

NIS-2 kompakt – das Wichtigste auf zwei Seiten

Orientierung für Geschäftsführung und iT im Mittelstand · Rechtsstand BSIG (NIS2UmsuCG), Juli 2026

Sind Sie betroffen? – Denken in Kategorien

- Besonders wichtige und wichtige Einrichtungen in 14 Sektoren (Anlagen 1 und 2 BSIG), ab Größen-/Umsatzschwellen.
- Betroffenheit ist eine Selbsteinschätzung — in Grenzfällen eine Rechtsfrage.
- Auch wer selbst nicht direkt fällt, wird oft über die Lieferkette vertraglich in die Pflicht genommen.

Erste Orientierung: BSI-Betroffenheitsprüfung (siehe Seite 2).

Warum es Chefsache ist (§ 38)

NIS-2 macht Cybersicherheit zur Chefsache – so bringt es das BSI auf den Punkt.

- Die Geschäftsleitung muss die Maßnahmen umsetzen, ihre Umsetzung überwachen und sich schulen lassen.
- Die Schulungspflicht der Leitung ist persönlich und nicht delegierbar.
- Die Umsetzung kann an Team oder Partner delegiert werden – die Steuerung und Verantwortung bleibt bei der Leitung.

Die drei prozessualen Pflichten

1 Registrierung (§ 33) – in 2 Schritten

1. ELSTER-Organisationszertifikat + "Mein Unternehmenskonto" (MUK)
 2. Registrierung im BSI-Portal (portal.bsi.bund.de)
- Gesetzliche Frist war der 06.03.2026 (Neubetroffene: 3 Monate ab Betroffenheit); BSI-Kulanz bis 31.07.2026 (keine neue Frist).
 - Verspätung ist ein eigenständiger Bußgeldtatbestand (§ 65, bis 500.000 €).
 - ELSTER braucht Vorlauf (~2 Wochen) – früh beantragen.
 - Bereithalten: Sektor, Größe, Rechtsform, Kontaktstelle(n).

2 Meldung (§ 32) – drei Stufen

- 24h Frühwarnung
 - 72h bewertende Meldung
 - 1 Monat Abschlussmeldung*
- Die Uhr startet mit Kenntnis des Vorfalls, nicht mit Abschluss der Analyse.
 - Der Monat läuft ab der bewertenden Meldung. **Dauert der Vorfall an: Fortschrittmeldung.*
 - Bei personenbezogenen Daten läuft die DSGVO-Meldung (72h) in der Regel parallel.
 - Gemeldet wird über das BSI-Portal – den Zugang (ELSTER/MUK) deshalb vor dem Ernstfall einrichten.

3 Nachweisen – Pflicht vs. Fähigkeit

- Nachweispflicht (§ 39): nur Betreiber kritischer Anlagen (KRITIS) – turnusmäßig alle 3 Jahre per Audit.
- Nachweisfähigkeit (§ 30): gilt für alle – jederzeit auf Verlangen belegen können.
- ISO 27001 hilft, das strukturiert zu belegen (Baustein, kein Ersatz).

Kernbotschaft

NIS-2 verlangt kein bestimmtes Werkzeug, sondern ein System, das entscheidet, prüft und steuert — ein Informationssicherheits-Managementsystem (ISMS). Zehn Einzelpflichten werden so zu einem steuerbaren Ganzen, das dauerhaft wirksam bleibt.



DISCOVER THE SPIRIT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

R.iT GmbH – Zentrale Lise-Meitner-Allee 37, 44801 Bochum
+49 (234) 43 88 00-0

R.iT GmbH – Niederlassung Süd Rodinger Straße 15, 93413 Cham
+49 (9971) 806 29-0

info@RiT.de | www.RiT.de

Die zehn Maßnahmen

§ 30 BSIG strukturiert angehen

1. Risikoanalyse & Sicherheitskonzepte	Risiken erfassen, bewerten, behandeln	6. Wirksamkeit bewerten	regelmäßig überprüfen
2. Bewältigung von Sicherheitsvorfällen	erkennen, reagieren, wiederherstellen	7. Cyberhygiene & Schulungen	Basispraktiken + Awareness
3. Aufrechterhaltung des Betriebs	Backup, Wiederanlauf, BCM	8. Kryptografie & Verschlüsselung	Konzepte und Verfahren
4. Sicherheit der Lieferkette	Anbieter & Dienstleister	9. Personalsicherheit & Zugriffskontrolle	Personal, Rechte, Inventar
5. Erwerb, Entwicklung & Wartung	inkl. Schwachstellenmanagement	10. Gesicherte Authentisierung & Kommunikation	MFA, gesicherte (Notfall-)Kommunikation

Nr. 1 und 6 bilden den Steuerungskern (das ISMS), die übrigen sind die operativen Handlungsfelder.

Ihr Weg – klare Etappen

1	Standort	Betroffenheit & Pflichten klären (Dauer: 1-2 Wochen)	Nutzen: NIS-2-Status geklärt
2a	Gap-Analyse	Abgleich mit § 30, priorisierter Fahrplan (Dauer: 2-4 Monate)	Nutzen: Klarheit über Prioritäten
2b	Quick Wins	MFA, Backup, Updates (Dauer: 1-3 Monate)	Nutzen: sofort höhere Sicherheit
3	Umsetzung	Technik, Organisation & Prozesse → ISMS entsteht (Dauer: 6-18 Monate)	Nutzen: weniger Vorfälle, handlungs- & nachweisfähig
4	Betrieb & Verbesserung	Laufende Steuerung → ISMS wirkt (Dauer: laufend)	Nutzen: dauerhaft wirksam, Sorgfaltsnachweis

Die Dauern sind Erfahrungswerte, kein fester Aufwand – vieles läuft parallel zum Tagesgeschäft.

Ihre drei Schritte – scannen & loslegen



1. Betroffenheit prüfen

betroffenheitspruefung-nis-2.bsi.de



2. Registrieren (BSI-Portal)

portal.bsi.bund.de



3. Cheat-Sheet & mehr

rit.de/infocenter

Alle Adressen zum Nachschlagen

Betroffenheitsprüfung: <https://betroffenheitspruefung-nis-2.bsi.de> **Registrierung / BSI-Portal:** <https://portal.bsi.bund.de> **Mein Unternehmenskonto:** <https://info.mein-unternehmenskonto.de> **NIS-2-Übersicht, Infopakete, Checkliste & alle Downloads:** https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html **Gesetzestext BSIG (§§ 30, 32, 33, 38, 39):** https://www.gesetze-im-internet.de/bsig_2025 Checkliste, Onepager ISO 27001 und Geschäftsleitungsschulung finden Sie als PDF-Download auf der BSI-NIS-2-Übersichtsseite (QR links) unter „Publikationen“.



DISCOVER THE SPIR.IT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

R.iT GmbH – Zentrale Lise-Meitner-Allee 37, 44801 Bochum
+49 (234) 43 88 00-0

R.iT GmbH – Niederlassung Süd Rodinger Straße 15, 93413 Cham
+49 (9971) 806 29-0

info@RiT.de | www.RiT.de