



NIS2 · SOFTWARE, IT-CONSULTING & MANAGED SERVICES

# NIS2 für IT-Dienstleister: **Ihr Zugang ist Ihr Risiko.**

Software-Häuser, IT-Berater und Managed-Service-Provider arbeiten täglich in den Systemen und Daten ihrer Kunden. Genau dieser privilegierte Zugang macht sie zum attraktiven Ziel und für den Gesetzgeber relevant. Das NIS2-Umsetzungsgesetz gilt seit Dezember 2025 ohne Übergangsfrist. Viele IT-Dienstleister fallen direkt darunter, alle übrigen über die Lieferkette ihrer regulierten Kunden. Dieses Whitepaper zeigt, wann NIS2 greift, wo der Zugang zum Risiko wird und wie sich die Pflichten aus §30, §32 und §38 auf einer starken Technikbasis erfüllen lassen.

MANAGEMENT SUMMARY

# Für IT-Dienstleister ist Sicherheit die Geschäftsgrundlage.

## 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.

Für IT-Dienstleister ist die Betroffenheit besonders direkt. Managed-Service-Provider und Managed-Security-Provider sind in NIS2 als eigener Sektor ausdrücklich genannt und fallen ab 50 Beschäftigten oder 10 Millionen Euro direkt darunter. Anbieter von Cloud-, Rechenzentrums- und DNS-Diensten zählen zur digitalen Infrastruktur. Wer nicht direkt erfasst ist, wird über die Lieferkette regulierter Kunden gebunden. Als Auftragsverarbeiter und Sub-Dienstleister geben diese Kunden ihre eigenen Pflichten aus DSGVO und NIS2 vertraglich weiter. Wer in die Lieferkette eines regulierten Auftraggebers gehört, muss liefern, was dieser nachweisen muss.

## WARUM JETZT HANDELN

Die BSI-Registrierungsfrist endete am 31. Juli 2026, über 10.000 Unternehmen waren zu diesem Termin

noch nicht registriert. Wer direkt betroffen und im Verzug ist, holt die Registrierung umgehend nach.

Hinzu kommt der Druck aus dem Markt. Ausschreibungen und Sicherheitsfragebögen verlangen den Nachweis, und ein einziger Angriff über einen Dienstleister trifft gleich viele seiner Kunden. Genau diesen Multiplikator nimmt NIS2 in den Blick.

## BETROFFENHEIT IN KÜRZE

Drei Fragen führen schnell zur Antwort. Erbringen Sie Managed Services, Sicherheits- oder Cloud-Dienste und erreichen 50 Beschäftigte oder 10 Millionen Euro? Beliefern Sie Kunden, die selbst unter NIS2 fallen? Verarbeiten Sie in deren Auftrag Produktiv- und Personendaten? Ein Ja genügt, um die Betroffenheit ernsthaft zu prüfen. Wer die Prüfung sauber dokumentiert, schafft Klarheit und schützt die Geschäftsführung im Zweifel vor Haftung.

Die folgenden Seiten liefern die Grundlage dafür: Branchenkontext, konkrete Risiken, die Pflichten aus dem Gesetz und eine Roadmap, die die starke Technikbasis von IT-Dienstleistern nutzt, statt bei null zu beginnen.

## BETROFFEN

**29.500**

Unternehmen in 18 Sektoren fallen unter NIS2, IT-Dienstleister mit großem Anteil.

