Cyber-Sicherheitsrat Deutschland e.V.

Handlungshilfe für Entscheider

NIS2 – Von der Pflicht zur strategischen Absicherung

Dezember 2025

Inhaltsverzeichnis

1. Einleitung: Cybersicherheit ist jetzt Chefsache – Die persönliche Verantwortung

Die **EU-Richtlinie zur Netz- und Informationssicherheit (NIS2)** markiert einen fundamentalen Wandel in der Unternehmensführung: Cybersicherheit ist nicht länger eine reine IT-Aufgabe, sondern ein **strategisches Thema der Unternehmensleitung**.

Die Brisanz für **Organmitglieder** (Vorstände, Geschäftsführer) ist immens. Das NIS2-Umsetzungsgesetz verschärft die Konsequenzen bei Pflichtverletzungen drastisch und führt eine **persönliche Haftung** der Leitungsebene ein:

- **Persönliche Haftung (§ 38 Abs. 2 BSIG):** Bei Verletzung der Aufsichts- und Organisationspflichten drohen direkte Geldbußen gegen die Organe.
- **Massive Sanktionen (§ 65 BSIG):** Unternehmen riskieren Bußgelder in Höhe von bis zu **10 Millionen Euro** oder **2 % des weltweiten Jahresumsatzes**.
- **Führungsuntersagung (§ 61 BSIG):** Im Extremfall kann die Ausübung der Führungsfunktion durch das BSI temporär untersagt werden.

Fazit der Relevanz:

Die Leitungsebene muss sich aktiv mit NIS2 auseinandersetzen, da sie die **Verantwortung** für die Angemessenheit der Sicherheitsmaßnahmen nicht delegieren kann. Die **Aufsichtspflicht** (§ 38 Abs. 1 BSIG) wird zur juristischen Beweislast.

Diese Handlungshilfe, erstellt vom **Cyber-Sicherheitsrat Deutschland e.V.**, dient als kompakte und praxisnahe Orientierung.[1] Sie fasst die wichtigsten Aspekte der NIS2-Umsetzung zusammen, beleuchtet die akuten Haftungsrisiken und bietet konkrete Empfehlungen für eine strategische Absicherung.

Nach Inkrafttreten des NIS2-Umsetzungsgesetzes (NIS2UmsuCG) in Deutschland ist jetzt ist dokumentiertes Handeln gefordert.

[1] Ein besonderer Dank an Jan Arfwedson, Leiter des eHealth Hub, für die inhaltliche Ausarbeitung dieser Handlungshilfe im Nachgang der Veranstaltung „Cyber im Dialog“ am 20.11.2025 in München.

2. NIS2: Die neue strategische Aufgabe der Unternehmensführung

Die EU-Richtlinie zur Netz- und Informationssicherheit (NIS2) löst die ursprüngliche NIS-Richtlinie (in Deutschland „IT-Sicherheitsgesetz“) ab und verfolgt das Ziel, die **kollektive Widerstandsfähigkeit kritischer und wichtiger Sektoren in Europa drastisch zu erhöhen**. Im Gegensatz zur Vorgängerversion stellt NIS2 Cybersicherheit explizit als **zentrale Aufgabe der Unternehmensleitung** heraus.

Die gesetzgeberischen Fristen erfordern schnelles und zum Teil unmittelbares Handeln. Die nationale Umsetzung der NIS2-Richtlinie erfolgt mithilfe des NIS2-Umsetzungsgesetz (NIS2UmsuCG), das am 5. Dezember 2025 mit der Veröffentlichung im Bundesgesetzblatt in Kraft getreten ist. Somit besteht **sofortiger Handlungsbedarf**, da die Umsetzung der umfassenden Anforderungen Zeit, Budget und Ressourcen bindet.

