// KI-Hub VON STRUKTURAFLOW

COMPLIANCE

NIS-2 in Österreich: NISG 2026 – Pflichten, Fristen, Kosten für KMU

Das NISG 2026 tritt am 1. Oktober 2026 in Kraft. Welche Betriebe betroffen sind, welche Maßnahmen bis wann umzusetzen sind und was die Compliance realistisch kostet.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
6. Mai 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/nis-2-pflichten-kmu-oesterreich-checkliste/

Ein IT-Dienstleister mit 40 Mitarbeitenden in Wien, der zum ersten Mal den Begriff „NIS-2“ im Newsletter seines Steuerberaters liest – das ist keine Randerscheinung. Vielen österreichischen Betrieben geht es gerade so. Und die meisten Suchergebnisse helfen wenig, weil sie entweder das deutsche BSI-Gesetz erklären, in EU-Amtsdeutsch verfasst sind – oder, besonders tückisch, sich auf einen österreichischen Gesetzentwurf beziehen, der nie in Kraft getreten ist.

Denn die österreichische Umsetzung hat einen Umweg genommen. Ein erster Entwurf, das **NISG 2024**, scheiterte im Nationalrat an der erforderlichen Zwei-Drittel-Mehrheit. Erst am 12. Dezember 2025 wurde das **NISG 2026** (Netz- und Informationssystemsicherheitsgesetz 2026) beschlossen, am 23. Dezember 2025 als BGBl I Nr. 94/2025 kundgemacht – und es tritt am **1. Oktober 2026** in Kraft. Bis dahin gilt noch das NISG 2018.

Wer also einen Artikel oder eine Beratungsunterlage vor sich hat, in der „NISG 2024“ steht: Das Papier ist überholt. Und wer darin liest, die zuständige Behörde sei die RTR, liest ebenfalls einen alten Stand. Die RTR ist in Österreich die KI-Servicestelle für den EU AI Act – für NIS-2 ist sie nicht zuständig.

Dieser Artikel beantwortet die drei Fragen, die österreichische Betriebe wirklich beschäftigen: Bin ich überhaupt betroffen? Was muss ich konkret umsetzen? Und was kostet das realistisch?

Was ist NIS-2 - und was hat das mit Ihrem Betrieb zu tun?

Die NIS-2-Richtlinie (Network and Information Security Directive 2, Richtlinie (EU) 2022/2555) ist eine EU-weite Regelung zur Cybersicherheit kritischer und wichtiger Einrichtungen. Die Umsetzungsfrist für die Mitgliedstaaten endete im Oktober 2024 – Österreich hat sie um rund zwei Jahre überzogen.

Das NISG 2026 setzt die Richtlinie nun in österreichisches Bundesrecht um und ersetzt das NISG 2018 samt Netz- und Informationssystemsicherheitsverordnung (NISV). Der Anwendungsbereich wächst dabei drastisch: von rund 100 bisher erfassten Einrichtungen auf **etwa 4.000 bis 5.000 Unternehmen** aus 18 Sektoren.

Der entscheidende Unterschied zu NIS-1: mehr Sektoren, niedrigere Schwellenwerte, strengere Pflichten. NIS-2 ist ausdrücklich kein reines Großkonzern-Thema. Betriebe ab 50 Mitarbeitenden oder 10 Millionen Euro Jahresumsatz können in bestimmten Sektoren direkt erfasst sein – und kleinere Betriebe geraten über die Lieferkette hinein, ohne selbst je registrierungspflichtig zu werden.

Die neue Behördenstruktur - der wichtigste Unterschied zum gescheiterten Entwurf

Einer der Hauptkritikpunkte am NISG 2024 war die Ansiedelung der Cybersicherheitsbehörde direkt beim Innenministerium. Das NISG 2026 löst das anders: Es richtet ein eigenes **Bundesamt für Cybersicherheit** ein, das dem Innenminister zwar nachgeordnet, organisatorisch aber außerhalb der Generaldirektion für die öffentliche Sicherheit angesiedelt ist (§ 3a Abs. 2 NISG 2026). Im Gesetzestext heißt es schlicht „Cybersicherheitsbehörde".