## FRIST ABGELAUFEN

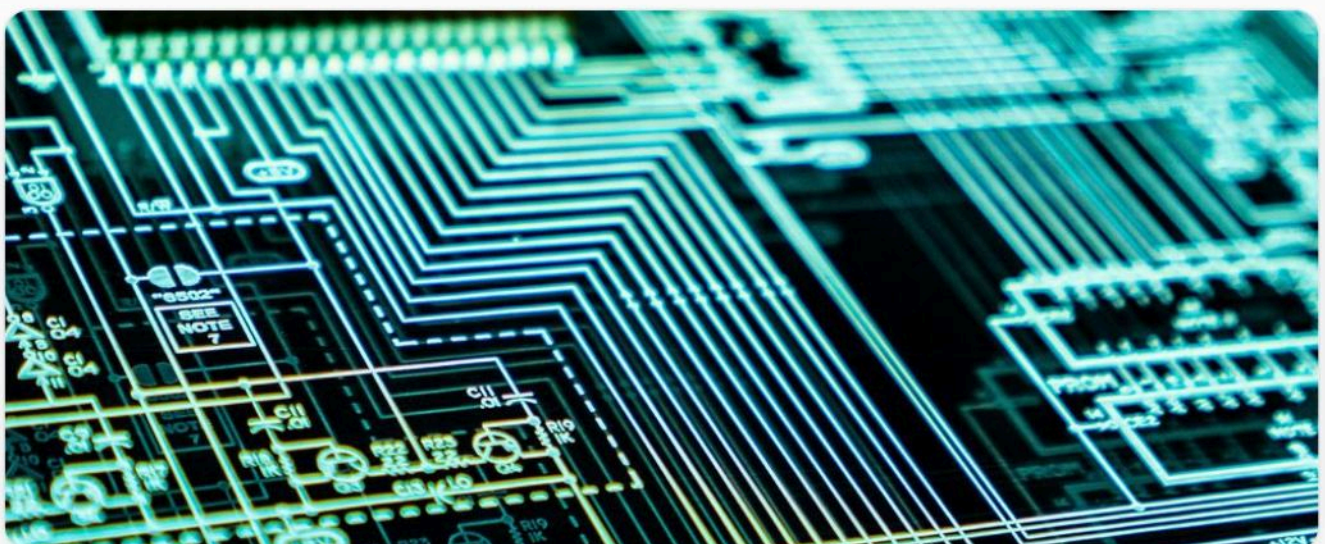
**31.07.2026**

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.



# Wer fremde Systeme betreut, steht im Fokus von NIS2.

Software-Häuser, IT-Berater und Managed-Service-Provider sitzen an einer besonders sensiblen Stelle: Sie haben Zugang zu allem. Genau deshalb prüfen Auftraggeber sie strenger, und genau deshalb nimmt NIS2 die Branche doppelt in die Pflicht.

## Ein IT-Dienstleister verkauft Vertrauen. *NIS2 macht es zur Pflicht.*

### PRIVILEGIERTER ZUGANG ZU ALLEM

Managed-Service-Provider verwalten die Infrastruktur ihrer Kunden, Software-Häuser verarbeiten deren Produktivdaten, Berater bekommen Administratorrechte für die Projektdauer. Kein anderer Lieferant kommt den Kronjuwelen eines Unternehmens so nah.

Dieser Zugang ist das Geschäftsmodell und das Risiko zugleich. Auftraggeber wissen das und verlangen Gewissheit, dass der Dienstleister den Zugang sauber verwaltet, protokolliert und absichert. NIS2 hebt genau diese Erwartung auf eine gesetzliche Grundlage. Was bisher Kür im Vertrieb war, wird damit zur nachprüfbaren Pflicht.

### DIREKT BETROFFEN ODER ÜBER DIE LIEFERKETTE

Managed-Service-Provider und Managed-Security-Provider stehen als eigener Sektor im NIS2UmsuCG, Cloud- und Rechenzentrumsdienste zählen zur digitalen Infrastruktur. Diese Dienstleister fallen ab 50 Beschäftigten oder 10 Millionen Euro direkt unter das Gesetz.

Wer nicht direkt erfasst ist, entkommt selten. Über DSGVO-Auftragsverarbeitung und die Lieferkettenpflichten nach §30 reichen regulierte Auftraggeber ihre Anforderungen vertraglich weiter. Wer den Nachweis nicht erbringt, riskiert einen

Auftrag, den er über Jahre aufgebaut hat. Die Einstufung hängt dabei nicht am Selbstbild, sondern an Leistungsangebot, Beschäftigtenzahl und Umsatz.

### DER MULTIPLIKATOR IM FADENKREUZ

Ein IT-Dienstleister ist ein attraktives Ziel, weil ein einziger Angriff über ihn gleich viele seiner Kunden trifft. Kompromittierte Zugänge oder manipulierte Software-Updates tragen den Schaden in die Netze der gesamten Kundenbasis. Genau diese Supply-Chain-Wirkung ist der Kern dessen, was NIS2 verhindern will. Ein einziger gut platzierter Angriff kann Dutzende Kundenumgebungen zugleich treffen.

