

NIS2-Risikomanagement – das Wichtigste auf einer Seite

Öffentliches Lernmaterial · Stand: Oktober 2026

Lernziele: Nach der Einheit können Sie prüfen, ob NIS2 für ein Unternehmen gilt (§ 28), Risiken in eine Matrix einordnen, Maßnahmen ableiten und § 30 zuordnen und begründen, ob das Restrisiko vertretbar ist (§ 38).

Der Fall

Die Altmühltal Wasser GmbH ist ein ausgedachtes Unternehmen. Sie versorgt 85.000 Menschen mit Trinkwasser und hat 140 Beschäftigte. Trinkwasser steht in Anlage 1 des BSI-Gesetzes. Das Unternehmen hat mehr als 50, aber weniger als 250 Beschäftigte. Deshalb ist es eine **wichtige Einrichtung** (§ 28) und muss sich nach § 30 schützen.

Die Risikomatrix

	vernachlässigbar	begrenzt	beträchtlich	existenzbedrohend
sehr häufig	gering	hoch	sehr hoch	sehr hoch
häufig	gering	mittel R2 nachher	hoch R1 Büro	sehr hoch R2 vorher
mittel	gering	mittel	hoch R3 Leitwarte	sehr hoch
selten	gering	gering	mittel	hoch R4 Hochwasser

So lesen Sie die Matrix: Je weiter oben, desto häufiger. Je weiter rechts, desto schlimmer. Die Fernwartung (R2) startet ganz oben rechts. Zwei Maßnahmen machen die Folgen kleiner: Büronetz und Steuerungsnetz trennen (§ 30 Nr. 1) und einen Notbetrieb von Hand üben (Nr. 3). Damit sinkt das Risiko auf „mittel“.

Was das Gesetz verlangt

Norm	Was Sie tun müssen
§ 28 BSIG	Selbst prüfen, ob NIS2 gilt: Sektor und Größe
§ 30 BSIG	Sich in allen zehn Bereichen schützen (siehe unten) – passend zum Risiko
§ 32 BSIG	Vorfälle an das BSI melden: nach 24 Stunden, nach 72 Stunden, nach einem Monat
§ 33 BSIG	Sich innerhalb von drei Monaten beim BSI anmelden
§ 38 BSIG	Die Geschäftsleitung gibt frei, kontrolliert, lässt sich schulen – und haftet
§ 65 BSIG	Bußgelder bis 10 Mio. € oder 2 % (besonders wichtig) bzw. 7 Mio. € oder 1,4 % (wichtig)

Die zehn Pflichtbereiche (§ 30 Abs. 2) – mit Beispiel

Nr. 1 Risiken & Konzepte IT und OT trennen	Nr. 2 Vorfälle bewältigen Notfallplan für Angriffe	Nr. 3 Betrieb sichern Notbetrieb, Offline-Backup	Nr. 4 Lieferkette Audit beim Dienstleister	Nr. 5 Einkauf & Wartung Updates für die Leitwarte
Nr. 6 Wirksamkeit prüfen jährlicher Penetrationstest	Nr. 7 Schulungen Phishing-Training	Nr. 8 Verschlüsselung Kundendaten verschlüsseln	Nr. 9 Zugänge & Personal eigene statt Sammelkonten	Nr. 10 Zwei-Faktor-Anmeldung für die Fernwartung

Merksätze

1. **Alle zehn Bereiche sind Pflicht.** Angefangen wird dort, wo das Risiko am höchsten ist – bei der Altmühltal Wasser an der Fernwartung.
2. **Seltener reicht nicht immer.** Ist die Gesundheit von Menschen in Gefahr, muss ein Risiko weniger schlimm werden, nicht nur seltener.
3. **Ein Rest bleibt immer.** Was übrig bleibt, akzeptiert die Geschäftsleitung bewusst und schriftlich (§ 38).

Begriffe kurz erklärt

NIS2	EU-Richtlinie für mehr Cybersicherheit; in Deutschland umgesetzt im BSI-Gesetz (BSIG)
Restrisiko	das Risiko, das nach allen Maßnahmen übrig bleibt
MFA	Zwei-Faktor-Anmeldung: Passwort plus ein zweiter Nachweis, z. B. ein Code
IT · OT	Büro-Technik · Technik, die Anlagen steuert, etwa Pumpen