Für die Praxis heißt das: Ihr Ansprechpartner ist weder das BSI noch die RTR, sondern das Bundesamt für Cybersicherheit. Die Registrierung soll über das **Unternehmer-Service-Portal (USP)** laufen; das genaue Verfahren wird noch per Verordnung festgelegt. Meldungen zu Sicherheitsvorfällen laufen über das zuständige CSIRT.

Die Fristen - der Fahrplan bis Herbst 2028

DATUM	WAS PASSIERT
bis 30.09.2026	NISG 2018 gilt weiter
01.10.2026	NISG 2026 tritt in Kraft. Risikomanagementmaßnahmen, Lieferkettensicherheit und Meldepflichten gelten ab diesem Tag
31.12.2026	Registrierung bei der Cybersicherheitsbehörde (3 Monate ab Inkrafttreten, § 29)
30.09.2027	Selbstdeklaration: Information über die umgesetzten Risikomanagementmaßnahmen
ab 01.10.2028	Frühestmöglicher Zeitpunkt, ab dem die Behörde eine externe Prüfung verlangen kann

Anders als in Deutschland gibt es also eine echte Vorlaufzeit. Das klingt nach viel – ist es aber nicht, wenn Sie bei null starten. Lieferkettenabsicherung und Business-Continuity-Konzepte brauchen Monate, nicht Wochen. Und die Uhr für die Selbstdeklaration läuft ab der Registrierungspflicht weiter, unabhängig davon, wie weit Sie inhaltlich sind.

Bin ich betroffen? So prüfen Sie Ihre Betroffenheit in 3 Schritten

Schritt 1 - Sektorzugehörigkeit prüfen

Das NISG 2026 unterscheidet zwischen **wesentlichen** und **wichtigen Einrichtungen** (§ 24, Anlagen 1 und 2). Die Unterscheidung bestimmt, wie streng die Aufsicht ausfällt und wie hoch die maximalen Geldbußen sind.

KATEGORIE	BEISPIEL-SEKTOREN
Wesentliche Einrichtungen	Energie, Trinkwasser, Abwasser, Gesundheit, digitale Infrastruktur, Bankwesen, Finanzmarktinfrastruktur, Verkehr, Weltraum, öffentliche Verwaltung
Wichtige Einrichtungen	Verwaltung von IKT-Diensten (u. a. MSP und MSSP), Post- und Kurierdienste, Abfallwirtschaft, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Dienste, Forschung

Besonders relevant: **Managed Service Provider**, **IT-Dienstleister und Cloud-Anbieter** fallen explizit unter NIS-2 – auch wenn sie selbst keine kritische Infrastruktur betreiben, sondern nur für Kunden tätig sind, die es tun.

Ein Gegenbeispiel: Eine Steuerberatungskanzlei mit 60 Mitarbeitenden fällt nicht direkt unter NIS-2. Aber wenn ihr Cloud-Softwareanbieter erfasst ist, können dessen Lieferkettenpflichten sehr wohl Anforderungen an die Kanzlei stellen – vertraglich weitergereicht.

Schritt 2 - Größenschwellen prüfen

Die Sektorzugehörigkeit allein reicht nicht. Die Einstufung folgt der EU-KMU-Definition:

Große Unternehmen (in Anlage-1-Sektoren regelmäßig wesentliche Einrichtungen): - ≥ 250 Mitarbeitende **ODER** - > 50 Mio. € Jahresumsatz **UND** > 43 Mio. € Bilanzsumme

Mittlere Unternehmen (regelmäßig wichtige Einrichtungen): - 50–249 Mitarbeitende **ODER** - > 10 Mio. € Jahresumsatz **UND** > 10 Mio. € Bilanzsumme

Wichtige Ausnahme: Bestimmte Einrichtungen – etwa Anbieter öffentlicher Kommunikationsnetze, Vertrauensdiensteanbieter oder Betreiber kritischer Infrastruktur – sind unabhängig von der Größe erfasst.

