CYBERSECURITY IN DER GEBÄUDESTEUERUNGEN

Network and Information Security Directive (NIS2)

Inhalt

1. Zweck des Dokuments **2**
1.1. Nationale Rahmenwerke für Cybersicherheit 2

2. Was sind die Kohlen der NIS2 ..... **2**

3. Betroffene Sektorenund Industrien **2**
3.1. Sektoren und Branchen: 2
3.2. Kriterien für die Größe: 3

4. Was erfordert die Einhaltung von NIS2? **3**
4.1. Festlegung einer Sicherheitsstrategie für Netzwerke und Informationssysteme 3
4.2. Rick Management Rahmen 3
4.3. Berichtspflicht 4

5. Wichtigste Erkenntnisse: **4**
5.1. Erweiterter Anwendungsbereich 4
5.2. Obligatorisches Cybersecurity-Risikomanagement 4
5.3. Strengere Berichtspflichten 4
5.4. Governance und Rechenschaftspflicht 4
5.5. Lieferkette und Drittparteirisiko 5

6. Zeitleiste **5**

1. Zweck des Dokuments

Dieses Dokument bietet einen Überblick über die Network and Information Security Directive EU-Richtlinie 2022/2555 (NIS2) zur Netz- und Informationssicherheit, die ab dem 18. Oktober 2024 gilt. Die Regelung definiert neue Cybersicherheitsanforderungen für zentrale Branchen mit dem Ziel, deren Geschäftsbetrieb zu schützen.

1.1. Nationale Rahmenwerke für Cybersicherheit

Die NIS2-Richtlinie verlangt von den EU-Staaten, Cybersicherheitsvorgaben für kritische Bereiche wie digitale Infrastruktur, Energie, Verkehr und Gesundheit festzulegen. Teilsektoren mit länderübergreifender Bedeutung unterliegen EU-weit einheitlichen Vorgaben. Am 17. Oktober 2024 hat die Kommission technische Standards in der Durchführungsverordnung (EU) 2024/2690 zur Umsetzung festgelegt.

- Jeder Mitgliedstaat muss eine nationale Cybersicherheitsstrategie haben,
- Behörden benennen und Ansprechpartner sowie CSIRTs (Computer Security Incident Response Teams) einrichten.

2. Was sind die Ziele von NIS2

Die NIS2-Richtlinie stärkt die Cyber-Resilienz wichtiger EU-Infrastrukturen. Unternehmen und Organisationen müssen ihre Netzwerke und IT-Systeme umfassend schützen.

3. Betroffene Sektoren und Industrien

Die NIS2-Richtlinie betrifft EU-Unternehmen mit zentralen oder wichtigen Dienstleistungen und bestimmten Größen. Ziel ist es, die Cybersicherheit und Abwehr gegen Angriffe zu stärken.

3.1. Sektoren und Branchen:

Neben den bereits im Rahmen der NIS 1 erfassten Sektoren – Energie, Verkehr, Gesundheitswesen, Finanzwesen, Wasserwirtschaft und digitale Infrastruktur – finden die neuen Vorschriften ebenfalls Anwendung auf Anbieter öffentlicher elektronischer Kommunikation, zusätzliche digitale Dienste wie soziale Plattformen, sowie die Abfall- und Abwasserwirtschaft und bestimmte kritische Produkte.

Betreiber kritischer Infrastrukturen (KRITIS): Dieser Begriff umfasst Unternehmen aus den Sektoren Energie, Verkehr, Gesundheitswesen, digitale Infrastruktur und Finanzwesen.

Wesentliche Entitäten: Unter diese Kategorie fallen Organisationen und Unternehmen, die für die Gesellschaft und Wirtschaft bedeutsame Dienstleistungen bereitstellen, ohne zwingend Teil der kritischen Infrastrukturen zu sein. Hierzu zählen unter anderem:

- Energie
- Transport
- Gesundheit
- Wasserversorgung
- Digitale Infrastruktur (beispielsweise Cloud-Anbieter, DNS-Dienste)
- Öffentliche Verwaltung

Wichtige Entitäten: Diese Stellen bieten zwar bedeutende Dienste, gelten aber nicht als kritisch. Dazu zählen:

- Postdienste
- Abfallwirtschaft
- Chemie
- Lebensmittelproduktion
- Medizinprodukteherstellung
- Digitale Dienste (z. B. soziale Netzwerke, Suchmaschinen)

3.2. Kriterien für die Größe:

Mittlere und große Unternehmen in den Sektoren Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, IKT-Dienstleistungsmanagement (Business-to-Business), öffentliche Verwaltung, Raumfahrt, Post- und Kurierdienste sowie Abfall unterliegen den Vorgaben der NIS2-Richtlinie.

Mittelständische Unternehmen: Unternehmen mit mindestens 50 Beschäftigten und einem Jahresumsatz oder einer Bilanzsumme von über 10 Millionen Euro fallen in diese Kategorie.

Große Unternehmen: Diese Kategorie umfasst Unternehmen mit mindestens 250 Beschäftigten oder einem Umsatz beziehungsweise einer Bilanzsumme oberhalb bestimmter Schwellenwerte (zum Beispiel 50 Millionen Euro Umsatz oder 43 Millionen Euro Bilanzsumme).

Besondere Fälle: Unabhängig von ihrer Größe können Unternehmen je nach Art der erbrachten Dienstleistungen oder Tätigkeiten als wesentlich eingestuft werden.