### WAS AUF DEM SPIEL STEHT

Für einen IT-Dienstleister ist Reputation alles. Ein Vorfall, der über ihn zu seinen Kunden durchschlägt, zerstört Vertrauen bei vielen auf einmal und ist im engen Markt kaum wiedergutzumachen.

In einem Markt, in dem Auftraggeber Sicherheit zur Bedingung machen, ist ein sauberer Nachweis bares Geld. Er sichert Aufträge und macht aus einer Pflicht einen Vorsprung im Vertrieb. Sicherheit ist hier kein Kostenposten, sondern die Lizenz zum Geschäft. Wer den Nachweis früh vorweist, verschafft sich einen Vorsprung, bevor der große Kunde ihn überhaupt einfordert.



## HERAUSFORDERUNGEN

# Warum NIS2 IT-Dienstleister **besonders fordert.**

Die Anforderungen gelten unabhängig von der Branche. Bei IT-Dienstleistern liegt die Hürde selten in der Technik, sondern an anderer Stelle. Sechs Eigenheiten machen die Umsetzung speziell, und für jede gibt es einen pragmatischen Umgang.

### TECHNIK STARK, STRUKTUR DÜNN

IT-Dienstleister beherrschen Firewalls, Verschlüsselung und Monitoring oft besser als ihre Kunden. Was fehlt, ist die Struktur drumherum: dokumentierte Richtlinien, nachvollziehbare Prozesse und der Nachweis der Wirksamkeit. Genau diese Formalisierung des ohnehin Vorhandenen ist die eigentliche Arbeit. Werkzeuge, die führen und Belege erzeugen, machen hier den Unterschied. So bleibt die knappe Zeit beim Kundenprojekt, statt in Formularen zu versickern.

### MANDANTENTRENNUNG

Wer viele Kunden gleichzeitig betreut, muss deren Daten und Zugänge sauber trennen. Eine Vermischung ist nicht nur ein Sicherheits-, sondern auch ein Vertrauensproblem. NIS2 verlangt wirksame Zugriffskontrolle und getrennte Umgebungen, gerade im Multi-Mandanten-Betrieb. Eine klare Trennung schützt zugleich vor dem Dominoeffekt, wenn ein Kunde getroffen wird.

### PRIVILEGIERTE ZUGÄNGE IM GRIFF

Administrator- und Fernzugänge zu Kundensystemen sind das größte Pfund und das größte Risiko. Sie müssen streng vergeben, protokolliert und nach Projektende wieder entzogen werden. Privileged-Access-Management und

lückenlose Protokollierung stehen für IT-Dienstleister besonders im Fokus. Ein automatisiertes Entzugsverfahren nach Projektende verhindert, dass Berechtigungen liegen bleiben.

