SECJUR

WHITEPAPER
2026

NIS2 · SCALE-UPS & WACHSTUM

NIS2 im Scale-up: keine Frage des Ob, nur des Wie.

Wer schnell wächst, hat die Schwellen des NIS2-Umsetzungsgesetzes meist längst überschritten, oft strenger, als die Geschäftsführung annimmt. Das Gesetz gilt seit Dezember 2025 ohne Übergangsfrist. Dieses Whitepaper zeigt, warum Scale-ups sicher betroffen sind, wo eine gewachsene Systemlandschaft angreifbar wird und wie sich die Pflichten aus §30, §32 und §38 skalierbar erfüllen lassen, ohne das Wachstum auszubremsen.

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

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Im Scale-up ist Sicherheit zur Führungsfrage 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 zu digitalen Diensten.

Für Scale-ups ist die Lage eindeutig. Wer die 50-Beschäftigten- oder 10-Millionen-Schwelle überschritten hat, ist wichtige Einrichtung, und viele nähern sich mit 250 Beschäftigten oder 50 Millionen Euro Umsatz der Stufe besonders wichtig, die deutlich strenger beaufsichtigt wird. Die Betroffenheit ist gesetzt, oft folgenreicher als gedacht. Anders als das frühere KRITIS-Recht knüpft NIS2 nicht mehr an einzelne Anlagen an, sondern an Sektor und Größe, und erfasst damit deutlich mehr Unternehmen. Für wachsende Unternehmen heißt das: Was gestern noch außerhalb des Anwendungsbereichs lag, fällt mit der nächsten Wachstumsstufe schnell darunter.

WARUM JETZT HANDELN

Die BSI-Registrierungsfrist endete am 31. Juli 2026, über 10.000 Unternehmen waren zu diesem Termin noch nicht registriert. Besonders wichtige Einrichtungen werden proaktiv geprüft, nicht erst nach einem Vorfall. Wer im Verzug ist, holt die Registrierung umgehend nach.

Hinzu kommt der Marktdruck. Enterprise- und Public-Sector-Kunden verlangen Nachweise über die Lieferkette, und in Finanzierungsrunden, Zukäufen und beim Exit wird die Sicherheitslage Teil der Due Diligence. Ein Vorfall trifft dann nicht nur den Betrieb, sondern auch die Bewertung. Wer die Sicherheitslage früh ordnet, verwandelt eine Pflicht in einen Vorteil bei Kunden und Kapitalgebern. Frühes Handeln senkt zugleich das Risiko teurer Nacharbeit, wenn ein Audit oder eine Kundenanfrage kurzfristig einen Nachweis verlangt.

BETROFFENHEIT IN KÜRZE

Drei Fragen führen schnell zur Antwort. Gehört Ihr Geschäft zu den digitalen Diensten, zur IT oder zur digitalen Infrastruktur? Erreichen Sie 50 Beschäftigte oder 10 Millionen Euro? Beliefern Sie Kunden, die selbst unter NIS2 fallen? Für die meisten Scale-ups lautet die Antwort mehrfach ja. Schon eine der drei Fragen genügt, um die Betroffenheit ernsthaft zu prüfen. Im Zweifel lohnt sich eine dokumentierte Einschätzung, die vor der Aufsicht und im Vertrieb Bestand hat.

Offen ist meist nur die Einstufung als wichtige oder besonders wichtige Einrichtung und die Frage, welche Konzerngesellschaften erfasst sind. Die folgenden Seiten liefern die Grundlage: Kontext, Risiken, Pflichten und eine skalierbare Roadmap.

BETROFFEN

29.500

Unternehmen in 18 Sektoren fallen unter NIS2, viele wachsende Tech-Unternehmen 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

Scale-ups sind über sich hinausgewachsen.

Das Geschäft ist digital, aber die Organisation hat sich in kurzer Zeit vervielfacht. Systeme, Teams und Lieferketten sind gewachsen, die Sicherheitsorganisation oft nicht im selben Tempo. Genau diese Lücke adressiert NIS2.

Was im Startup ein Tool war, ist im Scale-up eine ganze Landschaft. *Komplexität wird zum Risiko.*

VOM TOOL ZUR LANDSCHAFT

Mit dem Wachstum vervielfachen sich die Systeme: mehrere Produkte und Umgebungen, oft Multi-Cloud über mehrere AWS-, Google- oder Azure-Konten, Dutzende SaaS-Dienste, mehrere Teams mit eigenen Stacks und häufig mehrere Standorte oder Gesellschaften.

