NIS2-Umsetzung in Unternehmen

Anforderungen, Vorgehen und praktische Umsetzung

amerdis
CONSULTING & IT-SOLUTIONS

Es besteht sofortiger Handlungs-bedarf, ohne Übergangsfrist

Mit dem NIS2-Umsetzungsgesetz gelten verbindliche europäische Sicherheitsstandards ohne Übergangsfristen.

Rund 30.000 Unternehmen in Deutschland müssen jetzt handeln: Verschärfte Meldepflichten und die persönliche Haftung der Geschäftsführung **machen Cybersicherheit zum zentralen Compliance-Thema.**

Seit dem **6.12.2025** gelten die Registrierungs- und Meldepflichten sowie die Geschäftsführerhaftung.

Innerhalb von **3 Monaten (6. März 2026)** mussten sich betroffene Unternehmen beim BSI registrieren.

Innerhalb von **2 Jahren (bis Dezember 2027)** ist der Nachweis der Sicherheitsmaßnahmen zu erbringen.

Welche Pflichten bringt NIS2 für Unternehmen mit sich?

NIS2 verpflichtet betroffene Unternehmen, ein angemessenes Niveau an Cyber- und Informationssicherheit sicherzustellen.

Dabei stehen nicht einzelne Maßnahmen im Fokus, sondern ein systematischer, risikobasierter Ansatz zur Prävention, Erkennung und Behandlung von Sicherheitsvorfällen.

Risikomanagement und Sicherheitsmaßnahmen

Unternehmen müssen technische und organisatorische Maßnahmen einführen, um Risiken für Netz- und Informationssysteme angemessen zu beherrschen.

Meldepflichten bei Sicherheitsvorfällen

Erhebliche Sicherheitsvorfälle sind innerhalb enger Fristen an das BSI zu melden und nachvollziehbar zu dokumentieren.

(Frühwarnmeldung innerhalb von 24 Stunden, detaillierte Vorfallmeldung innerhalb von 72 Stunden und Abschlussbericht spätestens nach einem Monat.)

Organisatorische Verantwortung und Governance

Klare Zuständigkeiten, Entscheidungswege und die Einbindung der Geschäftsführung sind verbindlich sicherzustellen.

Nachweis- und Prüfungspflichten

Unternehmen müssen die Umsetzung der Anforderungen dokumentieren und auf Anforderung gegenüber Aufsichtsbehörden nachweisen können.

Welche Risiken bringt NIS2 für Unternehmen mit sich?

NIS2 erhöht nicht nur die Anforderungen an Cybersicherheit, sondern auch die Risiken bei unzureichender Umsetzung deutlich.

Ein strukturiertes Vorgehen reduziert Risiken und schafft Sicherheit für Organisation und Management. NIS2 macht Cybersicherheit zu einem zentralen Risiko- & Management-thema.

- **Hohe Bußgelder und behördliche Maßnahmen**

  Bußgelder bis zu 10 Mio. € oder bis zu 2 % des weltweiten Jahresumsatzes sowie verbindliche Anordnungen der Aufsichtsbehörden.

- **Erhöhte Verantwortung der Geschäftsleitung und mögliche persönliche Haftungsrisiken.**
- **Betriebsunterbrechungen und Versorgungsausfälle**
- **Reputationsschäden und Vertrauensverlust**
- **Extremer Zeitdruck im Sicherheitsvorfall**

NIS2 Umsetzung auf Basis einer etablierten Zusammenarbeit

amerdis begleitet Klienten seit Jahren im Bereich Cyber Security bzw. Datenschutz und kann diese Erfahrung gezielt auf die NIS2-Umsetzung übertragen.

Wir kennen Strukturen, Prozesse und Entscheidungswege bereits. **Heißt:**

- ✓ **Aufbau auf Bestehendem statt Neuanalyse**
- ✓ **Weniger Abstimmungsaufwand**
- ✓ **Kürzere Einarbeitung**

amerdis kann unterstützen bei:

Betroffenheit und Pflichten klären

Wir prüfen die NIS2-Betroffenheit, definieren konkrete Pflichten und schaffen eine verlässliche Entscheidungs-grundlage für Management und Compliance.

