NIS2 Betroffenheits-Check für den Mittelstand

Registrierungsfrist und Duldungsfrist bis 31.07.2026. Sofortige Orientierung für Geschäftsführung und IT.

STAND: AUGUST 2026

Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) ist seit dem 6. Dezember 2025 in Kraft – ohne Übergangsfrist. Die gesetzliche Registrierungsfrist nach §33 BSIG endete am 6. März 2026 und wurde nicht verlängert. Die vom BSI gewährte Duldung für verspätete Nachmeldungen ist am 31. Juli 2026 ausgelaufen.

Von rund 29.500 betroffenen Unternehmen in Deutschland waren Ende Mai 2026 erst etwa 18.500 registriert. Wer bis heute nicht registriert ist, ist säumig – ohne Schonfrist, und in einem Umfeld, in dem die Aufsicht die Einhaltung nun konsequent prüft.

NIS2 verpflichtet Unternehmen, bei einem Cyberangriff handlungsfähig zu bleiben – und das nachzuweisen. Vergleichbar einer Brandschutzvorschrift für die digitale Welt. Dieser Check gibt Ihnen eine erste Einschätzung in drei Fragen.

Vorbemerkung: NIS2 ist im Kern ein GRC-Thema, kein IT-Thema. Die drei Dimensionen spiegeln sich direkt in den Anforderungen:

- **Governance –** Wer ist verantwortlich, wer berichtet wem, wie ist Informationssicherheit in der Unternehmenssteuerung verankert?
- **Risk –** Risikoanalyse, Risikoregister, Bewertung von Lieferanten und Dienstleistern.
- **Compliance –** Nachweisführung, Auditierbarkeit, Meldepflichten gegenüber dem BSI.

TEIL 1 · BETROFFENHEIT PRÜFEN

1 Mehr als 50 Mitarbeitende oder mehr als 10 Mio. € Jahresumsatz?
Ab dieser Schwelle fällt Ihr Unternehmen in den Anwendungsbereich – abhängig vom Sektor. Bei Konzernzugehörigkeit zählt die wirtschaftliche Einheit, nicht die einzelne Gesellschaft.

2 Tätig in einem der 18 regulierten Sektoren?
Energie · Verkehr · Wasser und Abwasser · Gesundheit · digitale Infrastruktur und IT-Dienstleistungen · verarbeitendes Gewerbe, insbesondere Maschinen-, Fahrzeug- und Elektrotechnikbau · Lebensmittelproduktion · Chemie · Post- und Kurierdienste · Abfallwirtschaft · Forschung.

3 Liefern Sie Produkte oder Dienstleistungen an NIS2-pflichtige Unternehmen?
Über die Lieferkette entstehen vertragliche Anforderungen auch für Zulieferer – unabhängig von Größe und Sektor.

Ja zu Frage 1 und 2: Ihr Unternehmen ist mit hoher Wahrscheinlichkeit registrierungs- und umsetzungspflichtig. Die Betroffenheit rechtssicher zu klären ist selbst eine regulatorische Pflicht – die Selbsteinstufung nimmt Ihnen niemand ab.

Nur Ja zu Frage 3: Direkte Betroffenheit unwahrscheinlich, faktische Betroffenheit sehr wahrscheinlich – Ihre Kunden werden Nachweise verlangen.

Dreimal Nein: Prüfen Sie dennoch künftiges Wachstum und Konzernzugehörigkeit.

TEIL 2 · WELCHE KATEGORIE – UND WAS DAS BEDEUTET

Das BSIG unterscheidet zwei Kategorien. Der Unterschied betrifft Aufsicht und Bußgeldrahmen.

	Besonders wichtige Einrichtung (§28 Abs. 1)	Wichtige Einrichtung (§28 Abs. 2)
Schwelle	ab 250 Mitarbeitende oder über 50 Mio. € Umsatz bei über 43 Mio. € Bilanzsumme	ab 50 Mitarbeitende oder über 10 Mio. € Umsatz
Aufsicht	proaktiv, auch unangekündigt (§61)	anlassbezogen, reaktiv (§62)
Bußgeldrahmen	bis 10 Mio. € oder 2 % des weltweiten Jahresumsatzes	bis 7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes

Maßgeblich ist jeweils der höhere Betrag. Die versäumte Registrierung allein ist ein eigenständiger Bußgeldtatbestand nach §65 BSIG mit bis zu 500.000 €.

TEIL 3 · TYPISCHE LÜCKEN IM MITTELSTAND

Bereich	Typische Lücke	Was das BSIG erwartet
Governance	Keine klar benannte Verantwortung	Formell bestellte Verantwortliche mit Mandat
Incident Response	Informelle, reaktive Prozesse	Definierter, geübter Meldeprozess: 24 Stunden Erstmeldung, 72 Stunden Konkretisierung, 30 Tage Abschluss (§32)
Backup & Restore	Backup vorhanden, nie getestet	Regelmäßige, dokumentierte Restore-Tests
Lieferkette	Dienstleister nie sicherheitsseitig bewertet	Bewertung und Nachhalten kritischer Lieferanten
Nachweisführung	Maßnahmen vorhanden, nicht dokumentiert	Strukturierte, auditierbare Evidenz zu allen zehn Maßnahmenbereichen aus §30

TEIL 4 · SOFORTMASSNAHMEN – KEIN BUDGET NÖTIG, NUR EINE ENTSCHEIDUNG

- **1 Verantwortung:** Person mit Mandat und Zugang zur Geschäftsführung formell bestellen.
- **2 Registrierung:** Registrierung im BSI-Portal unverzüglich nachholen. Sie bleibt verpflichtend und ist auch nach Ablauf der Duldung möglich – und sie zeigt der Aufsicht, dass das Unternehmen tätig geworden ist.
- **3 Kritische Systeme:** Die fünf Systeme benennen, die nicht ausfallen dürfen.
- **4 Incident-Prozess:** Schriftlich festhalten, wer bei einem Angriff was tut – und die 24-Stunden-Frist kennen.
- **5 Restore-Test:** Ein Restore tatsächlich durchführen, nicht nur das Backup prüfen.

PERSÖNLICHE HAFTUNG DER GESCHÄFTSFÜHRUNG

Nach §38 BSIG haben Geschäftsleitungen die Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen. Sie haften persönlich für Versäumnisse – unabhängig davon, ob ein IT-Dienstleister beauftragt ist. Die Pflicht lässt sich nicht delegieren und ein Haftungsverzicht ist unwirksam.

Nächster Schritt: NIS2 Management Briefing

Für Geschäftsführung und Entscheider · online oder vor Ort · kein IT-Vorwissen nötig · kostenfreie Erstberatung. Inhalt: was die Geschäftsführung jetzt wissen und entscheiden muss, in welcher Reihenfolge, und wie sich die Nachweisführung aufbauen lässt.

Termin anfragen: info@teamas.de · Tel 0211-86808930 · www.teamas.de

Kontakt: Tel 0211-86808930, info@teamas.de, TEAM A.S. GmbH, Düsseldorfer Str.31, 40545 Düsseldorf, www.teamas.de

Stand: August 2026.

Dieser Check ersetzt keine rechtliche Prüfung der Betroffenheit im Einzelfall.