### TEMPO UND VERTEILTE TEAMS

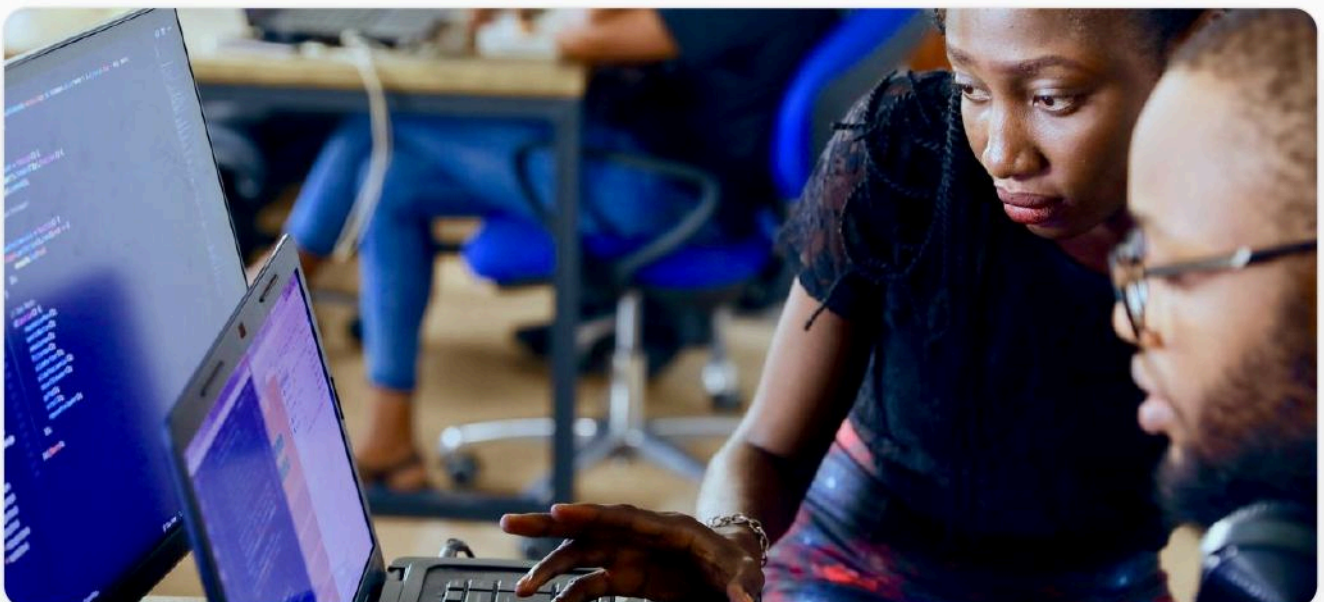
Projektgeschäft, Remote-Arbeit und schnelle Teamwechsel erschweren ein sauberes On- und Offboarding. Werden Zugänge nicht konsequent entzogen, sammeln sich verwaiste Berechtigungen an. Geregelter Prozesse halten diese Lücke klein und lassen sich weitgehend automatisieren.

### EIGENE LIEFERKETTE AUS SAAS

IT-Dienstleister nutzen selbst zahlreiche Cloud- und SaaS-Dienste, über die wiederum Kundendaten laufen. Jeder ist ein Sub-Dienstleister im Sinne der Lieferkettenpflicht. Ohne Übersicht über diese Kette bleibt die Risikoanalyse unvollständig, und die eigene Betroffenheit lässt sich nicht sauber begründen.

### NACHWEIS UNTER ZEITDRUCK

Kunden fragen den Sicherheitsstand oft kurzfristig ab, mitten im Projektgeschäft. Wer den Nachweis erst dann aufbaut, verliert wertvolle Zeit. Ein früher, gelebter Prozess liefert die Antwort auf Knopfdruck und macht aus dem Fragebogen ein Verkaufsargument statt einer Belastung.



## Wo IT-Dienstleister konkret angreifbar sind.

Die Risiken hängen am privilegierten Zugang und an der Rolle als Multiplikator: Wer einen IT-Dienstleister trifft, trifft viele seiner Kunden. Fünf Szenarien tauchen in der Praxis immer wieder auf.

### 1 · SUPPLY-CHAIN-ANGRIFF ÜBER DEN DIENSTLEISTER

Der Albtraum der Branche. Angreifer kompromittieren einen IT-Dienstleister, um über dessen Zugänge oder Software-Updates gleich in die Netze vieler Kunden zu gelangen. Der Schaden vervielfacht sich und trifft das Vertrauen ins Mark. Strenge Zugriffskontrolle, getrennte Umgebungen und sichere Entwicklung sind hier zentral. Genau dieses Szenario begründet die Lieferkettenpflicht nach §30. Getrennte Test- und Produktivumgebungen begrenzen, wie weit ein Angreifer überhaupt kommt.

### 2 · MISSBRAUCH PRIVILEGIERTER ZUGÄNGE

Administrator- und Fernzugänge sind das lohnendste Ziel. Werden Zugangsdaten abgegriffen oder nach Projektende nicht entzogen, steht Angreifern die Kundenumgebung offen. Privileged-Access-Management, Mehrfaktor-Anmeldung und lückenlose Protokollierung schließen diese Tür. Ein fester Rhythmus zur Prüfung aktiver Zugänge hält die Übersicht aktuell.

### 3 · DATENABFLUSS AUS KUNDENPROJEKTEN

IT-Dienstleister verarbeiten fremde Produktiv- und Personendaten. Ein Abfluss ist zugleich ein DSGVO-Vorfall des Kunden und ein Vertrauensbruch.