Diese Landschaft ist über Monate organisch entstanden, selten nach einem zentralen Plan. Ein vollständiger Überblick über Assets, Zugänge und Datenflüsse fehlt vielen, und die Schatten-IT einzelner Abteilungen wächst leise mit. Ohne ein zentrales Inventar weiß am Ende niemand mehr genau, welche Systeme laufen und wer worauf Zugriff hat.

WARUM NIS2 JETZT SICHER GREIFT

Die Schwellen von 50 Beschäftigten oder 10 Millionen Euro sind im Scale-up längst überschritten, viele bewegen sich Richtung 250 Beschäftigte oder 50 Millionen Euro und damit in die Stufe besonders wichtig. Digitale Dienste und IKT stehen ausdrücklich im Anwendungsbereich.

Nach Zukäufen entsteht Betroffenheit zudem über die Gruppe, und internationale Kundschaft zieht grenzüberschreitende Pflichten nach sich. Wer regulierte Unternehmen beliefert, liefert den Sicherheitsnachweis ohnehin mit. Wer sich zu klein rechnet, erlebt die Betroffenheit oft erst, wenn ein großer Kunde den Nachweis vertraglich einfordert.

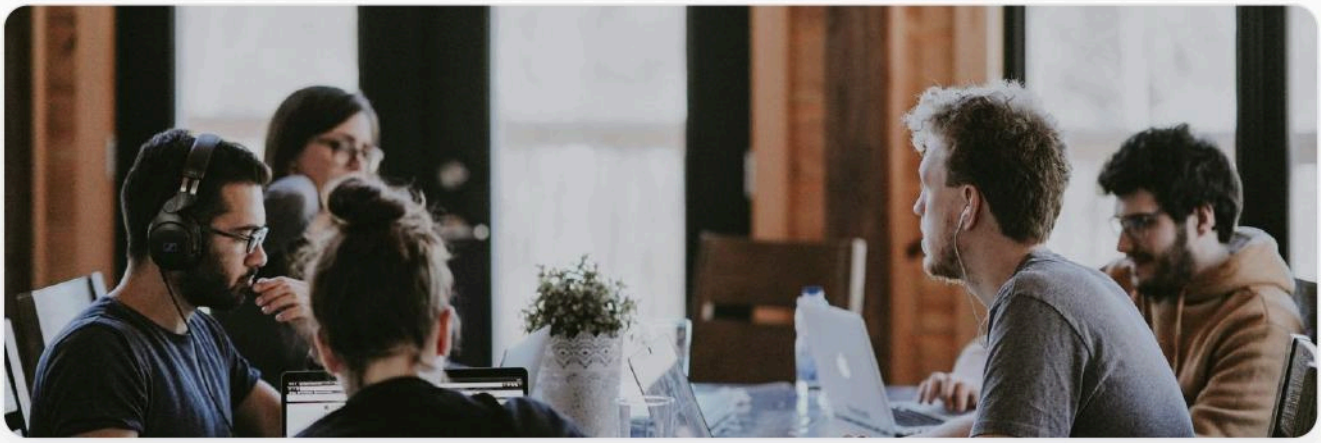
EIN ATTRAKTIVERES ZIEL

Mit Umsatz, Datenmenge und Sichtbarkeit steigt die Attraktivität für Angreifer. Ein Scale-up verwaltet mehr Kundendaten, hat mehr zu verlieren und ist in der Presse präsenter als ein junges Team. Genau darauf zielen professionelle Kampagnen. Zugleich zieht die öffentliche Sichtbarkeit Erpressungsversuche und gezieltes Social Engineering an.

WAS AUF DEM SPIEL STEHT

Es geht um Enterprise-Verträge, Ausschreibungen und die Bewertung in der nächsten Runde. Ein sichtbarer Vorfall bremst nicht nur den Betrieb, sondern auch Vertrieb, Finanzierung und einen möglichen Exit.

In einem Markt, in dem Sicherheit zum Vergabekriterium wird, ist ein sauberer Nachweis bares Geld. Er verkürzt Prüfungen, überzeugt in der Due Diligence und wird zum Verkaufsargument statt zur Last. So finanziert sich der Aufwand über gewonnene Deals und eine reibungslosere Finanzierung von selbst.



HERAUSFORDERUNGEN

Warum NIS2 im Scale-up besonders fordert.

