NIS2 und ISO 27001

Warum Unternehmen ihre Informationssicherheit jetzt neu bewerten sollten.

Einordnung für Unternehmen mit bestehendem ISMS.

amerdis

CONSULTING & IT-SOLUTIONS

Inhalt

1. Einleitung 3

2. ISO 27001 als Grundlage für Informationssicherheit 3

3. Warum NIS2 über ISO 27001 hinausgeht 4

4. Zentrale Unterschiede zwischen ISO 27001 und NIS2 5

5. Typische Anforderungen der NIS2-Richtlinie 5

   5.1 Risikomanagement 5
   5.2 Sicherheitsrichtlinien und Governance 5
   5.3 Vorfallmanagement 5
   5.4 Meldepflichten 5
   5.5 Lieferkettenrisiken 5
   5.6 Business Continuity 5
   5.7 Schulung und Awareness 5

6. Typische NIS2-Lücken bei Unternehmen mit ISO 27001 6

7. Erste Schritte zur Umsetzung von NIS2 6

8. Fazit 6

Unterstützung bei der Umsetzung 7

1. Einleitung

Mit der NIS2-Richtlinie hat die Europäische Union einen neuen regulatorischen Rahmen für Cybersicherheit geschaffen. Ziel der Richtlinie ist es, die Widerstandsfähigkeit von Unternehmen und Organisationen gegenüber Cyberangriffen deutlich zu erhöhen und gleichzeitig ein einheitliches Sicherheitsniveau innerhalb der EU zu etablieren.

Während bisher vor allem Betreiber kritischer Infrastrukturen im Fokus regulatorischer Anforderungen standen, betrifft die NIS2-Richtlinie künftig deutlich mehr Unternehmen. In Deutschland wird davon ausgegangen, dass mehrere zehntausend Organisationen unter die neuen Vorgaben fallen können.

Für viele Unternehmen stellt sich daher aktuell die Frage, wie sie die Anforderungen der NIS2-Richtlinie praktisch umsetzen können und welche bestehenden Sicherheitsmaßnahmen bereits einen Teil der Anforderungen abdecken.

Ein häufiger Ausgangspunkt ist dabei ein bereits etabliertes Informationssicherheitsmanagementsystem nach ISO 27001.

2. ISO 27001 als Grundlage für Informationssicherheit

Die internationale Norm ISO 27001 ist einer der weltweit etabliertesten Standards für Informationssicherheitsmanagement. Sie beschreibt, wie Unternehmen ein strukturiertes Managementsystem für den Schutz von Informationen aufbauen und kontinuierlich verbessern können.

Ein ISMS nach ISO 27001 umfasst unter anderem:

- ✓ systematisches Risikomanagement
- ✓ Sicherheitsrichtlinien und organisatorische Maßnahmen
- ✓ technische Schutzmaßnahmen
- ✓ Prozesse für Sicherheitsvorfälle
- ✓ Schulungs- und Awarenessprogramme
- ✓ kontinuierliche Verbesserung der Sicherheitsmaßnahmen

Unternehmen mit einem funktionierenden ISMS verfügen daher bereits über eine wichtige Grundlage für den Umgang mit Cyberrisiken.

Dennoch ersetzt eine ISO 27001-Zertifizierung keine regulatorische Prüfung nach NIS2.

Diese Matrix zeigt typische NIS2-spezifische Ergänzungen, die ISO 27001 oft nicht vollständig abdeckt:

NIS2 Anforderung	ISO 27001 Abdeckung	Typische Lücke	Maßnahmen
Incident Reporting an Behörden	teilweise	Meldefristen (24h/72h) fehlen	Meldeprozess definieren
Management Liability	gering	Vorstandshaftung nicht explizit geregelt	Governance & Reporting an Vorstand
Nationale Behördenkommunikation	gering	keine regulatorische Schnittstelle	Kontaktstelle definieren
Supply Chain Risikoanalyse	mittel	oft nur Vertragsprüfung	Cyber-Risikobewertung von Lieferanten
Cyber Crisis Management	mittel	Fokus auf IT-BCM	Krisenmanagement inkl. Kommunikation
Registrierung bei Behörden	keine	organisatorisch neu	Compliance Prozess
Nationale Sicherheitsanforderungen	gering	ISO ist international	Mapping zu nationaler NIS2 Umsetzung

