
DEKRA
002
Data Security
004
NIS2

Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) im Überblick

Ein Leitfaden für NIS-2-Umsetzungsgesetz (NIS2UmsuCG) -Compliance und erhöhte Cyber-Resilienz

Whitepaper NIS2

1. Einleitung: Eine neue Ära der Cybersicherheitspflichten

Die überarbeitete EU-Richtlinie zur Netz- und Informationssicherheit (NIS2) stellt einen bedeutenden Fortschritt in der Cybersicherheitsstrategie der Europäischen Union dar. In Deutschland werden die Vorgaben durch das NIS2UmsuCG insbesondere über das reformierte BSI-Gesetz (BSIG) konkret umgesetzt. Artikel 1 des NIS2UmsuCG regelt dabei ausdrücklich die Umsetzung der NIS2-Anforderungen im BSI-Gesetz und definiert somit den gesetzlichen Rahmen für die Anpassungen im deutschen Recht. Für viele Organisationen bedeutet dies, dass Cybersicherheit nicht mehr nur eine bewährte Praxis (Best Practice) ist, sondern eine gesetzliche Verpflichtung – inklusive strenger Meldepflichten und erheblicher Sanktionen bei Nichteinhaltung. Dieses Whitepaper gibt einen Überblick über die zentralen Aspekte des NIS2UmsuCG und skizziert einen strategischen Ansatz, um Compliance zu erreichen und dauerhaft sicherzustellen.

2. Erweiterter Anwendungsbereich: Wer fällt unter NIS2UmsuCG?

Ein zentrales Ziel des NIS2UmsuCG ist die Ausweitung des Geltungsbereichs. Die bisherige Unterscheidung zwischen Betreibern wesentlicher Dienste und digitalen Dienstleistern entfällt. Der Kreis der betroffenen Organisationen im BSIG u. a. wird über die Kategorien besonders wichtige Einrichtungen und wichtige Einrichtungen (sowie weitere Gruppen wie Betreiber kritischer Anlagen) abgebildet. Die sektorale Zuordnung orientiert sich an den gesetzlichen Aufzählungen, insbesondere Anlage 1 BSIG:

- **Besonders wichtige Einrichtungen:** Sektoren, die für Gesellschaft und Wirtschaft kritisch sind, z. B. Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur sowie Weltraum (Details und Abgrenzung gemäß Anlage 1 BSIG).

- **Wichtige Einrichtungen:** Weitere zentrale Bereiche wie Post- und Kurierdienste, Abfallwirtschaft, Verarbeitendes Gewerbe/Herstellung von Waren, chemische Industrie, Lebensmittelproduktion und -vertrieb sowie bestimmte Forschungs- und Digitalbereiche (Details und Abgrenzung gemäß Anlage 2 BSIG).

Die Einstufung richtet sich nach Sektor und Unternehmensgröße sowie nach gesetzlich definierten Ausnahmen. In vielen Fällen sind in erster Linie mittlere und große Unternehmen erfasst (typischerweise ab 50 Beschäftigten oder 10 Mio. € Jahresumsatz bzw. Bilanzsumme). Je nach Einrichtungsart kann die Betroffenheit jedoch auch unabhängig von klassischen Schwellenwerten greifen. Maßgeblich sind in Deutschland die konkreten Definitionen und Zuordnungen im BSIG (u. a. über Anlage 1) sowie die dazugehörigen Pflichten (z. B. Registrierung und Meldewesen gegenüber den zuständigen Stellen).

3. Der Kern der Compliance: Wichtige Managementmaßnahmen

Die Anforderungen an das Cybersicherheits-Risikomanagement sind im Kern durch das NIS2UmsuCG konkretisiert (insbesondere § 30 ff. BSIG). Diese Vorgaben verpflichten betroffene Einrichtungen, technische und organisatorische Maßnahmen umzusetzen, die angemessen und verhältnismäßig zum Risiko sind. Dazu gehören insbesondere:

1. **Richtlinien zur Risikoanalyse und Sicherheit von Informationssystemen:** Implementierung formeller Prozesse zur Identifizierung, Bewertung und Minderung von Risiken.

2. **Incident Handling:** Etablierung von robusten Verfahren zur Erkennung, Reaktion und Wiederherstellung von Sicherheitsvorfällen.

3. **Geschäftskontinuität (Business Continuity) und Krisenmanagement:** Sicherstellung der Betriebsfähigkeit durch effektive Backup-Strategien, Disaster-Recovery-Pläne und Krisenmanagementprotokolle.

4. **Lieferkettensicherheit:** Management von Cybersicherheitsrisiken innerhalb der Lieferkette und in Beziehungen zu Dienstleistern.

5. **Schwachstellenmanagement:** Implementierung von Prozessen zur Behandlung und Offenlegung von Schwachstellen in Systemen.

6. **Wirksamkeitsbewertung:** Regelmäßige Tests und Bewertungen der Wirksamkeit von Cybersicherheitsmaßnahmen.

7. **Cyber-Hygiene und Schulungen:** Förderung grundlegender Sicherheitspraktiken und regelmäßige Mitarbeiterschulungen.

8. **Kryptografie:** Einsatz von Verschlüsselung und kryptografischen Kontrollen, wo notwendig, zum Schutz von Daten.

9. **Mitarbeitersicherheit:** Anwendung von Richtlinien zur Zugangskontrolle und sicherem Asset-Management.

10. **Multi-Faktor-Authentifizierung (MFA) und sichere Kommunikation:** Einsatz von MFA und Schutz interner Kommunikation.

