokumentieren, dass sie im Audit Bestand hat. Vieles davon lässt sich in den vorhandenen Cloud- und Entwicklungswerkzeugen direkt aktivieren. Externe Dienstleister werden über klare Anforderungen und, wo nötig, vertragliche Zusicherungen eingebunden.

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 zuverlässig, wo der Prozess noch hakt.

6 · LEITUNG EINBINDEN UND NACHWEISEN

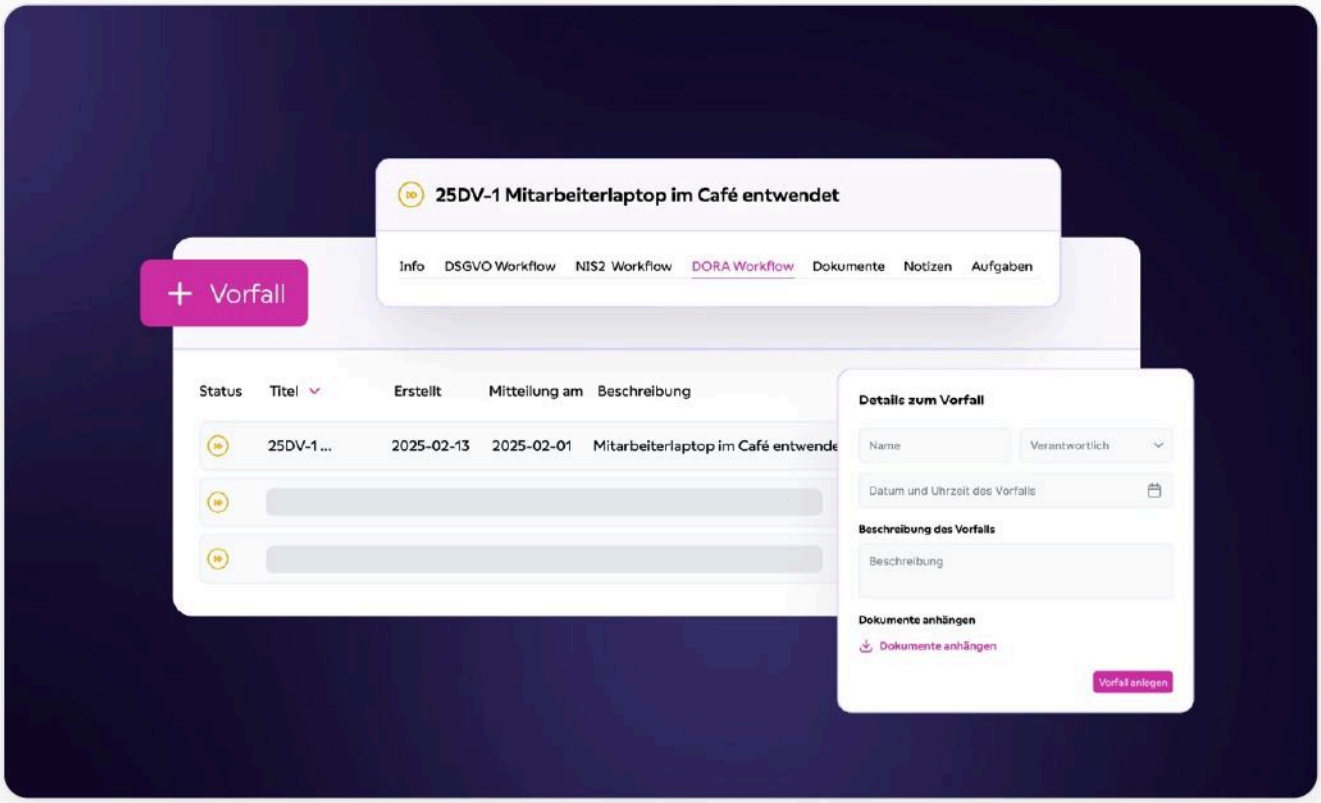
Geschäftsführung schulen, Billigung und Überwachung dokumentieren, einen Audit-Trail führen. NIS2 ist kein Projekt mit Enddatum, sondern ein dauerhafter Prozess mit regelmäßiger Wirksamkeitskontrolle. Wer das früh verankert, besteht auch das nächste Kundenaudit ohne Sonderaufwand.