Ein Hinweis zur Verlässlichkeit: Die endgültige Einstufung ergibt sich aus § 24 in Verbindung mit den Anlagen 1 und 2 des NISG 2026 und ist in Grenzfällen nicht trivial. Wer knapp an einer Schwelle liegt oder in mehreren Sektoren tätig ist, sollte das nicht allein anhand einer Tabelle entscheiden.

Schritt 3 - Registrierung vorbereiten

Betroffene Einrichtungen müssen sich binnen drei Monaten nach Inkrafttreten registrieren, also **bis 31. Dezember 2026**. Die Registrierung ist nicht optional und selbst sanktionsbewehrt – sie ist zugleich Voraussetzung für Meldeprozesse und die gesamte weitere behördliche Kommunikation.

Mit der Registrierung beginnt automatisch die Frist für die Selbstdeklaration zu laufen. Wer spät registriert, verkürzt sich also nicht die Vorbereitungszeit für den nächsten Schritt – sie hängt an der Registrierungspflicht, nicht am tatsächlichen Registrierungsdatum.

Sanktionen - und die Haftung der Geschäftsführung

Das ist der Punkt, der im NISG 2026 neu und für Entscheider unangenehm konkret ist.

VERSTOSS DURCH	HÖCHSTBETRAG
Wesentliche Einrichtung	10 Mio. € oder 2 % des weltweiten Jahresumsatzes – der höhere Wert gilt
Wichtige Einrichtung	7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes – der höhere Wert gilt

Dazu kommt ein Instrumentarium jenseits von Geld: Die Cybersicherheitsbehörde kann verbindliche Anweisungen erteilen und bei wesentlichen Einrichtungen im Extremfall die Tätigkeit vorübergehend aussetzen – bis hin zu einem vorübergehenden Tätigkeitsverbot für Personen mit Geschäftsleitungsaufgaben.

Erstmals ausdrücklich geregelt: die Verantwortung der Leitungsorgane (§ 31). Die Geschäftsführung muss die Risikomanagementmaßnahmen billigen, ihre Umsetzung überwachen – und sich selbst schulen lassen. Cybersicherheit ist damit rechtlich keine Aufgabe mehr, die man vollständig an die IT delegieren kann. Sie bleibt an der Person hängen, die im Firmenbuch steht.

Die NIS-2-Pflichten im Überblick - was konkret umzusetzen ist

Artikel 21 der NIS-2-Richtlinie, in Österreich umgesetzt in § 32 NISG 2026, definiert zehn Mindestmaßnahmen. Hier sind alle zehn – mit Bezug auf den Alltag eines mittelständischen Betriebs:

1. Risikoanalyse und Sicherheitskonzept Ein dokumentiertes Verfahren, das identifiziert, welche IT-Systeme kritisch sind und welche Risiken bestehen. In der Praxis: ein strukturiertes Dokument, kein 100-seitiges ISMS-Manual.

2. Incident Response (Reaktion auf Sicherheitsvorfälle) Definierte Prozesse für den Fall eines Cyberangriffs oder Systemausfalls. Wer ist verantwortlich? Wer wird wann informiert? Schriftlich, nicht im Kopf des IT-Leiters.

3. Business Continuity und Backup-Management Notfallpläne für längere Systemausfälle, regelmäßige Backups mit **nachgewiesener** Wiederherstellbarkeit. Viele Betriebe haben Backups – aber kein dokumentiertes Wiederherstellungskonzept. Genau das ist der Unterschied.