Die Anforderungen sind für alle gleich, die Wachstumsdynamik eines Scale-ups ist es nicht. Sechs Eigenheiten machen die Umsetzung anspruchsvoll, und für jede gibt es einen pragmatischen Umgang.

GOVERNANCE HINKT DEM WACHSTUM HINTERHER

Prozesse sind in der Hochwachstumsphase entstanden, schnell und pragmatisch. Was fehlt, sind dokumentierte Verantwortlichkeiten, eine gelebte Sicherheitsleitlinie und der Nachweis dahinter. NIS2 verlangt genau diese Struktur, nicht die Heldentaten Einzelner. Der erste Schritt ist meist, Rollen und Zuständigkeiten schriftlich festzuhalten, damit im Ernstfall klar ist, wer entscheidet. Ein benannter Verantwortlicher für Informationssicherheit gibt dem Thema ein Gesicht, auch wenn die Rolle anfangs nur einen Teil der Arbeitszeit ausmacht.

ZERSPLITTERTE SYSTEMLANDSCHAFT

Mehrere Clouds, Konten und Tools sind ohne zentralen Überblick gewachsen. Ein vollständiges Asset-Inventar ist die Grundlage jeder Risikoanalyse und im Scale-up oft die erste echte Fleißarbeit, die sich aber sofort auszahlt. Ist die Landschaft einmal erfasst, lassen sich Risiken und Maßnahmen zum ersten Mal verlässlich priorisieren. Cloud-native Werkzeuge, die Konten automatisch inventarisieren, nehmen dem Team einen Großteil der Handarbeit ab.

ZUGRIFFS-WILDWUCHS

Schnelles Einstellen und Offboarding hinterlässt breite Rechte, verwaiste Konten und zu viele Administratoren. Regelmäßige Zugriffsprüfungen und eine zentrale Identitätsverwaltung bringen die Kontrolle zurück. Ein sauberes Onboarding und Offboarding sorgt dafür, dass Rechte mit der Rolle entstehen und mit ihr wieder enden. Rollenbasierte Rechte und ein zentrales Single Sign-on machen aus vielen Einzelentscheidungen ein nachvollziehbares System.

KOMPLEXE LIEFERKETTE

Mit der Größe wächst das Netz aus Subdienstleistern, von denen manche selbst reguliert sind. Die Lieferkettensicherheit nach §30 skaliert mit und verlangt Bewertung und Nachweise über viele Partner hinweg. Eine risikobasierte Einstufung der Anbieter hält den Aufwand beherrschbar, statt jeden Partner gleich tief zu prüfen. Standardisierte Fragebögen und wiederverwendbare Nachweise halten die Prüfung auch bei Dutzenden Anbietern effizient.

MEHRERE ENTITÄTEN UND LÄNDER

Nach Zukäufen und Expansion entstehen Gruppenstrukturen mit grenzüberschreitenden Meldewegen und uneinheitlichen Standards. Betroffenheit und Pflichten müssen je Gesellschaft geklärt und dann zusammengeführt werden. Ein gemeinsamer Rahmen mit lokalen Ergänzungen verhindert, dass jede Einheit ihr eigenes Sicherheitsniveau erfindet. Eine Muttergesellschaft gibt den Rahmen vor, während die Töchter nur ihre lokalen Besonderheiten ergänzen.

SICHERHEIT SKALIERT NICHT VON ALLEIN

Ein kleines Sicherheitsteam betreut eine große, verteilte Organisation. Ohne Werkzeuge, die führen und Nachweise automatisch erzeugen, wächst der Aufwand schneller als das Team. Struktur schlägt hier Einsatz. Automatisierte Nachweise und wiederverwendbare Vorlagen entlasten das Team genau dort, wo es sonst manuell nacharbeiten müsste. So wächst das Schutzniveau mit der Organisation mit, ohne dass parallel ein großes Sicherheitsteam aufgebaut werden muss.

BEDROHUNGSLAGE & RISIKEN

Wo Scale-ups konkret angreifbar sind.

Die Risiken hängen an einer gewachsenen Landschaft und an vielen Zugängen, die ein kleines Team kaum lückenlos überwacht. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · KOMPROMITTIERTE ZUGÄNGE UND RECHTE-WILDWUCHS

Der häufigste Ernstfall. Zu breite Rechte, geteilte Administratorzugänge und verwaiste Konten öffnen einem einzigen erbeuteten Login viele Systeme auf einmal. Multifaktor-Authentifizierung, zentrale Identitäten und regelmäßige Zugriffsprüfungen schließen diese Tür weitgehend. Auch privilegierte Zugänge von Dienstleistern gehören dabei auf den Prüfstand. Ein zeitlich begrenzter, protokollierter Zugriff für Wartungsfälle ersetzt dauerhafte Admin-Rechte, die niemand mehr überblickt.