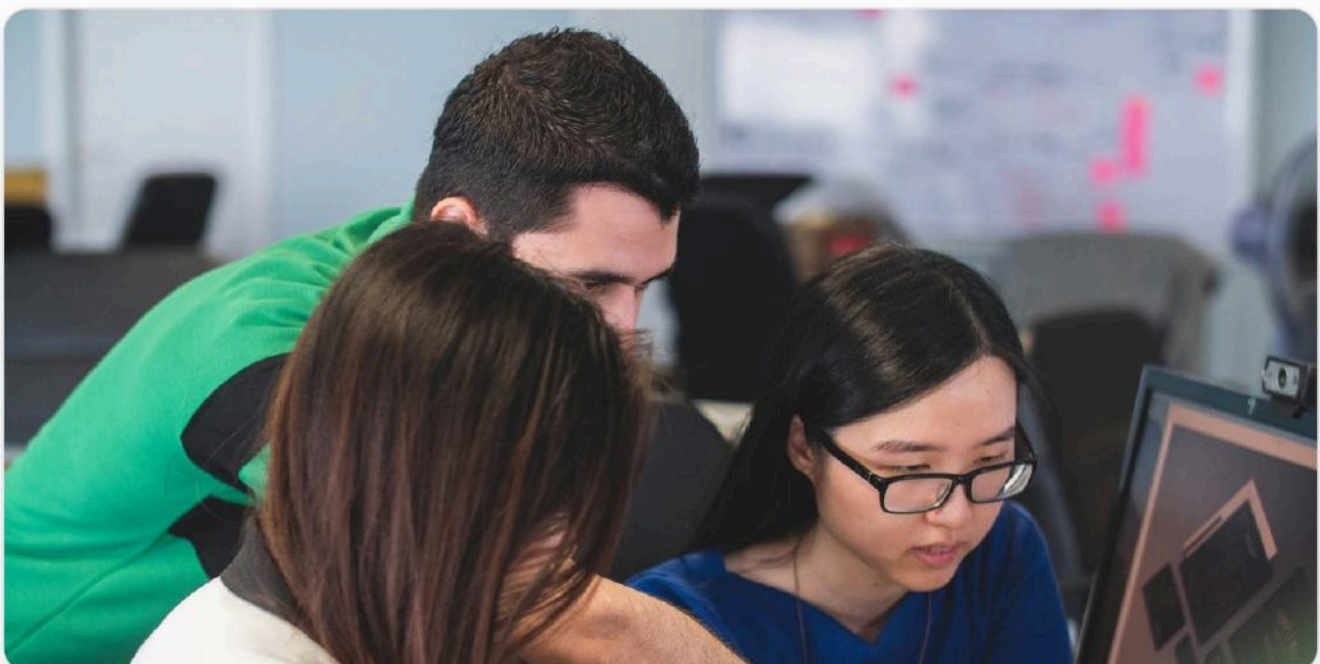
Verschlüsselung, saubere Mandantentrennung und enge Zugriffsrechte begrenzen den Schaden. Wer weiß, wo die sensibelsten Daten liegen, kann sie zuerst und am stärksten schützen. Eine Protokollierung der Zugriffe macht ungewöhnliche Muster früh sichtbar.

### 4 · SCHWACHSTELLEN IM EIGENEN CODE

Wer Software entwickelt, liefert mit jeder Schwachstelle auch ein Einfallstor an seine Kunden aus. Sichere Entwicklung, Code-Prüfung und getrennte Test- und Produktivumgebungen sind für Software-Häuser keine Kür, sondern Pflicht. NIS2 rechnet die Sicherheit des eigenen Produkts der Betriebssicherheit zu. Ein fester Prüfschritt vor jedem Release hält diese Tür geschlossen.

### 5 · PHISHING UND RANSOMWARE

Auch IT-Profis werden Opfer von Phishing, und ein Ransomware-Vorfall im eigenen Haus legt nicht nur den Dienstleister, sondern auch die betreuten Kunden lahm. Awareness, Mehrfaktor-Anmeldung und getestete, vom Netz getrennte Backups gehören zu den wirksamsten Maßnahmen. Ein geübter Wiederanlauf entscheidet über Stunden oder Wochen. Wer den Ernstfall nie geübt hat, verliert im Angriff die wertvollste Zeit.