Umsetzung und Integration begleiten

Wir integrieren Informationssicherheits-, Risiko- und Meldeprozesse passgenau in bestehende Strukturen und Governance.

Betrieb und Absicherung

Wir etablieren technische und organisatorische Maßnahmen und sichern Handlungsfähigkeit sowie Nachweise auch im Ernstfall.

Konkrete Umsetzung Roadmap

Die Umsetzung von NIS2 ist kein einmaliges Projekt, sondern ein strukturierter Veränderungsprozess.

Mit einem klar definierten Vorgehen lassen sich Anforderungen systematisch erfassen, umsetzen und **dauerhaft im Betrieb verankern.**

amerdis unterstützt bei der strukturierten Umsetzung mit einem vierstufigen Fahrplan:

1. **Betroffenheit prüfen & BSI-Registrierung**
2. **Bestandsaufnahme & Gap-Analyse**
3. **Priorisierung, Planung & Umsetzung**
4. **Kontinuierliche Überprüfung & Anpassung**

1 Betroffenheit & BSI-Registrierung

Nach der Klärung der Betroffenheit folgt die strukturierte Vorbereitung der gesetzlichen Pflichten und der formalen Registrierung beim BSI.

- ✓ **Festlegung der NIS2-Rolle**
  - Einordnung als Essential oder Important Entity
  - Abgrenzung der betroffenen Organisationseinheiten & Leistungen
- ✓ **Benennung zentraler Ansprechpartner**
  - Festlegung der verantwortlichen Kontaktstelle für das BSI
  - Definition von Vertretungen und Eskalationswegen
  - Abstimmung Geschäftsführung, IT und Compliance
- ✓ **Zusammenstellung der Registrierungsinformationen**
  - Rechtliche Unternehmensdaten
  - Beschreibung der wesentlichen Dienstleistungen
  - Zuordnung zu Sektor und Untersektor nach NIS2
- ✓ **Vorbereitung der Melde- und Kommunikationsfähigkeit**
  - Definition interner Meldewege für Sicherheitsvorfälle
  - Sicherstellung der Erreichbarkeit innerhalb der gesetzlichen Fristen
  - Abstimmung technischer und organisatorischer Zuständigkeiten
- ✓ **Durchführung der Registrierung beim BSI**
  - Strukturierte Registrierung im BSI Portal
  - Dokumentation der Angaben als Compliance Nachweis

2 Bestandsaufnahme & Gap-Analyse

In Phase 2 wird der aktuelle Stand der Informationssicherheit systematisch erfasst und mit den Anforderungen aus NIS2 abgeglichen.

✓ Aufnahme bestehender Sicherheitsmaßnahmen

- Erfassung bestehender technischer & organisatorischer Maßnahmen
- Berücksichtigung bestehender Datenschutz, IT Sicherheits- und Governance-Strukturen

✓ Analyse relevanter Systeme und Prozesse

- Identifikation kritischer IT-Systeme, Anwendungen und Dienstleister
- Bewertung der Abhängigkeiten für den operativen Betrieb und die Versorgungssicherheit

✓ Abgleich mit NIS2-Anforderungen

- Systematischer Vergleich des Ist Zustands mit den gesetzlichen Mindestanforderungen
- Berücksichtigung von Meldepflichten, Risikomanagement und Nachweispflichten

✓ Identifikation von Handlungsbedarfen

- Transparente Darstellung bestehender Lücken und Risiken
- Priorisierung nach Kritikalität, Aufwand und Risiko

✓ Ergebnisdokumentation als Entscheidungsgrundlage

- Klar strukturierte Gap Analyse als Basis für Management Entscheidungen
- Grundlage für die zielgerichtete Umsetzung in Phase 3

3 Priorisierung, Planung & Umsetzung

In Phase 3 werden die identifizierten Handlungsbedarfe priorisiert umgesetzt und organisatorisch sowie technisch verankert: Aufbau eines NIS2-konformes Management-systems/ISMS.