4. Was erfordert die Einhaltung von NIS2?

4.1. Festlegung einer Sicherheitsstrategie für Netzwerke und Informationssysteme

Die NIS 2 verpflichtet die Führungsebene zur Einhaltung und Dokumentation von Cybersicherheitsmaßnahmen.

Gefordert wird ein ganzheitlicher Ansatz zum Schutz von Netzwerken und Informationssystemen. Die Sicherheitsstrategie umfasst Risikoanalysen, Zwischenfallmanagement, Geschäftskontinuität, Lieferkettensicherheit, sichere Entwicklung und Wartung, Wirksamkeitsprüfungen, Cyberhygiene, Verschlüsselung, Personalsicherheit und Multi-Faktor-Authentifizierung. IT-Dokumentation sowie Überblick über Infrastruktur und Berechtigungen sind zu erstellen oder zu aktualisieren. Mitarbeiter sowie externe Partner müssen die Richtlinien anerkennen und erhalten gezielte Informationen, ohne vertrauliche Daten offenzulegen.

4.2. Rick Management Rahmen

Unternehmen müssen einen effektiven Risikomanagementrahmen einrichten und pflegen, um Sicherheitsbedrohungen systematisch zu identifizieren und zu bekämpfen. Sie führen umfassende Bewertungen durch, dokumentieren die Ergebnisse und erstellen darauf basierend einen Risikobehandlungsplan, der von Leitungsorganen geprüft und genehmigt wird.

Der Plan verknüpft Risiken mit Vermögenswerten, beschreibt Maßnahmen zur Risikominderung und enthält Zeitpläne sowie Verantwortlichkeiten.

Restrisiken wie Datenschutzverletzungen oder Abhängigkeit von Drittanbietern sind ebenfalls zu berücksichtigen und müssen von befugten Personen akzeptiert werden. Die Genehmigung der Bewertung und des Plans erfolgt durch die zuständigen Leitungsorgane.

4.3. Berichtspflicht

Wesentliche Einrichtungen sind verpflichtet, die betroffenen Dienstleistungsempfänger zeitnah über erhebliche Cyber-Bedrohungen sowie mögliche Maßnahmen zu informieren. Bei Bedarf sollen auch relevante Details zur jeweiligen Bedrohung mitgeteilt werden. Ein Vorfall wird als bedeutsam eingestuft, wenn er zu erheblichen Störungen, finanziellen Verlusten für die Organisation oder zu materiellem beziehungsweise immateriellem Schaden für andere führen kann.

Ebenso müssen wesentliche Einrichtungen die zuständige Behörde über bedeutende Vorfälle wie folgt benachrichtigen:

- Frühe Warnung innerhalb von 24 Stunden nach Feststellung des Vorfalls unter Angabe, ob möglicherweise rechtswidrige, böswillige oder grenzüberschreitende Aspekte vorliegen.
- Innerhalb von 72 Stunden ist eine vollständige Meldung einzureichen, die aktualisierte Informationen bereitstellt und eine erste Bewertung von Schweregrad, Auswirkungen sowie bekannte Indikatoren für eine Kompromittierung enthält.

5. Wichtigste Erkenntnisse:

Die NIS2-Richtlinie (EU 2022/2555) ist der neue EU-Standard für Cybersicherheit. Sie ersetzt die alte Richtlinie, erweitert die regulierten Bereiche und verschärft Risikomanagement sowie Berichtspflichten.

5.1. Erweiterter Anwendungsbereich

Die NIS2-Richtlinie betrifft mehr Branchen als zuvor, etwa Energie, Verkehr, Banken, Gesundheit, digitale Infrastruktur und IT-Hersteller. Unternehmen werden anhand von Größe und Branche als "wesentlich" oder "wichtig" kategorisiert; die Schwellenwerte richten sich nach Mitarbeiterzahl und Umsatz.

5.2. Obligatorisches Cybersecurity-Risikomanagement

Organisationen müssen technische und organisatorische Maßnahmen gegen Cybersicherheitsrisiken ergreifen sowie Richtlinien für Zwischenfälle, Geschäftskontinuität und Lieferkettensicherheit festlegen. Die Orientierung an ISO/IEC 27001 ist sinnvoll, aber nicht verpflichtend.

5.3. Strengere Berichtspflichten

Betroffene Unternehmen müssen Vorfälle spätestens 24 Stunden nach Entdeckung melden. Die Meldung muss eine Folgenabschätzung beinhalten und Gegenmaßnahmen aufzeigen. Nationale CSIRTs und zuständige Behörden müssen informiert werden.

5.4. Überwachung und Rechenschaftspflicht

Die Geschäftsleitung muss die Vorschriften einhalten. Verstöße können Geldstrafen bis zu 10 Millionen Euro oder 2 % des weltweiten Umsatzes nach sich ziehen. CEOs und gesetzliche Vertreter riskieren bei schweren Vergehen eine zeitweise Führungssperre.

5.5. Lieferkette und Drittparteirisiko

Unternehmen sollten Cybersicherheitsrisiken in der Lieferkette prüfen und steuern. Auch Drittanbieter und Dienstleister müssen bei der Risikobetrachtung und dem Risikomanagementberücksichtigt werden.

6. Zeitleiste

Die Mitgliedstaaten müssen die Richtlinie bis zum 17. Oktober 2024 umsetzen.

Die Maßnahmen gelten ab dem 18. Oktober 2024.

Die ENISA und die Kommission werden die Umsetzung alle 36 Monate überprüfen (Artikel 40).