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. Statt einem Dutzend Tools und externer Beratung arbeiten Sie in einer 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 Sie 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 Produktentwicklung stehen bleibt.

EIN AUFBAU, MEHRERE ERGEBNISSE

Weil sich NIS2, ISO 27001 und SOC 2 weitgehend überschneiden, deckt das DCO mehrere Anforderungen zugleich ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, von Microsoft 365 bis GitHub, sodass der Nachweis aktuell bleibt, ohne dass jemand Tabellen pflegt.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

Startups, Scale-ups und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Startup-Welt:

„Eine *starke europäische Lösung* für relevante Compliance-Standards wie DORA, DSGVO und SOC 2."

Moritz Poewe
Chief Operating Officer,
Vestlane

REFERENZEN AUS DER STARTUP- UND TECH-WELT

1KOMMA5° yfood deepset Tomorrow Masterplan.com vestlane

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 STARTUPS SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die zum kleinen Team passen statt zum Konzern. Das Team bleibt beim Produkt, die Compliance entsteht parallel.

Nachweise wachsen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass Entwicklung, Betrieb und Geschäftsführung an einer Quelle arbeiten statt an verstreuten Tabellen.

Die Plattform denkt in Startup-Realität. Sie priorisiert die Maßnahmen mit der größten Wirkung, verteilt Aufgaben klar im Team und macht auf einen Blick sichtbar, was noch offen ist. So bleibt die Umsetzung planbar, auch wenn parallel ein Release ansteht oder das Team gerade wächst.

Wo Fachwissen fehlt, schalten sich Expertinnen und Experten gezielt zu, statt ein dauerhaftes Beratungsmandat zu verlangen. Das hält die Kosten niedrig und die Kontrolle im Haus. Gerade in einer frühen Phase, in der jede Stunde und jeder Euro zählt, entscheidet dieser Zuschnitt zwischen Aufschieben und Erledigen.

MEHR ALS EINE PFLICHTÜBUNG

Am Ende steht nicht nur ein erledigtes Gesetz, sondern ein Startup, das seine Risiken kennt und seine Lieferkette im Griff hat. Genau das gewinnt Enterprise-Deals und beruhigt Investoren in der Due Diligence.

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

Ein sauberer Nachweis wirkt weit über die Aufsicht hinaus. Er verkürzt die Sicherheitsprüfungen potenzieller Kunden, entkräftet Einwände im Vertrieb und verschafft einen Vorsprung gegenüber Wettbewerbern, die den Nachweis erst noch aufbauen müssen. Aus einer Pflicht wird ein Argument, das Umsatz schützt und öffnet.

Und der Aufwand bleibt einmalig. Was heute für NIS2 entsteht, trägt morgen die ISO-27001-Zertifizierung, den SOC-2-Bericht und die nächste Kundenanfrage. Sicherheit wird so vom Projekt zum festen Bestandteil der Art, wie das Unternehmen arbeitet, und wächst mit jeder Runde mit.

SECJUR

Mit SECJUR zu 100 % NIS2-Compliance

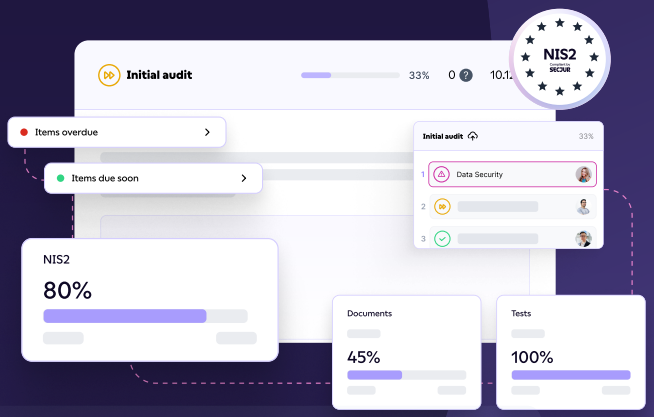
Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

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 zu Informationssicherheitszertifizierungen:

“Dank Kundenvertrauen auf die Financial-Times-1000-Liste”

René Schlüß
Founder & Managing Director, reanmo

reanmo

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

Masterplan.com · 1KOMMA5° · Tomorrow · deepset · yfood · vestlane

www.secjur.com