

CYBERSICHERHEIT WIRD VERPFLICHTEND: BUNDESTAG GIBT GRÜNES LICHT FÜR NIS-2



Am 13.11.2025 wurde das deutsche NIS-2-Umsetzungsgesetz (NIS2UmsuCG) vom Bundestag verabschiedet und am 21.11.2025 vom Bundesrat bestätigt. Mit der NIS-2-Richtlinie verfolgt die EU das Ziel, die Widerstandsfähigkeit kritischer und wichtiger Dienste gegenüber Cyberangriffen deutlich zu erhöhen. Für viele Unternehmen bedeutet das, dass sie erstmals unter eine verbindliche Cybersicherheitsregulierung fallen.

Die mit uns verbundene DOMUS Consult Wirtschaftsberatungsgesellschaft mbH möchte die Wohnungsgenossenschaften daher über die mögliche Betroffenheit informieren.

I. Mögliche Betroffenheit

Auch Wohnungsgenossenschaften können mittelbar betroffen sein – insbesondere durch Lieferanten oder Dienstleister, die selbst NIS-2-pflichtig sind. Das betrifft z. B. den Einkauf von Telekommunikationsdiensten, Netz-Infrastruktur oder anderen digital kritischen Services. In seiner Stellungnahme weist der Zentrale Immobilien Ausschuss (ZIA) genau auf dieses Problem hin: Wohnungsgenossenschaften, die Telekommunikationsdienste Dritter bereitstellen, etwa Kabel-Internet im Rahmen der Vermietung, haben oft keinen direkten Einfluss auf die zugrundeliegenden technischen Sicherheitsmaßnahmen. Sie sind daher darauf angewiesen, dass ihre Vorlieferanten die geforderten Sicherheitsstandards einhalten.

Damit wirkt NIS-2 nicht nur für unmittelbar verpflichtete Unternehmen, sondern entfaltet auch starke Auswirkungen auf mittelbar betroffene Akteure wie Wohnungsgenossenschaften. Für sie steigen die Anforderungen an Sicherheitsüberprüfungen, Vertragsgestaltung und das Management ihrer Dienstleister erheblich.

Auch Wohnungsgenossenschaften, die eigene Energieerzeugungsanlagen (z. B. Blockheizkraftwerke, größere PV-Anlagen) betreiben, können im Einzelfall in den Anwendungsbereich der NIS-2-Regulierung fallen. Maßgeblich ist, ob die Genossenschaft als Energieversorgungs- oder -anlagenbetreiber im Sinne der einschlägigen energiewirtschaftsrechtlichen Vorschriften eingeordnet wird und die für NIS-2 relevanten Schwellenwerte (insbesondere Zahl der Beschäftigten und Jahresumsatz) erreicht oder als Betreiber einer kritischen Anlage eingestuft wird. Für solche Konstellationen ist eine individuelle Betroffenheitsprüfung (Rolle im Energiesektor, Umfang der Energieversorgung – Eigenversorgung vs. Versorgung Dritter –, Unternehmensgröße, Einstufung der Anlagen) erforderlich; ohne diese Prüfung kann eine Betroffenheit durch NIS-2 nicht sicher ausgeschlossen werden.

Wohnungsgenossenschaften mit Spareinrichtung (WumS) sind dem Finanzsektor zuzuordnen und unterliegen in Fragen der digitalen Betriebs- und Informationssicherheit primär der europäischen DORA-Verordnung (Digital Operational Resilience Act).

DORA regelt eigenständig die Anforderungen an das IKT-Risikomanagement, Meldepflichten und die Resilienz kritischer Finanzsysteme; NIS-2 tritt insoweit grundsätzlich hinter die speziellere Finanzmarktregulierung zurück. Für WumS ist daher maßgeblich, die Vorgaben aus DORA zu analysieren und umzusetzen; ergänzend kann im Einzelfall zu prüfen sein, ob daneben NIS2-Pflichten relevant werden, etwa bei Erreichen bestimmter Größenkriterien oder besonderen Infrastruktureigenschaften.

Folglich können neben klassischen Unternehmen der Energiewirtschaft und des Bankwesens auch Wohnungsgenossenschaften mit Energieerzeugungsanlagen sowie Wohnungsgenossenschaften mit Spareinrichtung von Sicherheits- und Resilienzanforderungen im Umfeld von NIS-2 bzw. sektorspezifischer EU-Regulierung (insbesondere DORA) betroffen sein.

Für diese „Grenzfälle“ wird ausdrücklich empfohlen, eine strukturierte Betroffenheitsprüfung vorzunehmen (Sektorzuordnung, Spezialaufsicht, Erreichen von Schwellenwerten, Einstufung von Anlagen), um den konkreten Handlungsbedarf rechtssicher zu bestimmen.

II. Allgemein

1. Ausweitung des Anwendungsbereichs

Die NIS-2-Richtlinie erfasst nun eine deutlich größere Vielfalt an Branchen und Unternehmensgrößen. Dazu zählen unter anderem das produzierende Gewerbe, Industrieunternehmen, Post- und Kurierdienste, die Chemiebranche sowie die Lebensmittelproduktion und -distribution. Auch IKT-Dienstleister, Anbieter von Managed Services und Managed Security, Forschungseinrichtungen sowie Hersteller von Medizinprodukten unterliegen den erweiterten Vorgaben. Darüber hinaus fallen zahlreiche weitere Bereiche unter die neuen Anforderungen.