4. Supply-Chain-Sicherheit (Lieferantenbewertung) Sie müssen sicherstellen, dass auch Ihre Dienstleister angemessene Sicherheitsstandards einhalten. Das geht deutlich über einen Auftragsverarbeitungsvertrag hinaus – und ist der Mechanismus, über den NIS-2 auf Betriebe durchschlägt, die selbst nie registrierungspflichtig werden.

5. Sicherheit bei Beschaffung und Entwicklung Neue Software und Hardware müssen mit Blick auf Sicherheitsanforderungen ausgewählt werden. Patch-Management und Update-Prozesse müssen geregelt sein.

6. Wirksamkeitsbewertung und Audits Die Maßnahmen müssen regelmäßig auf Wirksamkeit überprüft werden – intern durch dokumentierte Reviews oder extern durch Sicherheitsaudits. Für die organisatorische Umsetzung akzeptiert die Behörde auch einschlägige Zertifikate wie ISO 27001; für die technischen Maßnahmen ist ein aktueller Prüfbericht zu übermitteln.

7. Cyberhygiene und Schulungen Regelmäßige Schulungen für Mitarbeitende – Phishing-Erkennung, sichere Passwörter, Umgang mit verdächtigen Nachrichten. Einmalige Schulungen genügen nicht. Und: Die Leitungsorgane sind ausdrücklich mitgemeint.

8. Kryptografie und Verschlüsselung Sensible Daten verschlüsselt übertragen und speichern. Konkret: HTTPS auf allen Systemen, verschlüsselte Endgeräte, verschlüsselte Kommunikation wo nötig.

9. Personalsicherheit und Zugriffskontrollen Rollenbasierte Rechtevergabe, saubere Offboarding-Prozesse, Zugriffsprotokolle. Wer diese Protokolle führt, sollte gleich mitdenken, wie lange sie aufbewahrt werden – Protokollierungspflicht und datenschutzrechtliche Speicherbegrenzung stehen in einem Spannungsverhältnis, das ab Oktober für deutlich mehr Betriebe relevant wird. Für einen umfassenden Überblick zur DSGVO-konformen Nutzung von KI-Tools im Unternehmen lohnt sich ein Blick auf die spezifischen Anforderungen.

10. Multi-Faktor-Authentifizierung (MFA) Verpflichtend für den Zugang zu kritischen Systemen, besonders bei Remote-Zugängen, E-Mail und Administrationsoberflächen. Viele Microsoft-365-Installationen sind hier noch nicht vollständig konfiguriert.

Eine Praxis-Note: Nicht alle zehn Maßnahmen sind gleich aufwändig. Wer bereits strukturierte IT-Prozesse hat, ist bei Punkt 7 und 10 schnell fertig. Wer keine dokumentierten Notfallpläne hat, braucht für Punkt 3 deutlich länger. Die sinnvolle Reihenfolge hängt vom Reifegrad ab, nicht von der Nummerierung.

Meldepflichten bei Sicherheitsvorfällen - was, wann, wie?

Ab 1. Oktober 2026 gilt ein **dreistufiges Meldeverfahren**, wenn ein erheblicher Sicherheitsvorfall eintritt:

STUFE	FRIST	INHALT
Frühwarnung	unverzüglich, jedenfalls binnen 24 Stunden	Erstinformation; insbesondere ob ein Verdacht auf eine rechtswidrige Handlung oder grenzüberschreitende Auswirkungen besteht
Meldung	unverzüglich, jedenfalls binnen 72 Stunden	Schweregrad, Auswirkungen, gegebenenfalls Kompromittierungsindikatoren
Abschlussbericht	spätestens 1 Monat nach der Frühwarnung	Beschreibung des Vorfalls, Art der Bedrohung, Ursachen, Abhilfemaßnahmen

Auf Ersuchen des CSIRT oder der Behörde kommen Zwischenberichte dazu. Zusätzlich gibt es die Möglichkeit der **freiwilligen Meldung** von Beinahe-Vorfällen und Bedrohungen – ein Weg, der für Betriebe unterhalb der Schwelle interessant sein kann.