3. Warum NIS2 über ISO 27001 hinausgeht

Die NIS2-Richtlinie verfolgt einen anderen Ansatz als klassische Sicherheitsstandards. Während ISO 27001 in erster Linie ein freiwilliger Managementstandard ist, handelt es sich bei NIS2 um eine gesetzliche Regulierung mit verbindlichen Anforderungen.

Das bedeutet, dass Unternehmen nicht nur geeignete Sicherheitsmaßnahmen implementieren müssen, sondern diese auch gegenüber Behörden nachweisen können müssen.

Darüber hinaus enthält NIS2 zusätzliche Anforderungen, die über die klassischen Strukturen eines Informationssicherheitsmanagementsystems hinausgehen.

Dazu gehören insbesondere:

- ✓ gesetzlich definierte Meldepflichten für Sicherheitsvorfälle
- ✓ stärkere Verantwortung der Geschäftsleitung
- ✓ Anforderungen an die Sicherheit von Lieferketten und Dienstleistern
- ✓ staatliche Aufsicht und mögliche Prüfungen
- ✓ mögliche Sanktionen bei Verstößen gegen regulatorische Vorgaben

Unternehmen müssen daher prüfen, ob ihr bestehendes Sicherheitskonzept auch diese regulatorischen Anforderungen abdeckt.

4. Zentrale Unterschiede zwischen ISO 27001 und NIS2

Die beiden Ansätze verfolgen unterschiedliche Zielsetzungen.

ISO 27001 beschreibt einen internationalen Managementstandard für Informationssicherheit. Unternehmen können sich freiwillig nach diesem Standard zertifizieren lassen, um ihre Sicherheitsorganisation strukturiert aufzubauen und zu betreiben.

Die NIS2-Richtlinie hingegen stellt einen regulatorischen Rahmen dar. Sie verpflichtet bestimmte Unternehmen dazu, definierte Sicherheitsmaßnahmen umzusetzen und bestimmte organisatorische Anforderungen zu erfüllen.

Ein weiterer Unterschied besteht in der Aufsicht. Während ISO 27001 im Rahmen von Zertifizierungen durch Auditoren geprüft wird, unterliegt die Einhaltung der NIS2-Vorgaben staatlicher Aufsicht. Verstöße gegen regulatorische Anforderungen können daher mit behördlichen Maßnahmen oder Bußgeldern verbunden sein.

5. Typische Anforderungen der NIS2-Richtlinie

Die NIS2-Richtlinie verlangt von betroffenen Unternehmen eine Reihe organisatorischer und technischer Maßnahmen zur Verbesserung ihrer Cybersicherheit.

Zu den zentralen Anforderungen gehören unter anderem:

5.1 Risikomanagement

Unternehmen müssen Risiken für ihre Informationssysteme systematisch identifizieren, bewerten und geeignete Maßnahmen zur Risikominimierung umsetzen.

5.2 Sicherheitsrichtlinien und Governance

Die Informationssicherheit muss organisatorisch klar verankert sein. Dazu gehört auch die Einbindung der Unternehmensleitung in zentrale Entscheidungen zur Cybersicherheit.

5.3 Vorfallmanagement

Unternehmen müssen über Prozesse verfügen, um Sicherheitsvorfälle zu erkennen, zu bewerten und angemessen darauf zu reagieren.

5.4 Meldepflichten

Bestimmte Sicherheitsvorfälle müssen innerhalb definierter Fristen an zuständige Behörden gemeldet werden.