2 · RANSOMWARE TRIFFT MEHRERE UMGEBUNGEN

Bei mehreren Produkten und Konten ist die Angriffsfläche größer, und ein Vorfall skaliert mit: Verschlüsselung oder eine gesperrte Cloud legen gleich mehrere Kunden lahm. Getestete, unveränderliche Backups und ein geübter Wiederanlauf entscheiden über Stunden oder Tage. Ein regelmäßig geprobtes Wiederanlaufszenario ist der Unterschied zwischen einem kontrollierten Vorfall und einem Kontrollverlust. Regelmäßige Restore-Tests stellen sicher, dass die Sicherung im Ernstfall auch wirklich funktioniert.

3 · LIEFERKETTEN- UND DEPENDENCY-ANGRIFFE

Mehr Anbieter und mehr Open-Source-Abhängigkeiten über verschiedene Teams vergrößern die Angriffsfläche. Ein manipuliertes Paket oder eine kompromittierte CI/CD-Pipeline verteilt Schadcode über die ganze Organisation. Genau hier setzt §30 an. Eine Übersicht der eingesetzten Komponenten und ihrer Versionen macht sichtbar, welche neue Schwachstelle die Organisation gerade betrifft. Automatisierte Warnungen bei neuen Schwachstellen verkürzen die Zeit zwischen Bekanntwerden und Reaktion deutlich.

4 · DATENABFLUSS ÜBER GEWACHSENE SYSTEME

Mehr Kundendaten, mehr Schnittstellen und unklare Datenflüsse erhöhen das Risiko, dass Daten quer über Systeme und Mandanten abfließen. Das ist zugleich ein DSGVO-Vorfall und eine Gefahr für laufende Verträge. Verschlüsselung, klare Mandantentrennung und dokumentierte Datenflüsse begrenzen den Schaden, bevor er entsteht. Ein aktuelles Verzeichnis der Verarbeitungstätigkeiten hilft, im Ernstfall schnell zu wissen, welche Daten betroffen sind.

5 · FEHLKONFIGURATION UND INSIDER BEI HOHEM TEMPO

Viele Änderungen in kurzer Zeit begünstigen Fehlkonfigurationen in der Multi-Cloud, und hohe Fluktuation erhöht das Insider-Risiko. Klare Prozesse, Vier-Augen-Prinzip und Protokollierung halten beides beherrschbar. Automatisierte Prüfungen der Cloud-Konfiguration fangen viele Fehler ab, bevor sie in Produktion gehen. Infrastruktur als Code mit festen Prüfregeln sorgt dafür, dass sichere Konfigurationen zur Norm werden statt zur Ausnahme.

REGULATORISCHE PFLICHTEN

Was das Gesetz konkret verlangt.

Fünf Paragraphen bilden den Kern, den jedes betroffene Scale-up 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, mit deutlich strengerer, proaktiver Aufsicht. Für viele Scale-ups ist diese Stufe realistisch. Bei Beteiligungen entsteht die Betroffenheit über die Gruppe, die Registrierung läuft je Gesellschaft über das Unternehmenskonto und das BSI-Portal. Die Einstufung sollte schriftlich begründet und bei jeder Änderung von Größe oder Struktur 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 abgedeckt und muss ihn nur über Teams und Entitäten ausrollen. Der Grundsatz der Verhältnismäßigkeit erlaubt, Tiefe und Umfang an Größe und Risiko der jeweiligen Gesellschaft 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. Über mehrere Gesellschaften und Länder hinweg braucht es dafür einen klar geregelten, geübten Ablauf. Die Uhr läuft ab Kenntnis des Vorfalls, und die erste Meldung darf unvollständig sein, solange sie fristgerecht 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, in einer Gruppe für jede Geschäftsführung ihrer Gesellschaft. Regelmäßige, kurze Schulungen der Leitung sind ausdrücklich Teil der 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. Die Höhe richtet sich nach Größe und Risiko, und der Reputationsschaden wiegt gerade in einer Wachstumsphase oft schwerer. Ein dokumentierter, gelebter Prozess ist zugleich die beste Verteidigung, falls die Aufsicht prüft.