Konkretes Beispiel: Ein IT-Dienstleister mit 60 Mitarbeitenden bemerkt am Dienstagmorgen, dass Ransomware drei Server verschlüsselt hat und mehrere Kundensysteme nicht erreichbar sind. Die Frühwarnung muss bis Mittwochmorgen übermittelt sein – unabhängig davon, ob der Angriff dann schon analysiert ist. Genau dafür braucht es einen vorbereiteten Prozess: Wer entscheidet mitten in der Krise, dass gemeldet wird, und wer schreibt die Meldung?

Zwei Punkte, die in der Praxis regelmäßig untergehen:

- Die Behördenmeldung ist **vertraulich** und nicht dasselbe wie eine öffentliche Bekanntmachung. Die Kommunikation mit betroffenen Kunden ist eine separate Entscheidung.
- Sind personenbezogene Daten betroffen, kommt **zusätzlich** die DSGVO-Meldepflicht nach Art. 33 ins Spiel – eigene Frist, eigene Behörde, eigener Adressat. Wer bereits DSGVO-Prozesse für Datenpannen definiert hat, kann diese als Ausgangspunkt nutzen, aber nicht als Ersatz.

Die Checkliste - NIS-2-Umsetzung Schritt für Schritt

Die folgende Checkliste gibt eine strukturierte Orientierung. Sie ersetzt keine Rechtsberatung, hilft aber, den Überblick zu behalten.

Phase 1 - Sofortmaßnahmen (jetzt bis Herbst 2026)

AUFGABE	STATUS
Betroffenheitscheck: Sektor + Größenschwelle nach § 24 und Anlagen 1/2 prüfen	☐ Offen
Verantwortliche Person für die NIS-2-Umsetzung intern benennen	☐ Offen
Ist-Stand der IT-Sicherheit erheben (intern oder mit externem Audit)	☐ Offen
Überblick über aktuelle Dienstleister und deren Sicherheitsstandards	☐ Offen
Registrierung vorbereiten – USP-Zugang klären, Verordnung beobachten	☐ Offen

Phase 2 - Strukturmaßnahmen (bis Ende 2026)

AUFGABE	STATUS
Risikoanalyse dokumentieren	☐ Offen
Meldeprozess für Sicherheitsvorfälle definieren und schriftlich festhalten	☐ Offen
Registrierung bei der Cybersicherheitsbehörde bis 31.12.2026 abschließen	☐ Offen
MFA für alle kritischen Systeme und Remote-Zugänge einführen	☐ Offen
Backup-Konzept überprüfen – inkl. dokumentierter Wiederherstellungstests	☐ Offen
Zugriffsrechte nach Rollen strukturieren, Offboarding-Prozess prüfen	☐ Offen
Verschlüsselung sensibler Systeme und Daten sicherstellen	☐ Offen
Schulung der Leitungsorgane einplanen (§ 31 – keine Kür, sondern Pflicht)	☐ Offen
Erste Mitarbeiterschulung zu Cyberhygiene durchführen	☐ Offen

Phase 3 - Nachweis und laufende Compliance (2027-2028)

AUFGABE	STATUS
Selbstdeklaration bis 30.09.2027 vorbereiten und übermitteln	☐ Offen
Jährliche Wirksamkeitsprüfung der Maßnahmen	☐ Offen
Regelmäßige Mitarbeiterschulungen (mindestens jährlich)	☐ Offen
Lieferantenbewertung aktuell halten	☐ Offen
Sicherheitskonzept bei wesentlichen Systemänderungen aktualisieren	☐ Offen
Prüfbereitschaft herstellen – Aufforderungen ab 01.10.2028 möglich	☐ Offen

Was kostet NIS-2-Compliance realistisch?

Das ist die Frage, die in den meisten Artikeln ausgespart wird. Hier eine ehrliche Einschätzung – ohne Beschönigung, aber auch ohne Horrorzahlen.