## REGULATORISCHE PFLICHTEN

# Was das Gesetz konkret verlangt.

Fünf Paragraphen bilden den Kern, den jeder betroffene Dienstleister 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. Managed-Service-Provider, Sicherheits- und Cloud-Dienste sind als Sektor ausdrücklich benannt. 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 Leistungsangebot aktualisiert werden. Im Zweifel hilft eine kurze rechtliche Einschätzung.

## §30 · DIE ZEHN MASSNAHMEN

Verlangt werden angemessene technische und organisatorische Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, sichere Beschaffung und Entwicklung, Wirksamkeitskontrolle, Schulungen, Kryptografie, Zugriffskontrolle und Multifaktor-Authentifizierung. Wer bereits ein ISMS nach ISO 27001 oder ein SOC-2-Testat 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

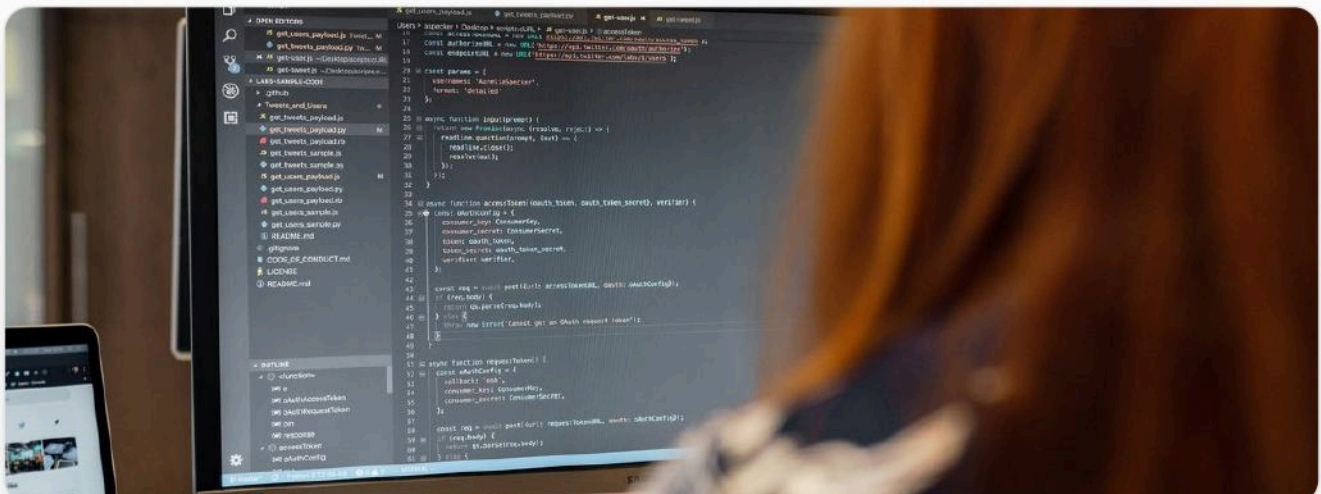
binnen 72 Stunden, Abschlussbericht binnen eines Monats. Für Dienstleister zählt zusätzlich die Information betroffener Kunden. Ohne vorab geübten Prozess sind diese Fristen kaum zu halten, und die Uhr läuft ab Kenntnis des Vorfalls. Ein vorbereitetes Meldeformular und klare Zuständigkeiten sparen im 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. Gerade in kleinen, technikgetriebenen Teams wird Cybersicherheit damit zur Führungsaufgabe. Das dokumentierte Engagement der Leitung ist im Ernstfall zugleich ein Nachweis gelebter Sorgfalt. Wer als Geschäftsführer belegen kann, dass er sich gekümmert hat, senkt zugleich sein persönliches Haftungsrisiko.

## §65 · SANKTIONEN UND VERHÄLTNISSÄSSIGKEIT

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.