UMSETZUNG IN DER PRAXIS

In sechs Schritten skalierbar 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 UND EINSTUFUNG KLÄREN

Sektor und Schwellenwerte je Gesellschaft prüfen, wichtige oder besonders wichtige Einstufung festlegen und dokumentieren. Diese Bewertung ist die Grundlage für alles Weitere und gehört in die Unterlagen jeder betroffenen Geschäftsführung. In Grenzfällen lohnt eine kurze rechtliche Einschätzung, damit die Einstufung auch vor der Aufsicht Bestand hat.

2 · BEIM BSI REGISTRIEREN

Unternehmenskonto anlegen, jede betroffene Gesellschaft im BSI-Portal registrieren, Kontaktstellen benennen. Wer die Frist versäumt hat, holt den Schritt umgehend nach, um Bußgelder zu vermeiden. Die benannten Kontaktstellen sind zugleich der Draht zum BSI, wenn ein Vorfall gemeldet werden muss.

3 · ASSETS UND RISIKEN ERFASSEN

Ein zentrales Inventar über die ganze Landschaft aufbauen, von Cloud-Konten über Repositories bis zu Datenflüssen und Lieferanten. Risiken bewerten, Lücken sichtbar machen und nach Wirkung priorisieren. Ein zentrales, gepflegtes Inventar ist danach die Grundlage für jede Wiederholung der Risikobeurteilung.

4 · MASSNAHMEN AUSROLLEN

Mit den wirksamsten Hebeln beginnen: zentrale Identitäten und Multifaktor-Authentifizierung, Backup, Zugriffsprüfungen, Lieferantenmanagement und Secrets-Management, einheitlich über Teams und Entitäten. Jede Maßnahme so dokumentieren, dass sie im Audit Bestand hat. Vieles davon lässt sich in den vorhandenen Cloud- und Identitätswerkzeugen direkt aktivieren und zentral erzwingen.

5 · MELDEPROZESS KONZERNWEIT AUFBAUEN

Eine 24-Stunden-Meldekette über alle Gesellschaften einrichten, Zuständigkeiten klären, den Notfallplan testen. Nur ein geübter, einheitlicher Ablauf hält die Fristen auch grenzüberschreitend. Eine kurze Übung pro Jahr zeigt zuverlässig, wo der Ablauf zwischen den Gesellschaften noch hakt.