Die wichtigsten Kostentreiber:

- **Interne Personalstunden:** Projektleitung, IT-Administration, Dokumentation. Der größte versteckte Kostenfaktor.
- **Externes IT-Sicherheitsaudit:** je nach Umfang etwa 3.000–10.000 €. Liefert die Grundlage für alles Weitere.
- **Technische Maßnahmen:** MFA ist oft in bestehenden Lizenzpaketen enthalten (z. B. Microsoft 365 Business Premium). EDR-Lösungen liegen bei 5–15 € pro Gerät und Monat, eine SIEM-Lösung für kleinere Umgebungen bei 300–800 € monatlich.
- **Schulungen:** externe Präsenzschulungen 200–600 € pro Person; E-Learning-Plattformen 20–80 € pro Mitarbeitendem und Jahr. Die Schulung der Leitungsorgane kommt dazu.

Grobe Orientierungswerte:

UNTERNEHMENSGRÖSSE	GESCHÄTZTER ERSTAUFWAND
10–50 Mitarbeitende	5.000–25.000 €
50–250 Mitarbeitende	20.000–80.000 €

Richtwerte, keine Garantien. Der tatsächliche Aufwand hängt stark vom Reifegrad ab.

Wichtige Relativierung: Wer bereits ein ISO-27001-zertifiziertes ISMS oder dokumentierte Sicherheitsprozesse betreibt, hat deutlich geringeren Zusatzaufwand – oft reicht eine Gap-Analyse. Auch regelmäßige KI-Tool-Sicherheitsaudits können als Grundlage für den Wirksamkeitsnachweis dienen. Und ein Zertifikat ist beim Wirksamkeitsnachweis gegenüber der Behörde ausdrücklich verwertbar.

Zur Einordnung: Die Kosten eines Cyberangriffs auf einen mittelständischen österreichischen Betrieb liegen erfahrungsgemäß im fünfstelligen bis niedrigen sechsstelligen Bereich – ohne Reputationsschaden und Kundenverlust. Besonders KI-automatisierte Ransomware-Angriffe senken die Angriffshürde massiv und erhöhen damit das Risiko für KMU. NIS-2-Compliance ist damit nicht nur Pflicht, sondern in vielen Fällen schlicht Risikoabsicherung.

Österreich und Deutschland - das Verhältnis hat sich umgedreht

Weil ein Großteil der deutschsprachigen Suchergebnisse auf deutsche Quellen verweist, hier der aktuelle Stand:

ASPEKT	ÖSTERREICH	DEUTSCHLAND
Nationales Gesetz	NISG 2026 (BGBl I 94/2025)	NIS2UmsuCG (novelliertes BSIG)
In Kraft seit	1. Oktober 2026	6. Dezember 2025
Zuständige Behörde	Bundesamt für Cybersicherheit („Cybersicherheitsbehörde“)	BSI
Registrierung	über USP, bis 31.12.2026	über das BSI-Portal MUK, gesetzliche Frist am 6.3.2026 abgelaufen
Betroffene Einrichtungen	rund 4.000–5.000	rund 29.500
Übergangsfrist	rund 9 Monate zwischen Kundmachung und Inkrafttreten	keine

Deutschland ist Österreich also inzwischen um fast ein Jahr voraus – und das Bild dort ist lehrreich: Von rund 29.500 betroffenen Einrichtungen hatten sich zur gesetzlichen Frist erst etwa 11.500 registriert. Das BSI hat daraufhin eine Nachfrist bis Ende Juli 2026 kommuniziert. Wer glaubt, so eine Frist ließe sich gemütlich aussitzen, sollte sich ansehen, wie viele deutsche Betriebe jetzt rückwirkend unter Zugzwang stehen.

Für Unternehmen mit Standorten in beiden Ländern gilt: zwei Registrierungen, zwei Meldewege, zwei Nachweislogiken. Die technische Basis lässt sich gemeinsam aufbauen, die Formalien nicht.