# In sechs Schritten mit Augenmaß NIS2-konform.

Die Umsetzung lässt sich planen. Diese Reihenfolge baut auf der starken Technikbasis von IT-Dienstleistern auf und priorisiert nach Risiko und Frist. 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 Auftragsverarbeiter und 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

Wer direkt betroffen ist, legt das Unternehmenskonto an, registriert sich im BSI-Portal und benennt Kontaktstellen. 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, von Kundenzugängen über die eigene Entwicklungs- und Betriebsumgebung bis zu den genutzten SaaS-Diensten. Risiken rund um Zugänge und Kundendaten bewerten, Lücken sichtbar machen und nach Wirkung priorisieren. Eine gute Analyse macht den Aufwand planbar.

## 4 · MASSNAHMEN UMSETZEN

Mit den wirksamsten Hebeln beginnen: Privileged-Access-Management, Mandantentrennung,

Multifaktor-Authentifizierung, sichere Entwicklung, abgesicherte Fernwartung und Lieferantenanforderungen. Die Technik ist oft da, der Nachweis fehlt. Jede Maßnahme so dokumentieren, dass sie im Audit Bestand hat. Vieles lässt sich in vorhandenen Systemen direkt aktivieren. So wirkt jede Maßnahme sofort im ganzen Betrieb.

## 5 · MELDEPROZESS AUFBAUEN

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

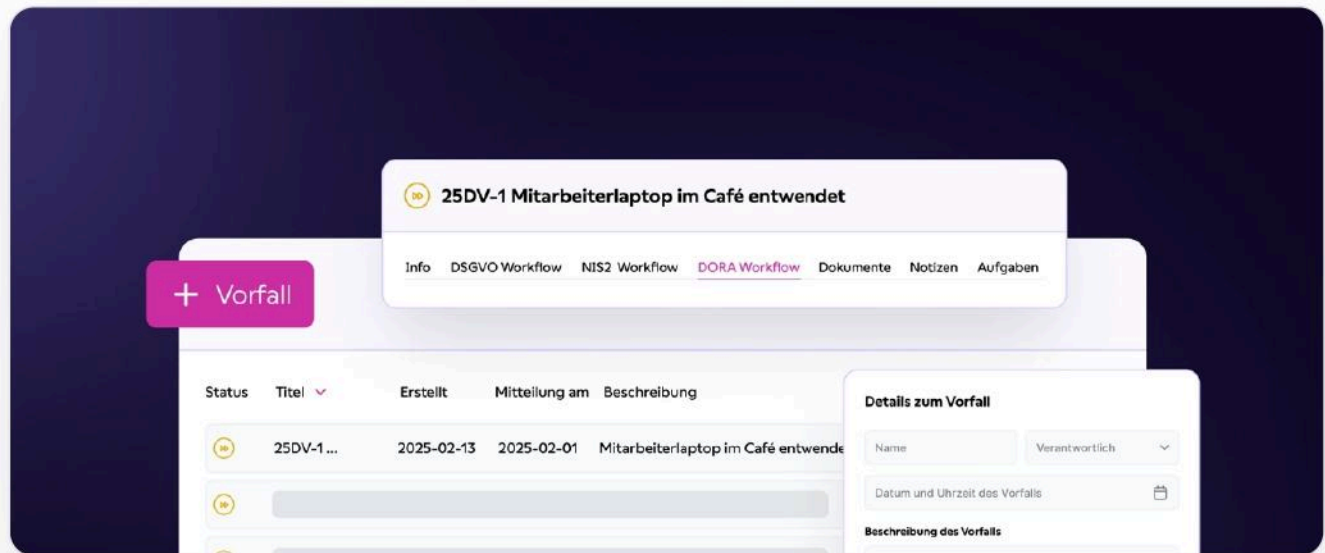
## 6 · LEITUNG UND LIEFERKETTE STEUERN

Die Geschäftsführung schulen, Billigung und Überwachung dokumentieren, die eigenen SaaS- und Sub-Dienstleister vertraglich einbinden und einen Audit-Trail führen. NIS2 ist kein Projekt mit Enddatum, sondern ein dauerhafter Prozess. Wer das verankert, ist zugleich reif für ISO 27001 und SOC 2. Der Aufwand von heute trägt so gleich mehrere Nachweise von morgen.