Wichtigste Neuerungen im Überblick

- **Erweiterte Adressaten:** Der Kreis der betroffenen „Kritischen Einrichtungen“ (KE) und „Wichtigen Einrichtungen“ (WE) wurde stark ausgeweitet.
- **Umfassendes Risikomanagement (§ 30 BSIG):** Ein **Risikomanagement mit mindestens 10 spezifischen Maßnahmen** ist nun Pflicht.
- **Verschärfte Sanktionen (§ 65 BSIG):** Die Bußgelder sind auf Dimensionen der DSGVO gestiegen.
- **Haftung der Leitung (§ 38 BSIG):** Die Unternehmensleitung haftet direkt und ist zur Überwachung und Begleitung der Maßnahmen verpflichtet.

3. Neue Pflichten und Fristen im Meldewesen, der Supply Chain und Governance

Die neuen Pflichten konzentrieren sich auf die Absicherung der gesamten Lieferkette, die radikale Verkürzung der Meldepflichten sowie die Stärkung der Governance in der Unternehmensführung.

3.1 Meldewesen und Fristen (Verschärfung)

Die Meldefristen für Sicherheitsvorfälle (§ 32 BSIG) wurden drastisch verkürzt und präzisiert. Die Einhaltung dieser Fristen ist eine zentrale Obliegenheit und muss im Notfall geübt sein.

- **Frühwarnung:** Innerhalb von **24 Stunden** nach Kenntnis.
- **Vollständige Vorfallmeldung:** Innerhalb von **72 Stunden** nach Kenntnis.
- **Abschlussbericht:** Spätestens **1 Monat** nach Abschluss des Vorfalls.

3.2 Neue Pflichten: Supply-Chain-Sicherheit

Die Absicherung der Lieferkette wurde zur Chefsache. Unternehmen müssen die Cybersicherheit ihrer unmittelbaren Zulieferer bewerten und überwachen.

- **Bewertung von Zulieferern:** Die Cyberrisiken von Managed Service Providern (MSPs), Cloud-Anbietern und anderen externen Dienstleistern müssen aktiv in die eigene Risikobewertung einfließen.
- **Vertragsanforderungen:** Neue Vertragsanforderungen und Due-Diligence-Prozesse sind notwendig, um von Dritten die Einhaltung angemessener Sicherheitsstandards zu fordern.

3.3 Neue Pflichten: Schulung und Governance

Die Unternehmensleitung wurde explizit zur Überwachung und Begleitung der Cybersicherheitsmaßnahmen (§ 38 Abs. 1 BSIG) verpflichtet.

- **Führungskräfteschulung (§ 38 Abs. 3 BSIG):** Die gesamte Führungsebene muss an **verpflichtenden Cybersicherheitsschulungen** teilnehmen, um den „Stand der Technik“ zu verstehen und ihre Aufsichtspflicht wahrnehmen zu können.
- **Regelmäßige Berichterstattung:** Die CISO/CIO-Funktion ist verpflichtet, der Unternehmensleitung (Vorstand/Aufsichtsrat) regelmäßig über den Status der Cybersicherheit und die **Restrisiken** zu berichten.

4. Die zentralen Haftungsrisiken und Sanktionen

Die Nichteinhaltung der NIS2-Pflichten kann die Unternehmensleitung **direkt persönlich** betreffen und hohe Bußgelder für das Unternehmen nach sich ziehen.

4.1 Direkte Bußgelder gegen die Leitung und persönliche Haftung

Die Haftungsgrundlage ist die **Verletzung der Organisations- und Aufsichtspflicht (§ 38 Abs. 1 BSIG)**. Das bedeutet, dass die Einrichtung der Prozesse nachweisbar sein muss.

- **Bußgelder gegen die Leitung (§ 65 Abs. 1a/2a BSIG i.V.m. § 38 BSIG):** Der Gesetzentwurf sieht direkte Bußgelder vor, wenn die Leitung ihre Pflichten nicht wahrnimmt, z. B. bei:
    - Unterlassener Aufsicht über die Cybersicherheitsmaßnahmen (z. B. fehlendes IKS);
    - Nichteinhaltung der verpflichtenden Schulungen für Führungskräfte.

