NIS2-Beraterleitfaden

Ausgabe 2026

Vollständiger Leitfaden für die NIS2-Beratung bei KMU – inkl. Gap-Analyse-Vorlage und Musterrichtlinien.

ITSB Deutschland UG (haftungsbeschraenkt)
Tegernseer Landstr. 98, 81539 München
Version 2.0 | März 2026 | Vertraulich

Inhaltsverzeichnis

1. Einfuehrung in die NIS2-Richtlinie

Die NIS2-Richtlinie (Network and Information Security Directive 2) ist die überarbeitete EU-Richtlinie zur Netz- und Informationssicherheit. Sie ersetzt die ursprüngliche NIS-Richtlinie aus 2016 und erweitert den Anwendungsbereich erheblich.

Wichtige Eckdaten:

- In Kraft seit: 16. Januar 2023
- Umsetzungsfrist: 17. Oktober 2024 (verzögert in DE)
- Betroffene: ca. 30.000 Unternehmen in Deutschland
- Bussgelder: Bis zu 10 Mio. EUR oder 2% des weltweiten Umsatzes

Kernziele der NIS2:

- Harmonisierung der Cybersicherheitsanforderungen in der EU
- Erweiterung des Anwendungsbereichs auf mehr Sektoren
- Stärkung der Meldepflichten bei Sicherheitsvorfaellen
- Verschärfung der Sanktionen bei Nichtbeachtung
- Persönliche Haftung der Geschäftsführung

2. Wer ist betroffen?

NIS2 unterscheidet zwischen "wesentlichen" und "wichtigen" Einrichtungen. Die Einstufung basiert auf Sektor und Unternehmensgröße.

Sektoren mit hoher Kritikalität (Anhang I):

- Energie (Strom, Gas, Öl, Fernwärme, Wasserstoff)
- Verkehr (Luft, Schiene, Wasser, Strasse)
- Bankwesen und Finanzmarktinfrastrukturen •
  Gesundheitswesen
- Trinkwasser und Abwasser
- Digitale Infrastruktur und IT-Dienste
- Öffentliche Verwaltung
- • Weltraum

Sonstige kritische Sektoren (Anhang II):

- Post- und Kurierdienste
- • Abfallbewirtschaftung
- Chemie und Lebensmittel
- Verarbeitendes Gewerbe / Herstellung
- Digitale Dienste (Marktplätze, Suchmaschinen, soziale Netzwerke)
- • Forschungseinrichtungen

Größenkriterien:

Kategorie	Mitarbeitende	Umsatz/Bilanz	Einstufung
Grossunternehmen	> 250	> 50 Mio. EUR	Wesentlich
Mittleres Unternehmen	50 - 250	10 - 50 Mio. EUR	Wichtig
Kleine Unternehmen	< 50	< 10 Mio. EUR	Ggf. betroffen*

* Kleine Unternehmen können betroffen sein, wenn sie als kritisch eingestuft werden.

3. Anforderungen im Überblick

NIS2 definiert 10 Kernmassnahmen, die betroffene Unternehmen umsetzen müssen:

1. Risikoanalyse & Sicherheitskonzepte

Systematische Identifikation und Bewertung von Cyberrisiken, Erstellung von Sicherheitsrichtlinien.

2. Incident Management

Prozesse zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen (Meldepflicht: 24h/72h).

3. Business Continuity

Backup-Management, Disaster Recovery, Krisenmanagement und Notfallpläne.

4. Supply Chain Security

Sicherheitsanforderungen für Lieferanten und Dienstleister, Vertragliche Regelungen.

5. Sicherheit bei Beschaffung

Sicherheitsanforderungen bei Einkauf, Entwicklung und Wartung von IT-Systemen.

6. Wirksamkeitsprüfung

Regelmässige Audits, Penetrationstests und Bewertung der Sicherheitsmaßnahmen.

7. Cyberhygiene & Schulung

Awareness-Programme, Schulungen für Mitarbeitende und Führungskräfte.

8. Kryptografie

Einsatz von Verschlüsselung und kryptografischen Verfahren wo erforderlich.

9. Zugangsmanagement

Multi-Faktor-Authentifizierung, Zugriffskontrolle, Identitätsmanagement.

10. Kommunikationssicherheit

Sichere Kommunikationswege, Notfallkommunikation.

4. Der Beratungsprozess

Als ITSB-Partner begleitest du Kunden durch den gesamten NIS2-Compliance-Prozess. Hier ist der empfohlene Ablauf:

Phase 1: Erstgespräch & Betroffenheitsanalyse (Woche 1)

- Branche und Unternehmensgröße erfassen
- Betroffenheit nach NIS2 prüfen (Anhang I/II)
- Einstufung als "wesentlich" oder "wichtig"
- Scope und Erwartungen klären

Phase 2: Gap-Analyse (Woche 2-3)

- IST-Zustand der IT-Sicherheit erfassen
- Abgleich mit NIS2-Anforderungen
- Identifikation von Lücken und Risiken
- Priorisierung der Handlungsfelder

Phase 3: Maßnahmenplanung (Woche 4-5)

- Konkreten Massnahmenplan erstellen
- Verantwortlichkeiten zuweisen
- Zeitrahmen und Meilensteine definieren
- Budget und Ressourcen schätzen

Phase 4: Implementierung (Woche 6-12)

- Technische Massnahmen umsetzen
- Richtlinien und Prozesse einführen
- Schulungen durchführen
- Dokumentation erstellen

Phase 5: Audit & Zertifizierung (Woche 13)

- Interne Auditierung der Maßnahmen
- Dokumentation prüfen und finalisieren
- Meldeprozesse testen
- Abschlussbericht und Empfehlungen

5. Gap-Analyse: Schritt für Schritt

Die Gap-Analyse ist das Herzstück der NIS2-Beratung. Verwende die separate "NIS2 Gap-Analyse Checkliste" für die detaillierte Durchführung. Hier die Kernbereiche:

- Governance & Organisation (Verantwortlichkeiten, Rollen, Berichtswege)
- Risikomanagement (Methodik, Durchführung, Dokumentation)
- Incident Management (Erkennung, Meldung, Reaktion, Nachbereitung)
- Business Continuity (Backup, Recovery, Notfallplüne)
- Supply Chain (Lieferantenbewertung, Verträge, Monitoring)
- Technische Sicherheit (Netzwerk, Endpunkte, Cloud, Verschlüsselung)
- Zugangsmanagement (IAM, MFA, Berechtigungskonzept)
- Awareness & Schulung (Programme, Frequenz, Dokumentation)

Bewertungsschema:

Stufe	Beschreibung	Handlungsbedarf
0 - Nicht vorhanden	Kein Prozess/Massnahme	Kritisch
1 - Initial	Ad-hoc, nicht dokumentiert	Hoch
2 - Wiederholbar	Dokumentiert, nicht durchgängig	Mittel
3 - Definiert	Standardisiert, dokumentiert	Gering
4 - Gesteuert	Gemessen, kontrolliert	Optimierung
5 - Optimiert	Kontinuierliche Verbesserung	Keine

Hinweis: Die vollständige Gap-Analyse-Checkliste mit 45 Pruefpunkten steht als separates Dokument im Partner-Portal bereit.