# Von der starken Technik zur **auditbereiten Umsetzung.**

Das Digital Compliance Office (DCO) führt IT-Dienstleister durch die gesamte NIS2-Umsetzung: Betroffenheit, Risiken, 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.



## Geführter Aufbau

Der Navigator formalisiert die vorhandene Technik Schritt für Schritt zu auditfähigen Prozessen und Nachweisen, ohne dass Sie das Rad neu erfinden.

## Zugänge & Lieferkette

Module für Zugriffskontrolle, Privileged-Access und Lieferantensteuerung, genau die Punkte, die Auftraggeber und §30 bei IT-Dienstleistern prüfen.

## Mehrere Frameworks

NIS2, ISO 27001 und SOC 2 laufen auf einem gemeinsamen ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt dreimal.

## 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 wird aus vorhandener Technik in Wochen ein auditbereiter Nachweis, statt in Quartalen.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Zugänge, 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 das Team die wirksamsten Maßnahmen zuerst ab und verteilt den Rest planbar über die folgenden Wochen. Der Fortschritt bleibt dabei jederzeit sichtbar, auch im laufenden Projektgeschäft.

## EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2, ISO 27001 und SOC 2 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, von Microsoft 365 bis zur Cloud, sodass das ISMS auch im Projektgeschäft aktuell bleibt.

Für einen IT-Dienstleister heißt das weniger Doppelarbeit. Der Nachweis für NIS2 lässt sich mit wenigen Ergänzungen zur ISO-27001-Zertifizierung oder zum SOC-2-Testat ausbauen, statt jedes Mal von vorn zu beginnen.

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

# Über 500 Unternehmen **arbeiten mit SECJUR.**

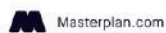
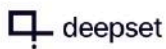
Software-Häuser, Managed-Service-Provider, IT-Berater und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem IT-Umfeld:

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



**René Schlöß**  
Founder & Managing  
Director, reanmo

## REFERENZEN AUS SOFTWARE, IT-CONSULTING UND MANAGED SERVICES



### 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 IT-DIENSTLEISTER SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, mit Vorlagen, die mehrere Frameworks zugleich bedienen. Das Team bleibt beim Kundenprojekt, die Compliance entsteht parallel.

Nachweise wachsen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den Systemen, mit denen ohnehin gearbeitet wird, sodass Geschäftsführung, Technik und Projektteams 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 in kleinen, technikgetriebenen Teams.

Und die Plattform denkt in der Realität des Projektgeschäfts. 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 Dienstleister, der seine Zugänge im Griff hat und seine Lieferkette steuert. Genau das sichert Aufträge und überzeugt große Kunden in ihren Sicherheitsprüfungen.

Ein gelebtes ISMS macht Sicherheit vom lästigen Fragebogen zum Verkaufsargument. Kundenaudits sind in Stunden beantwortet, Sicherheitsprüfungen verlieren ihren Schrecken, und Auftraggeber sehen belegt, dass ihre Daten in verlässlichen Händen liegen.

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 SOC-2-Testat und die nächste Kundenanfrage. Sicherheit wird so zum festen Bestandteil der Art, wie der Dienstleister arbeitet.



# 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.

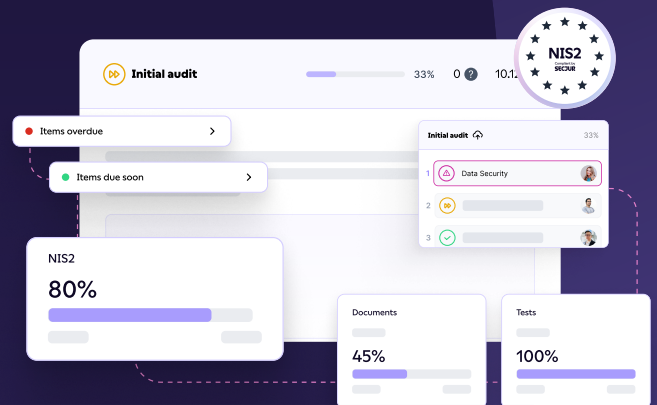
Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- ✓ 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 Schluß**  
Founder & Managing  
Director, reanmo



FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR



[www.secjur.com](https://www.secjur.com)