5.5 Lieferkettenrisiken

Auch Risiken, die durch Dienstleister oder externe Partner entstehen, müssen berücksichtigt werden.

5.6 Business Continuity

Unternehmen müssen sicherstellen, dass kritische Prozesse auch im Falle eines Cybervorfalls weitergeführt werden können.

5.7 Schulung und Awareness

Mitarbeitende müssen regelmäßig für Cyberrisiken sensibilisiert werden.

6. Typische NIS2-Lücken bei Unternehmen mit ISO 27001

Unternehmen mit bestehendem ISMS verfügen häufig bereits über viele organisatorische und technische Sicherheitsmaßnahmen. Dennoch zeigen erste Analysen, dass in der Praxis häufig bestimmte regulatorische Aspekte fehlen.

Dazu gehören beispielsweise:

- ✓ keine formale Betroffenheitsanalyse im Kontext von NIS2
- ✓ fehlende Prozesse für behördliche Vorfallmeldungen
- ✓ unklare Verantwortlichkeiten der Geschäftsleitung
- ✓ unzureichende Bewertung von Lieferkettenrisiken
- ✓ fehlende Dokumentation regulatorischer Anforderungen

Diese Punkte führen dazu, dass Unternehmen ihre bestehende Sicherheitsorganisation gezielt erweitern müssen.

7. Erste Schritte zur Umsetzung von NIS2

Für Unternehmen empfiehlt sich ein strukturiertes Vorgehen bei der Umsetzung der neuen Anforderungen.

Ein möglicher Ansatz umfasst mehrere Schritte:

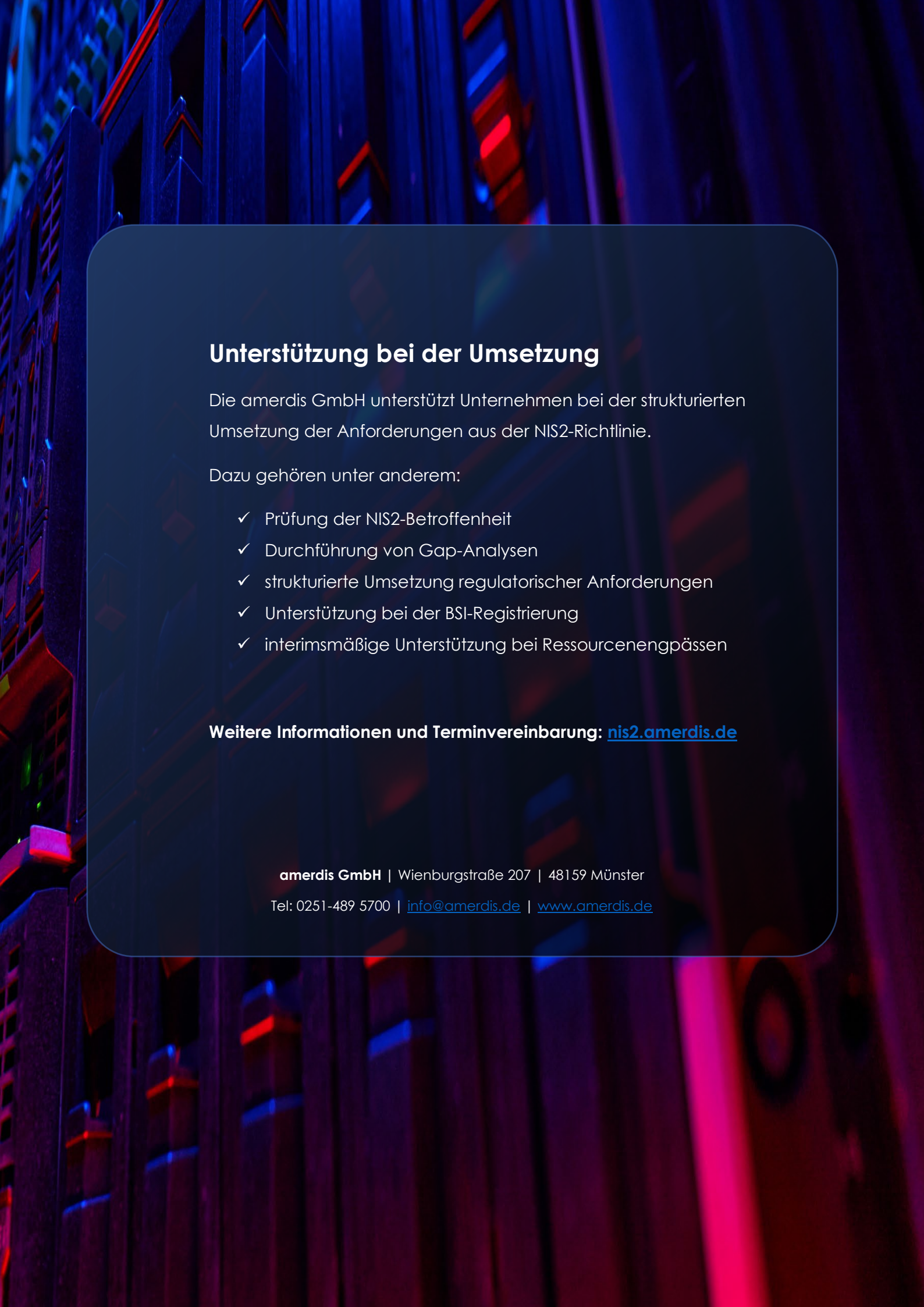
1. Zunächst sollte geprüft werden, ob das eigene Unternehmen unter den Anwendungsbereich der NIS2-Richtlinie fällt.
2. Anschließend empfiehlt sich eine Analyse der bestehenden Sicherheitsorganisation. Dabei wird überprüft, welche Maßnahmen bereits vorhanden sind und wo mögliche Lücken bestehen.
3. Auf dieser Grundlage kann eine sogenannte Gap-Analyse durchgeführt werden, um konkrete Handlungsfelder zu identifizieren.
4. Im nächsten Schritt werden die erforderlichen Maßnahmen priorisiert und schrittweise umgesetzt.
5. Dabei kann es sinnvoll sein, bestehende Strukturen eines Informationssicherheitsmanagementsystems zu nutzen und gezielt um regulatorische Anforderungen zu erweitern.

8. Fazit

Die ISO 27001 bietet eine sehr gute Grundlage für den strukturierten Umgang mit Informationssicherheit. Für Unternehmen, die unter die NIS2-Richtlinie fallen, reicht sie jedoch allein nicht aus.

Die regulatorischen Anforderungen der NIS2-Richtlinie gehen über klassische Managementstandards hinaus und erfordern zusätzliche organisatorische Maßnahmen sowie klare Prozesse im Umgang mit Sicherheitsvorfällen.

Eine strukturierte Analyse hilft Unternehmen dabei, bestehende Sicherheitsmaßnahmen mit regulatorischen Anforderungen abzugleichen und mögliche Lücken zu identifizieren.



Unterstützung bei der Umsetzung

Die amerdis GmbH unterstützt Unternehmen bei der strukturierten Umsetzung der Anforderungen aus der NIS2-Richtlinie.

Dazu gehören unter anderem:

- ✓ Prüfung der NIS2-Betroffenheit
- ✓ Durchführung von Gap-Analysen
- ✓ strukturierte Umsetzung regulatorischer Anforderungen
- ✓ Unterstützung bei der BSI-Registrierung
- ✓ interimsmäßige Unterstützung bei Ressourcenengpässen

Weitere Informationen und Terminvereinbarung: nis2.amerdis.de

amerdis GmbH | Wienburgstraße 207 | 48159 Münster

Tel: 0251-489 5700 | info@amerdis.de | www.amerdis.de