KOSTENFREIE VORLAGE

NIS-2-Selbst-Check

In zehn Minuten zur Antwort: Fällt Ihr Unternehmen unter das NIS-2-Umsetzungsgesetz — und welche Pflichten folgen daraus? Teil 1 klärt die Betroffenheit, Teil 2 ist eine Arbeitsliste der zehn Mindestmaßnahmen nach § 30 BSIG.

TEIL 1 · BETROFFENHEIT

Schritt 1 — Größe des Unternehmens

Maßgeblich ist § 28 BSIG. Kreuzen Sie an, was auf Ihr Unternehmen zutrifft:

- ☐ **Besonders wichtige Einrichtung:** mindestens 250 Beschäftigte — oder mehr als 50 Mio. € Jahresumsatz *und* mehr als 43 Mio. € Bilanzsumme.
- ☐ **Wichtige Einrichtung:** mindestens 50 Beschäftigte — oder mehr als 10 Mio. € Jahresumsatz *und* mehr als 10 Mio. € Bilanzsumme.
- ☐ Keine der beiden Schwellen erreicht.

Die Größe allein entscheidet nicht — sie wirkt nur zusammen mit Schritt 2. Unterhalb der Schwellen kann eine Einrichtung dennoch erfasst sein, etwa als einziger Anbieter eines für die Gesellschaft kritischen Dienstes.

Schritt 2 — Sektor

Ist Ihr Unternehmen in einem dieser Bereiche tätig?

- ☐ Energie · Transport und Verkehr · Finanz- und Versicherungswesen · Gesundheit
- ☐ Trinkwasser · Abwasser · digitale Infrastruktur · IT-Dienstleistung und Managed Services
- ☐ Öffentliche Verwaltung · Weltraum
- ☐ Post- und Kurierdienste · Abfallwirtschaft · Chemie · Lebensmittel
- ☐ Verarbeitendes Gewerbe — u. a. Maschinenbau, Fahrzeugbau, Medizinprodukte, Elektronik
- ☐ Digitale Dienste · Forschung

Gerade „verarbeitendes Gewerbe“ nimmt viele Mittelständler in die Pflicht, die sich nie als kritische Infrastruktur verstanden haben.

Schritt 3 — Lieferkette

- ☐ Wir beliefern Unternehmen, die selbst unter NIS-2 fallen.
- ☐ Kunden fragen bereits Sicherheitsnachweise, Audits oder Zertifikate ab.
- ☐ Wir betreiben oder warten IT-Systeme für Dritte.

Auswertung. Trifft in Schritt 1 eine der beiden Schwellen zu *und* in Schritt 2 mindestens ein Sektor, ist Ihr Unternehmen mit hoher Wahrscheinlichkeit betroffen — dann gilt die Registrierungspflicht beim BSI. Kreuze nur in Schritt 3 bedeuten: Sie werden die Anforderungen vertraglich über Ihre Kunden erreichen.

TEIL 2 · DIE ZEHN MINDESTMASSNAHMEN

Wo stehen Sie heute?

§ 30 Abs. 2 BSIG verlangt geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen. Diese zehn Punkte sind der Mindestumfang.

Nr. und Maßnahme nach § 30 Abs. 2 BSIG	ERFÜLLT	TEILWEISE	OFFEN
1. Risikoanalyse und Konzepte für die Sicherheit in der Informationstechnik Dokumentierte Risikobetrachtung, daraus abgeleitete Leitlinie und Richtlinien.	☐	☐	☐
2. Bewältigung von Sicherheitsvorfällen Definierter Prozess von der Erkennung über die Meldung bis zur Nachbereitung.	☐	☐	☐
3. Aufrechterhaltung des Betriebs Backup-Management, Wiederherstellung nach einem Notfall, Krisenmanagement.	☐	☐	☐
4. Sicherheit der Lieferkette Sicherheitsaspekte in den Beziehungen zu direkten Anbietern und Dienstleistern.	☐	☐	☐
5. Sicherheit bei Erwerb, Entwicklung und Wartung Einschließlich Umgang mit Schwachstellen und deren Offenlegung.	☐	☐	☐
6. Bewertung der Wirksamkeit Konzepte und Verfahren, um zu prüfen, ob die Maßnahmen tatsächlich greifen.	☐	☐	☐
7. Schulung und Sensibilisierung Grundlegende Cyberhygiene für alle Beschäftigten, regelmäßig wiederholt.	☐	☐	☐
8. Kryptografie und Verschlüsselung Konzepte für den Einsatz kryptografischer Verfahren.	☐	☐	☐
9. Personalsicherheit, Zugriffskontrolle, Verwaltung von Anlagen Wer darf was — nachvollziehbar geregelt und dokumentiert.	☐	☐	☐
10. Multi-Faktor-Authentifizierung und gesicherte Kommunikation Auch gesicherte Sprach-, Video- und Textkommunikation sowie Notfallkommunikation.	☐	☐	☐

TEIL 3 · FRISTEN UND VERANTWORTUNG

Meldepflichten bei erheblichen Sicherheitsvorfällen

Gemeldet wird nach § 32 BSIG an die gemeinsame Meldestelle des BSI und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe:

Erstmeldung	**unverzüglich, spätestens 24 Stunden nach Kenntniserlangung** Mit Angabe, ob ein rechtswidriges Handeln vermutet wird oder grenzüberschreitende Auswirkungen möglich sind.
Folgemeldung	**unverzüglich, spätestens 72 Stunden nach Kenntniserlangung** Bestätigung oder Aktualisierung der Erstmeldung, erste Bewertung von Schweregrad und Auswirkungen.
Abschlussmeldung	**spätestens einen Monat nach der Folgemeldung** Ausführliche Beschreibung, Bedrohungsanalyse und ergriffene Abhilfemaßnahmen. Dauert der Vorfall noch an, zunächst Fortschrittsmeldung.

Pflichten der Geschäftsleitung

§ 38 BSIG verpflichtet die Geschäftsleitung, die Maßnahmen nach § 30 umzusetzen *und* ihre Umsetzung zu überwachen. Wer diese Pflicht schuldhaft verletzt, haftet der eigenen Einrichtung für den entstandenen Schaden nach den Regeln der jeweiligen Rechtsform. Zusätzlich besteht eine persönliche Schulungspflicht: Die Geschäftsleitung muss regelmäßig an Schulungen teilnehmen, um Risiken erkennen und bewerten zu können.

Was das praktisch heißt. Die Verantwortung lässt sich nicht delegieren, die Arbeit schon. Ein formal bestellter, qualifizierter Informationssicherheitsbeauftragter erledigt die Umsetzung und erzeugt dabei genau die Dokumentation, die im Ernstfall den Sorgfaltsnachweis trägt.

Nächster Schritt

Unsicher bei der Einstufung? Wir nehmen sie im Erstgespräch gemeinsam vor — 15 Minuten, kostenfrei und ohne Verpflichtung.

Telefon 069 66 3 666 30 · sicherheit@infosectec.de · isb.infosectec.de

Rechtsstand August 2026. Diese Unterlage gibt den Gesetzesstand verkürzt wieder und ersetzt keine Rechtsberatung im Einzelfall; maßgeblich ist allein der Gesetzestext. Gesetzestext: gesetze-im-internet.de/bsig_2025 (Abruf 13.08.2026)