Bereits ab **50 Mitarbeitenden** oder **10 Mio. € Jahresumsatz** kann ein Unternehmen in den Anwendungsbereich der NIS-2 fallen.

2. Erhöhte Sicherheitsanforderungen

Unternehmen müssen künftig ein umfassendes und nachweisbares Cybersicherheitsniveau etablieren, das alle wesentlichen Bereiche der IT- und Informationssicherheit abdeckt. Dazu gehören u. a.:

- ein wirksames Risikomanagementsystem,
- strukturiertes Patch- und Schwachstellenmanagement,
- ein belastbares Notfall- und Krisenmanagement,

- definierte Incident-Response-Prozesse (strukturierte Prozesse und strategische Maßnahmen, um auf ungeplante sicherheitsrelevante Ereignisse, Störungen oder Cyberangriffe zu reagieren),
- die konsequente Sicherheitsüberprüfung der Lieferkette.

Zudem müssen IT- und OT-Umgebungen gezielt gehärtet und strengere Authentifizierungs- und Zugriffskontrollen umgesetzt werden, um ein durchgängig hohes Sicherheitsniveau zu gewährleisten.

3. Verschärfte Meldepflichten

Nach NIS-2 müssen Cybervorfälle in mehreren Stufen und innerhalb eng gefasster Fristen gemeldet werden:

- **Innerhalb von 24 Stunden:** Frühwarnung an das zuständige CSIRT bzw. die Behörde, inkl. Hinweis auf mögliche böswillige Absichten oder grenzüberschreitende Auswirkungen,
- **Innerhalb von 72 Stunden:** ausführlicher Incident-Report mit einer ersten Bewertung des Vorfalls, seiner Schwere, Auswirkungen sowie bekannten Indikatoren einer Kompromittierung,
- **Spätestens nach einem Monat:** Abschlussbericht mit detaillierter Beschreibung des Vorfalls, Ursache/Bedrohung, getroffenen Maßnahmen sowie Informationen zu etwaigen grenzüberschreitenden Folgen.

Diese Meldepflichten sind in **Artikel 23 NIS-2** klar definiert.

4. Persönliche Haftung der Geschäftsleitung

Die NIS-2-Richtlinie verpflichtet Unternehmen zur regelmäßigen Schulung von Führungskräften und Mitarbeitenden in Cybersicherheit. Die Geschäftsleitung trägt die Verantwortung für die Einführung, Überwachung und Wirksamkeit der Sicherheitsmaßnahmen und damit eine zentrale Rolle für die Cyber-Resilienz des Unternehmens.

Organisationsversäumnisse können zu erheblichen persönlichen Haftungsrisiken für das Management führen. Die rechtliche Basis hierfür bilden insbesondere **Artikel 20 und 21 NIS-2**. Artikel 21 Absatz 2 Buchstabe g schreibt explizit regelmäßige Schulungen vor; Verstöße können gemäß **Artikel 32 und 34** zu empfindlichen Sanktionen führen.

5. Bußgelder auf neuem Niveau

Verstöße gegen die NIS-2-Vorgaben können mit **bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes** geahndet werden – maßgeblich ist der jeweils höhere Wert.

Wie müssen Unternehmen jetzt reagieren?

- **Schritt 1:** Betroffenheit prüfen
- **Schritt 2:** Gap-Analyse durchführen
- **Schritt 3:** Governance, Verantwortlichkeiten & Schulungen stärken
- **Schritt 4:** Technische und organisatorische Schutzmaßnahmen umsetzen
- **Schritt 5:** Incident-Response- und Krisenstrukturen etablieren
- **Schritt 6:** Dokumentation & Compliance dauerhaft verankern

III. Angebot der DOMUS Consult

Wir unterstützen Sie bei der NIS-2-Umsetzung

Wir begleiten Wohnungsgenossenschaften ganzheitlich auf dem Weg zur NIS-2-Konformität. Unser Leistungsumfang umfasst:

Betroffenheitsanalyse:

Wir prüfen, ob und in welchem Umfang Ihre Genossenschaft unter NIS-2 fällt.

Gap- und Prioritätenanalyse:

Identifikation bestehender Schwachstellen und Ableitung der wichtigsten Handlungsfelder.

Umsetzung technischer & organisatorischer Maßnahmen:

Vom Risikomanagement über Patch- und Zugriffsprozesse bis hin zur Härtung von IT- und OT-Systemen.

Aufbau von Incident-Response- und Krisenstrukturen: Entwicklung belastbarer Abläufe für den Ernstfall.

Schulungen für Geschäftsführung und Mitarbeitende:

Vermittlung des notwendigen Sicherheitsbewusstseins und der rechtlichen Verantwortlichkeiten.

Dokumentation & Nachweisführung:

Erstellung aller erforderlichen Unterlagen zur Erfüllung der NIS-2-Compliance.

Mit unserem Ansatz wird Ihr Unternehmen **pragmatisch, effizient und nachhaltig** NIS-2-konform – und gewinnt zugleich ein höheres Maß an Cyber-Resilienz. Kontaktieren Sie uns unter datenschutz@domusconsult.de.