- ✓ **Priorisierung der Maßnahmen**
  - Ableitung konkreter Maßnahmen aus der Gap Analyse
  - Priorisierung nach Risiko, Kritikalität und Umsetzbarkeit
  - Abstimmung mit Geschäftsführung, IT und Fachbereichen
- ✓ **Umsetzung technischer Maßnahmen**
  - Einführung oder Anpassung technischer Sicherheitsmaßnahmen
  - Absicherung kritischer Systeme, Zugänge und Schnittstellen
  - Berücksichtigung bestehender IT und Sicherheitsarchitekturen
- ✓ **Umsetzung organisatorischer Maßnahmen**
  - Definition und Einführung von Richtlinien, Prozessen und Verantwortlichkeiten
  - Etablierung von Risiko-, Melde- und Eskalationsprozessen
  - Anbindung an bestehende Governance- und Datenschutzstrukturen
- ✓ **Integration in den operativen Betrieb**
  - Verankerung der Maßnahmen im Tagesgeschäft
  - Sicherstellung der praktischen Anwendbarkeit und Akzeptanz
  - Schulung relevanter Rollen und Funktionen
- ✓ **Dokumentation und Nachweisführung**
  - Aufbau einer konsistenten und prüffähigen Dokumentation
  - Vorbereitung auf Prüfungen, Nachfragen und Meldepflichten

4 Kontinuierliche Überprüfung und Anpassung

In Phase 4 werden die umgesetzten Maßnahmen dauerhaft betrieben, überwacht und kontinuierlich weiterentwickelt.

- ✓ **Etablierung des Regelbetriebs**
  - Überführung der Sicherheitsmaßnahmen in den operativen Alltag
  - Klare und feste Abläufe für Betrieb und Überwachung
- ✓ **Umgang mit Sicherheitsvorfällen**
  - Anwendung der definierten Melde und Eskalationsprozesse
  - Sicherstellung fristgerechter Kommunikation mit dem BSI
  - Strukturierte Nachbereitung und Lessons Learned
- ✓ **Kontinuierliche Überprüfung und Verbesserung**
  - Regelmäßige Überprüfung von Risiken, Maßnahmen und Prozessen
  - Anpassung an neue Bedrohungen und regulatorische Änderungen
- ✓ **Nachweis und Prüfungssicherheit**
  - Pflege einer aktuellen und prüffähigen Dokumentation
  - Vorbereitung auf Audits, Prüfungen und behördliche Anfragen
- ✓ **Sensibilisierung und Befähigung der Organisation**
  - Regelmäßige Schulungen und Awareness Maßnahmen
  - Stärkung der Sicherheitskultur im Unternehmen

Empfehlung: Nutzung eines geeigneten NIS2/ISMS-Tools zur strukturierten Unterstützung und zur laufenden Steuerung, Dokumentation und kontinuierlichen Verbesserung.

Warum bei der NIS2-Einführung der Aufbau eines ISMS und die Nutzung eines geeigneten Tools sinnvoll ist?

NIS2 verlangt kein Zertifikat, wohl aber ein dauerhaft wirksames Sicherheitsmanagement.

Der strukturierte Aufbau eines ISMS und die Unterstützung durch ein geeignetes Tool helfen, die gesetzlichen Anforderungen effizient, nachvollziehbar und nachhaltig umzusetzen.

- NIS2 lässt sich nicht mit Einzelmaßnahmen erfüllen. Ein ISMS schafft Ordnung, Priorisierung und einen klaren Rahmen für alle Sicherheitsanforderungen.
- **Auf Knopfdruck:** Ein ISMS mit Tool macht Risiken, Maßnahmen und Verantwortlichkeiten jederzeit transparent, steuerbar und prüffähig gegenüber Management und Aufsicht.
- Ein etabliertes ISMS reduziert manuellen Aufwand, stabilisiert den Betrieb und trägt regulatorische Anforderungen auch über NIS2 hinaus.