Und auch ohne deutschen Standort relevant: Wenn Ihr österreichischer Betrieb als Lieferant für ein deutsches Unternehmen tätig ist, das unter NIS-2 fällt, werden dessen Supply-Chain-Anforderungen vertraglich an Sie weitergereicht – seit Dezember 2025, nicht erst ab Oktober 2026. Mehr zur deutschen Umsetzung und den unterschiedlichen Anforderungen finden Sie im Artikel NIS2 / NISG 2026: Auch ohne direkte Pflicht relevant für KMU? Das ist keine theoretische Gefahr; entsprechende Klauseln stehen bereits in Lieferantenverträgen.

Praxis-Tipp - wo Digitalisierung bei der Umsetzung hilft

NIS-2-Compliance ist kein reines Papierprojekt. Verschiedene Werkzeuge reduzieren den Aufwand – wenn man sie richtig einsetzt.

Asset-Inventarisierung und Risikoanalyse: Plattformen, die IT-Assets automatisiert erfassen und Risikobewertungen strukturieren, ersetzen keine fachkundige Einschätzung, beschleunigen aber die Erhebungsphase erheblich.

Automatisierte Anomalie-Erkennung: SIEM- und XDR-Lösungen erfassen auffällige Aktivitäten in Echtzeit. Das ist nicht nur eine NIS-2-Anforderung (Wirksamkeitsbewertung, Incident Response), sondern praktisch wertvoll: Vorfälle werden früher erkannt.

Digitale Dokumentations-Workflows: Statt Excel-Tabellen helfen No-Code-Tools wie n8n oder spezialisierte GRC-Plattformen, Richtlinien, Schulungsnachweise und Auditprotokolle strukturiert und nachweisbar zu verwalten. Für die Selbstdeklaration 2027 brauchen Sie genau das: eine Dokumentation, die auf Knopfdruck zeigbar ist.

Ehrliche Einschätzung: Software löst NIS-2-Compliance nicht. Sie reduziert Dokumentations- und Überwachungsaufwand – die inhaltliche Bewertung von Risiken und die Entscheidung über Maßnahmen bleiben menschliche Aufgaben. Und seit § 31 auch ausdrücklich Aufgaben der Geschäftsführung.

Ein Hinweis für Betriebe, die selbst KI-Systeme einsetzen oder anbieten: Solche Systeme können unter NIS-2 als kritische IT-Systeme eingestuft werden, während gleichzeitig der EU AI Act eigene Compliance-Pflichten mitbringt. Beide Regelwerke sollten gemeinsam betrachtet werden – das vermeidet Doppelarbeit und hebt Synergien bei Dokumentation und Schulung.

Nächste Schritte

Die drei wichtigsten Sofortmaßnahmen: Betroffenheitscheck durchführen, den aktuellen IT-Sicherheitsstand erheben, eine verantwortliche Person benennen. Alles andere baut darauf auf.

Für viele Betriebe ist externe Begleitung beim ersten Durchlauf sinnvoll – nicht weil das Gesetz unlesbar wäre, sondern weil die Priorisierung im laufenden Betrieb der eigentliche Stolperstein ist. Welche der zehn Pflichtmaßnahmen hat bei Ihrem Reifegrad Vorrang? Welche Lücken sind tatsächlich kritisch, welche können bis 2027 warten? Diese Einschätzung kostet Zeit, und die meisten Teams haben sie nicht.

Wenn Sie unsicher sind, ob Ihr Unternehmen überhaupt betroffen ist – oder welche der zehn Maßnahmen bei Ihnen Priorität haben: In einem kostenlosen 30-Minuten-Gespräch klären wir gemeinsam Ihren NIS-2-Status und die nächsten sinnvollen Schritte. Ohne Verkaufsgespräch, ohne Verpflichtung.

Bis zum 1. Oktober sind es noch keine zwei Monate.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

https://wissen.strukturaflow.it.com