



13.11.2025

Ist Ihr Unternehmen NIS-2-
konform aufgestellt?

Unsere Checkliste für Sie



LÖSUNG|N

Checkliste: Ist Ihr Unternehmen bereit?



Betroffenheit

- Gehört Ihre Organisation zu den „besonders wichtigen“ oder „wichtigen“ Einrichtungen?
- Fällt sie als KRITIS-Anlage ohnehin unter verschärfte Anforderungen?
- Ist die Registrierung bei der gemeinsamen Registrierungsstelle von BSI und BBK bereits erfolgt bzw. vorbereitet?

Checkliste: Ist Ihr Unternehmen bereit?



Verantwortung & Governance

- Ist die Geschäftsführung über ihre persönlichen Pflichten und Haftungsrisiken informiert?
- Sind Rollen, Verantwortlichkeiten und Eskalationswege für Cyber- und Informationssicherheit klar definiert?
- Gibt es ein verbindliches ISMS (z. B. orientiert an ISO 27001 oder BSI-Grundschutz)?

Checkliste: Ist Ihr Unternehmen bereit?



Risikomanagement

- Gibt es ein aktuelles, dokumentiertes IT- und Cyberrisikomanagement?
- Sind die Risiken bewertet, priorisiert und mit Maßnahmen hinterlegt?
- Gibt es ein Verfahren zur regelmäßigen Neubewertung der Risiken?

Checkliste: Ist Ihr Unternehmen bereit?



Technische & organisatorische Sicherheitsmaßnahmen

- Erfüllen die Schutzmaßnahmen mindestens den „Stand der Technik“ gemäß NIS-2?
- Sind die Sicherheitsrichtlinien aktuell und verbindlich?

Checkliste: Ist Ihr Unternehmen bereit?

5



Lieferketten- & Dienstleistermanagement

- Werden die IT-Sicherheitsrisiken der Dienstleister und IT-Lieferanten bewertet?
- Sind Sicherheitsanforderungen und SLAs vertraglich festgelegt?
- Wird die Einhaltung dieser Vorgaben regelmäßig geprüft?

Checkliste: Ist Ihr Unternehmen bereit?



Incident Response und Meldewesen

- Gibt es ein dokumentiertes Notfall- und Incident-Response-Konzept?
- Ist das Unternehmen vorbereitet, um Sicherheitsvorfälle innerhalb von 24h/72h gemäß NIS-2 an die zuständige Behörde zu melden?
- Gibt es ein funktionierendes Monitoring zur Erkennung von Vorfällen?
- Sind alle relevanten Personen geschult und wissen, was im Ernstfall zu tun ist?

Checkliste: Ist Ihr Unternehmen bereit?

7



Kontinuität & Krisenmanagement

- Liegen dokumentierte und getestete Notfall- und Wiederanlaufpläne (BCM) vor?
- Sind Notfallprozesse regelmäßig geübt (z. B. Cyberangriff-Simulation)?
- Wie könnte im Krisenfall der Betrieb aufrechterhalten oder schnell wiederhergestellt werden?

Checkliste: Ist Ihr Unternehmen bereit?

8



Awareness & Schulungen

- Erhalten alle Mitarbeitenden regelmäßige Security-Awareness-Schulungen?
- Gibt es spezielle Trainings für kritische Rollen (Admin, Management, Incident-Team)?
- Werden die Schulungen dokumentiert und deren Wirksamkeit überprüft?

Checkliste: Ist Ihr Unternehmen bereit?

9



Dokumentation & Auditfähigkeit

- Ist die gesamte Sicherheitsorganisation prüfungsfest dokumentiert?
- Sind Policies, Prozesse, Schulungsnachweise und Risikoanalysen aktuell?
- Gibt es eine interne Kontrollfunktion oder regelmäßige Audits?

NIS-2- Gesetz in Deutschland

Zusammenfassung

NIS-2 bringt das Sicherheitsniveau für Unternehmen und öffentliche Einrichtungen auf **ein neues Level**.

Cybersicherheit wird zur **Führungspflicht**.

Der bisherige Geltungsbereich der Kritischen Infrastrukturen wird durch die Einführung der Kategorien „besonders wichtiger“ und „wichtiger Einrichtungen“ deutlich ausgeweitet – **mehr Organisationen** sind betroffen.

Das Gesetz **gilt sofort** ohne Übergangsfristen.





Falk Möller

Geschäftsführer

LÖSUNG|N

„Wir unterstützen unsere Kunden dabei, ihre **IT- und Cybersicherheitsstrukturen** zu **stärken** und wirksame Schutzmaßnahmen umzusetzen.

Mit dem nun in Deutschland beschlossenen NIS-2-Gesetz beginnt für viele Unternehmen eine **neue Phase der Verantwortung**.

Unser Anspruch ist es, unsere Kunden nicht nur technisch und organisatorisch optimal aufzustellen, sondern sie auch für die wachsenden Risiken zu sensibilisieren und eine **nachhaltige NIS-2-Konformität** sicherzustellen.“

www.loesung-n.de





LÖSUNG|N –
mehr Sicherheit.