Ohne ISMS-Tool

- Hoher manueller Aufwand durch Excel Listen
- verteilte Dokumente
- E-Mail-Abstimmungen
- Medienbrüche bei Nachweisen, Maßnahmen und Meldungen
- Keine sichere Versionierung

Grundlegende NIS2-Compliance erreichbar, jedoch begrenzt stabil und aufwendig im Betrieb; Richtwert ca. 60–70 %

Mit ISMS-Tool

- ✓ Zentrale Pflege von Risiken, Maßnahmen, Verantwortlichkeiten, Nachweisen und Dokumentation
- ✓ Automatisierte Workflows
- ✓ Erinnerungen und konsistente Strukturen
- ✓ Reduktion des laufenden Pflege- und Dokumentationsaufwands um ca. 30–50 %
- ✓ Deutlich geringerer Abstimmungsaufwand zwischen IT, Compliance und Management
- ✓ Weniger Nacharbeit bei Prüfungen, Vorfällen und Meldungen

---

Reduziert den laufenden Dokumentations- und Koordinationsaufwand erfahrungsgemäß um ca. 30–50 %. Deutlich höherer und dauerhaft stabiler Compliancegrad Richtwert ab ca. 80 %

Zeitplanung

Phase 1: Einordnung und Registrierung
ca. 1 Monat

Phase 2: Bestandsaufnahme & Gap Analyse
ca. 2-3 Monate

Phase 3: Umsetzung und Verankerung
ca. 4-12 Monate

Phase 4: Betrieb und Absicherung
laufend

Gesamtdauer bis zur belastbaren Grundumsetzung ca. 6 bis 12 Monate

Ressourcenplanung

Intern:

- **Management und Geschäftsführung**
  Setzt Prioritäten, trifft Entscheidungen und trägt die Verantwortung für die NIS2-Umsetzung.
- **Interne Fachbereiche und IT**
  Setzen Maßnahmen fachlich um und integrieren sie in den operativen Betrieb.

Extern:

- **amerdis als Umsetzungspartner**
  Strukturiert den Gesamtprozess, sorgt für Umsetzungssicherheit und entlastet interne Ressourcen.
- **ISMS-Tool**
  Zentrale Steuerung und Dokumentation bei deutlich reduziertem manuellem Aufwand.

Abhängig von Unternehmensgröße und Reifegrad der Informationssicherheit

Warum viele Unternehmen mit NIS2 aktuell überfordert sind:

Unklare Betroffenheit

- Viele Unternehmen wissen nicht, ob und in welchem Umfang sie unter die NIS2-Regulierung fallen.

Fehlende Ressourcen

- IT- und Fachbereiche sind bereits stark ausgelastet.

Komplexe Anforderungen

- NIS2 betrifft IT-Sicherheit, Governance, Meldepflichten und Dokumentation.

Hoher Abstimmungsbedarf

- Geschäftsführung, IT und Compliance müssen eng zusammenarbeiten.

Zeitdruck

- Die Umsetzung erfordert strukturierte Prozesse und klare Verantwortlichkeiten.

Warum amerdis der richtige Umsetzungspartner ist:

Strukturiertes Vorgehensmodell
- Klare Schritte von Betroffenheitsprüfung über Gap-Analyse bis zur Umsetzung.

Praxisorientierte Integration
- Einbindung der Maßnahmen in bestehende IT-, Compliance- und Governance-Strukturen.

Entlastung interner Ressourcen
- Unterstützung bei Planung, Umsetzung und Dokumentation.

Interimsmäßige Unterstützung
- Bei Ressourcenengpässen können Aufgaben temporär übernommen werden.

Nachweisbare Compliance
- Aufbau prüffähiger Dokumentation und Vorbereitung auf behördliche Anforderungen.

amerdis
CONSULTING & IT-SOLUTIONS

amerdis GmbH
Wienburgstraße 207
48159 Münster

Tel: 0251-489 5700

info@amerdis.de
www.amerdis.de

nis2.amerdis.de