- **Haftungskette:** Der Verstoß gegen NIS2 führt zum Bußgeld gegen die Einrichtung, was eine Prüfung des Verschuldens der Leitung (Regress) durch die Gesellschaft auslösen kann.

4.2 Bußgelder gegen das Unternehmen (neue Dimensionen)

Die Bußgelder im NIS2UmsuCG (§ 65 BSIG) erreichen neue Dimensionen, die denen der DSGVO ähneln und **zusätzlich** verhängt werden können:

- **Kritische Einrichtungen (KE):** Bis zu **10 Millionen Euro** oder **2 %** des weltweiten Jahresumsatzes (höherer Betrag gilt);

- **Wichtige Einrichtungen (WE):** Bis zu **7 Millionen Euro** oder **1,4 %** des weltweiten Jahresumsatzes.

4.3 Risiko Management III: Reputations- und Vertrauensschaden

Ein erfolgreicher Angriff schädigt das Vertrauen zwischen Kunden, Partnern und Lieferanten nachhaltig und kann die Geschäftsgrundlage zerstören.

4.4 NIS2-Compliance als Wettbewerbsfaktor

Compliance signalisiert Stabilität, Resilienz und Professionalität. Wer NIS2-konform ist, schafft einen Wettbewerbsvorteil:

- **Wichtig bei Ausschreibungen:** NIS2-Konformität wird zum De-facto-Mindeststandard und entscheidend in der Due Diligence von Geschäftspartnern (insbesondere in der Supply Chain);

- **Qualitätsmerkmal:** Sicherheit wird als zentrales Qualitätsmerkmal wahrgenommen, was Vertrauen schafft und zu günstigeren Konditionen bei Cyberversicherungen führen kann.

5. Die vier Säulen der strategischen Absicherung

Ein ganzheitlicher Ansatz, der die Bereiche Governance, Technik, Risikotransfer und Krisenmanagement umfasst, ist notwendig, um die Compliance-Anforderungen zu erfüllen und die Unternehmensresilienz zu stärken.

Säule 1: Governance & Compliance (Checkliste Führung)

Hier liegt die Hauptverantwortung der Unternehmensleitung:

- **Governance-Verantwortlichkeit (CIO/CISO) festlegen:** Formelle Zuweisung der Umsetzungs- und Berichtsverantwortung sowie Sicherstellung ausreichender Ressourcen.
- **Regelmäßige Berichterstattung:** Standardisiertes Reporting, das sich auf **Restrisiken** konzentriert und eine transparente Entscheidungsbasis liefert.
- **Schulungen der Leitungsebene sicherstellen (§ 38 Abs. 3 BSIG):** Nachweisbare Teilnahme an extern geführten Schulungen, um den aktuellen Stand der Technik zu kennen und die Aufsichtspflicht zu belegen.
- **Detaillierte Gap-Analyse durchführen:** Erstellung eines Maßnahmenplans mit Fristen zur Schließung der Lücken bei den 10 NIS2-Maßnahmen **(§ 30 Abs. 2 BSIG)**.

Säule 2: Technische Resilienz – NIS2 Quick Wins

Der Fokus liegt auf den wichtigsten technischen Schutzmaßnahmen, die die Angriffsfläche massiv reduzieren:

- **Multi-Faktor-Authentifizierung (MFA):** Dort implementieren, wo es möglich ist, insbesondere bei Fernzugriffen (VPN, Cloud-Dienste) und alle privilegierten Konten.
- **Netzwerk-Segmentierung (Zero Trust Ansätze):** Strikte Trennung kritischer Systeme (OT/ICS) und Implementierung des Prinzips der geringsten Rechte.
- **Krisenrelevante Backups:** Einsatz von **Immutable Backups** (unveränderlich) und Sicherstellung der **Georedundanz**. Regelmäßige Tests der Wiederherstellungsfähigkeit (MTPD/RTO).
- **Patch-Management optimieren:** Etablierung eines Vulnerability-Management-Prozesses und - sofern möglich - Ausweitung der Verfahren auf die Betriebstechnik (OT/ICS).