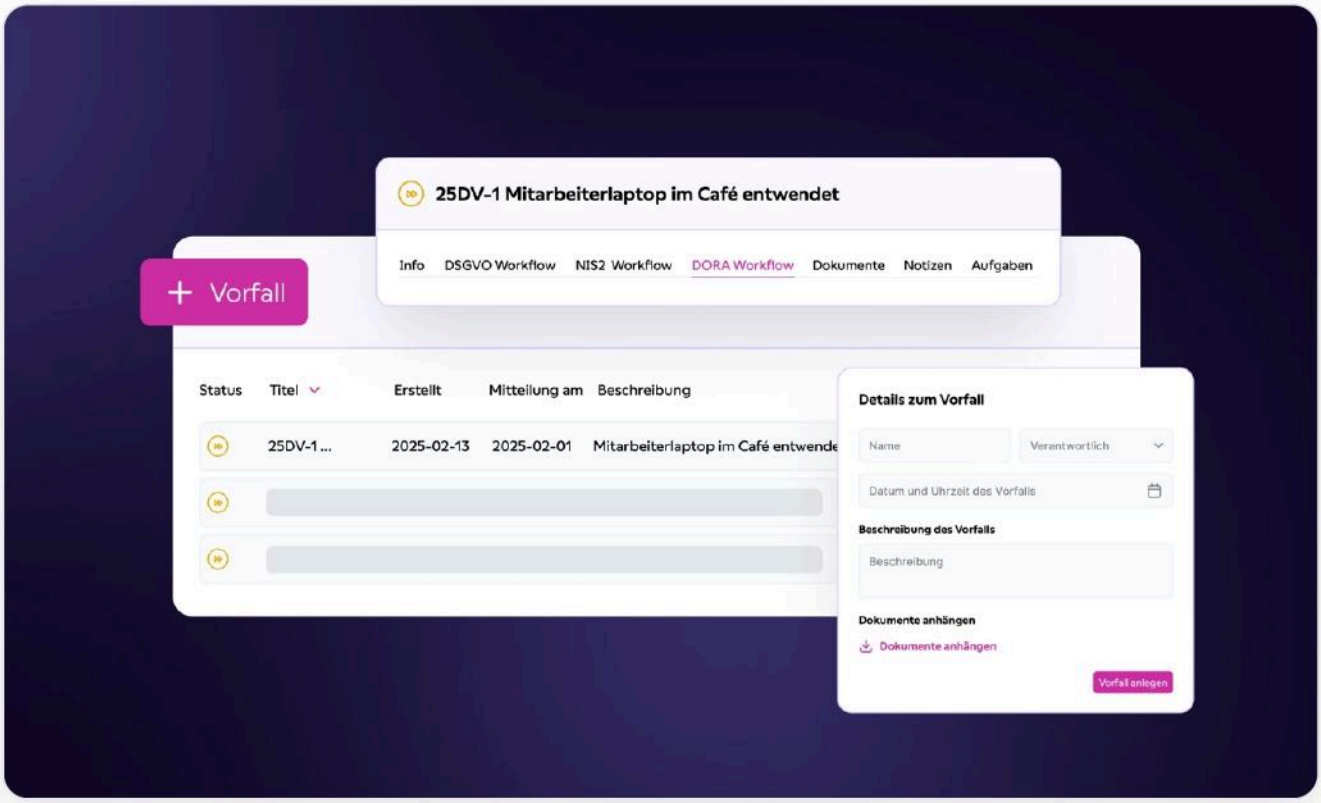
6 · LEITUNG EINBINDEN UND NACHWEISEN

Geschäftsführungen schulen, Billigung und Überwachung dokumentieren, einen Audit-Trail führen. Wer das verankert, ist zugleich reif für die ISO-27001-Zertifizierung und besteht das nächste Kundenaudit ohne Sonderaufwand. NIS2 wird so vom Projekt mit Enddatum zu einem dauerhaften Prozess mit regelmäßiger Wirksamkeitskontrolle.

WIE SECJUR ES EINFACH MACHT

Vom Gesetzestext zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) bündelt die NIS2-Umsetzung an einem Ort, über Teams und Gesellschaften hinweg: 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 über die ganze Landschaft 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 je Gesellschaft 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 das Wachstum 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 über alle Teams aktuell bleibt, ohne dass jemand Tabellen pflegt.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen arbeiten mit SECJUR.

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

„Dank Kundenvertrauen auf die *Financial-Times-1000-Liste.*"

René Schlüß
Founder & Managing Director, reanmo

REFERENZEN AUS DER SCALE-UP- UND TECH-WELT

1KOMMA5° · yfood · deepset · Tomorrow · Masterplan.com · AllDent Zahnzentrum

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 SCALE-UPS SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die zur wachsenden Organisation passen. Die Teams bleiben 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 über alle Gesellschaften an einer Quelle arbeiten statt an verstreuten Tabellen.

Die Plattform ist auf Komplexität ausgelegt. Sie bündelt mehrere Standorte, Entitäten und Frameworks, priorisiert die Maßnahmen mit der größten Wirkung und macht auf einen Blick sichtbar, wo etwas offen ist. So bleibt die Umsetzung auch bei hohem Tempo planbar.

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 mehrere Vorhaben gleichzeitig laufen.

MEHR ALS EINE PFLICHTÜBUNG

Am Ende steht nicht nur ein erledigtes Gesetz, sondern eine Organisation, die ihre Risiken kennt und ihre 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 Unternehmen 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, den SOC-2-Bericht und die nächste Kundenanfrage. Sicherheit wird so vom Projekt zum festen Bestandteil der Art, wie das Unternehmen arbeitet.

SECJUR

Mit SECJUR zu 100 % NIS2-Compliance

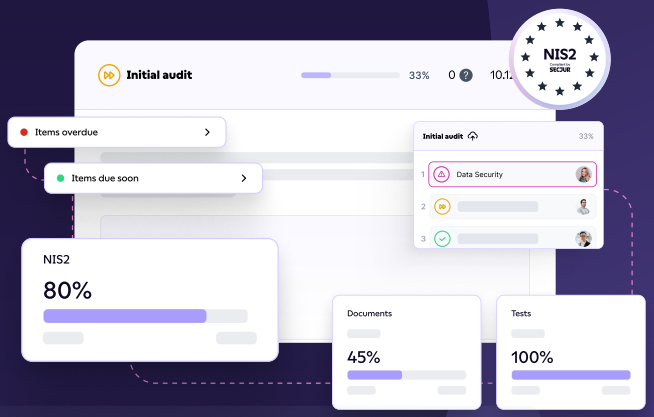
Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

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 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