4. Strenge Meldepflichten und Management-Verantwortung

Das NIS2UmsuCG sieht strenge und zeitnahe Meldepflichten vor. Besonders wichtige Einrichtungen und wichtige Einrichtungen müssen erhebliche Sicherheitsvorfälle an die vom BSI (Bundesamt für Sicherheit in der Informationstechnik) und dem BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) eingerichtete gemeinsame Meldestelle melden. Die Meldung erfolgt gestuft: eine Frühwarnung innerhalb von 24 Stunden nach Kenntnis, anschließend eine Meldung innerhalb von 72 Stunden mit einer ersten Bewertung (u. a. Schweregrad und Auswirkungen). Gegebenenfalls sind Zwischenberichte erforderlich. Ein Abschlussbericht ist grundsätzlich innerhalb eines Monats vorzulegen.
Die Vorgaben begründen zudem eine klare Management-Verantwortung: Die oberste Führungsebene muss Cybersicherheits-Risikomanagementmaßnahmen nicht nur genehmigen, sondern auch deren Umsetzung aktiv überwachen und sicherstellen. Darüber hinaus besteht gemäß §38 BSIG eine Schulungspflicht für die Geschäftsleitung. Die Führungsebene muss regelmäßig an geeigneten Schulungen teilnehmen, um ihre Kenntnisse im Bereich Cybersicherheit auf dem aktuellen Stand zu halten und ihrer Verantwortung im Rahmen des Risikomanagements gerecht zu werden. Bei Nichteinhaltung drohen – je nach Einrichtungsart und Pflichtverletzung – empfindliche Maßnahmen und Geldbußen nach den einschlägigen Vorschriften des NIS2UmsuCG.

5. Erhebliche Sanktionen bei Nichteinhaltung

Die finanziellen Auswirkungen der Nichteinhaltung der Anforderungen aus des NIS2UmsuCG sind erheblich. Geldbußen können – abhängig von der Einordnung als besonders wichtige Einrichtung bzw. wichtige Einrichtung und vom konkreten Verstoß – bis zu 10 Millionen Euro oder 2 % des gesamten weltweiten Jahresumsatzes bzw. bis zu 7 Millionen Euro oder 1,4 % des Umsatzes betragen, je nachdem, welcher Wert höher ist. Maßgeblich sind die einschlägigen Bußgeld- und Durchsetzungsvorschriften im BSIG.

6. Strategische Empfehlungen für die Umsetzung

Die Erreichung der NIS2UmsuCG -Compliance erfordert eine strategische, unternehmensweite Anstrengung. Zu den wichtigsten Schritten gehören:

- **GAP-Analyse:** Durchführung einer gründlichen Bewertung Ihres aktuellen Sicherheitsniveaus gegenüber den Anforderungen aus NIS2UmsuCG.
- **Stärken Sie Ihr Fundament:** Konzentrieren Sie sich auf Maßnahmen, die eine stabile Grundlage für die Widerstandsfähigkeit Ihrer Organisation schaffen. So können Sie Ihr Unternehmen wirksam gegen unbefugte Zugriffe und potenzielle Angriffe schützen.
- **Überprüfung von Lieferkettenverträgen:** Sicherstellen, dass Verträge mit Lieferanten Cybersicherheitsverantwortlichkeiten und Incident-Meldungen explizit adressieren.
- **Schulung und Befähigung der Führungsebene:** Sensibilisierung der oberen Führungsebene für ihre gesetzlichen Verantwortlichkeiten gemäß NIS2UmsuCG.
- **Testen Sie Ihre Pläne:** Regelmäßiges Testen von Incident-Response- und Business-Continuity-Plänen durch Simulationen.

7. Wie DEKRA Sie auf Ihrer Reise unterstützen kann

DEKRA bietet Expertise und Lösungen, um Organisationen bei der Bewältigung der Anforderungen aus dem NIS2UmsuCG zu unterstützen. Unsere Dienstleistungen sind darauf ausgelegt, Resilienz von Grund auf aufzubauen. Wir können Sie unterstützen bei:

- Durchführung von GAP-Analysen und Risikobewertungen.
- Unterstützung bei der Erstellung robuster Incident-Response- und Business-Continuity-Pläne zur Sicherstellung der schnellen Wiederherstellung kritischer Geschäftsprozesse im Ernstfall.
- Bereitstellung gezielter Schulungen für technisches Personal und die Geschäftsleitung.

8. Fazit: Von der Compliance zur Resilienz

Das NIS2UmsuCG ist mehr als eine regulatorische Hürde; sie ist ein Bauplan für den Aufbau einer sichereren und widerstandsfähigeren Organisation. Indem Sie diese Anforderungen als Chance betrachten, Ihre Cybersicherheitsgrundlage zu stärken, mindern Sie nicht nur das Risiko finanzieller Strafen, sondern verbessern auch erheblich Ihre Fähigkeit, Cyberangriffe abzuwehren und sich davon zu erholen. Dadurch schützen Sie Ihre Betriebsabläufe, Ihren Ruf und Ihre Kunden.

Kontakt

Manuel Schneck
Senior Account Manager
Datenschutz/Informationssicherheit
Zertifizierter IT-Security-Beauftragter
manuel.schneck@dekra.com
Telefon +49.160 6173551

DEKRA Assurance Services GmbH
DEKRA Assurance Services GmbH
Handwerkstraße 15
70565 Stuttgart