Säule 3: Risikotransfer – Cyber- und D&O-Versicherungen

Die Versicherung mildert das finanzielle Risiko, ersetzt aber keine Compliance.

- **Cyber-Versicherung:** Deckt Kosten eines Cyberangriffs (Forensik, Betriebsunterbrechung). **Grenze:** Reduzierte Leistung droht bei grober Fahrlässigkeit (Verletzung von Mindeststandards).
- **D&O-Versicherung:** Schutz der Organe gegen Vermögensschäden. **Besondere Beachtung:** Sicherstellen, dass die Deckung den **Abwehrschutz** gegen Bußgeldvorwürfe und Regressansprüche der Gesellschaft umfasst. Bußgelder selbst sind meist ausgeschlossen.

Säule 4: Notfall- und Business Continuity Management

Die Übung der Pläne ist entscheidend, denn ohne Übung ist kein Erfolg möglich:

- **Vorher definierte Kommunikationswege:** Klare, schriftliche Anweisungen für die Meldung an das BSI und die interne/externe Krisenkommunikation.
- **Regelmäßige Tabletop-Übungen:** Training der Leitungsebene zur Entscheidungsfindung und zur Validierung der Meldeprozesse.
- **Wiederherstellungspläne, die ohne IT funktionieren:** Bereithalten von Offline-Dokumentation und Plänen für die **manuelle Weiterführung** kritischer Geschäftsprozesse im Falle eines Totalausfalls.

6. Handlungsempfehlungen und Fazit

Die wichtigsten Schritte jetzt

- **Governance-Struktur prüfen:** Governance-Verantwortlichkeit (CIO/CISO) festlegen und die eigene Aufsichtspflicht durch dokumentierte Schulungen und Berichte belegen.
- **Fokus auf MFA und Offline-Backups:** Diese technischen Quick Wins sind die Basis der Resilienz und der kritischste Prüfpunkt.
- **Notfallpläne testen (§ 32 BSIG):** Die **24-/72-Stunden-Meldepflicht** muss in Tabletop-Übungen trainiert werden, um Fehler und damit verbundene Bußgelder zu vermeiden.
- **Haftungsrisiken managen:** D&O- und Cyber-Versicherungen aktiv auf **Ausschlüsse bei mangelnder Compliance** überprüfen.

Fazit und Ausblick

Sehen Sie NIS2 nicht als regulatorischen Kostenfaktor, sondern als **strategische Investition in die Stabilität** und Wettbewerbsfähigkeit Ihres Unternehmens.

Die geforderten technischen und organisatorischen Maßnahmen (TOMs) machen grundsätzlich Sinn. Sie dienen nicht nur der formalen Compliance gegenüber NIS2, sondern erhöhen vor allem die **fundamentale Cyber-Resilienz** Ihres Unternehmens.

Entscheidend für den Erfolg ist die gelebte Wirksamkeit

- **Wirksamkeit validieren:** Das Thema Cybersicherheit wird nur dann ernst genommen und die Resilienz nachhaltig erhöht, wenn die Wirksamkeit der ergriffenen Vorkehrungen und Prozesse **regelmäßig validiert** wird (z. B. durch Penetrationstests, interne Audits und Krisenübungen).
- **Daueraufgabe der Führung:** NIS2 ist keine einmalige IT-Projektarbeit, sondern eine **strategische Daueraufgabe der Unternehmensführung**, die kontinuierliches Engagement erfordert.

Handeln Sie jetzt und machen Sie Cybersicherheit zur dokumentierten Chefsache.