NIS-2-Richtlinie – Anforderungen, Umsetzung und Lösungen

Informationen und Beratung zur neuen EU-Richtlinie von CANCOM Austria

Ab Mitte Oktober 2024 müssen alle EU-Mitgliedsstaaten die NIS-2-Richtlinie (NIS-2-RL) umsetzen. Die NIS-2-RL hat das Ziel, die Informationssicherheit von kritischen Unternehmen und Organisationen sicherzustellen. Durch die Erweiterung des Anwendungsbereiches sind zukünftig deutlich mehr Unternehmen und Organisationen in Österreich von der Umsetzung und Erfüllung der Informationssicherheitsanforderungen betroffen.

CANCOM

NIS-2-RL – wer ist betroffen?

Unternehmen in 18 Sektoren sind betroffen, wenn sie zumindest über **50 Mitarbeiter:innen oder 10 Mio. € Jahresumsatz/Jahresbilanzsumme** verfügen. Zusätzlich fallen öffentliche Kommunikationsdienste, qualifizierte Signatur- und digitale Zustelldienste, die öffentliche Verwaltung und von der Behörde per Bescheid benannte Unternehmen unter den Anwendungsbereich.

Sektoren für wesentliche und wichtige Einrichtungen[1] (+3 zu NIS-1):

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten B2B
- Öffentliche Verwaltung
- Weltraum

Sektoren für wichtige Einrichtungen (+6 zu NIS-1):

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemische Industrie
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes bzw. herstellendes Gewerbe
- Anbieter digitaler Dienste
- Forschung

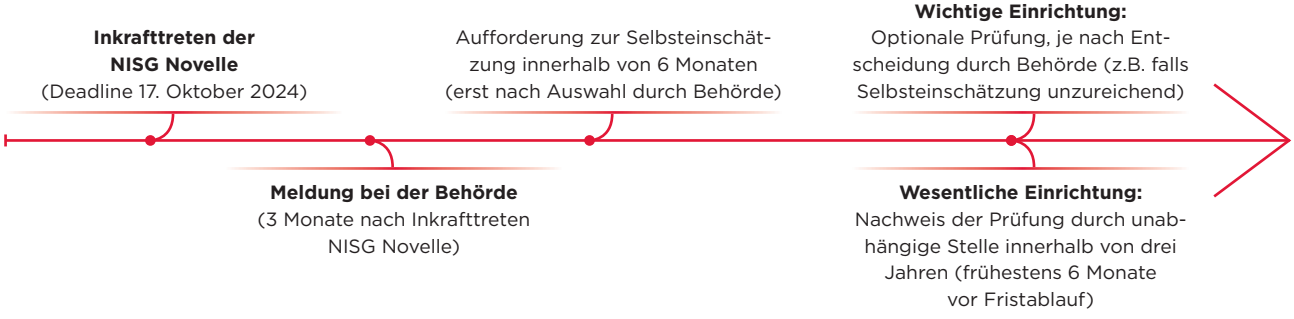
[1] Die Kategorie wesentliche Einrichtung betrifft Unternehmen ab 250 Mitarbeiter:innen oder über 50 Mio. € Jahresumsatz und Jahresbilanzsumme

NIS-2-Anforderungen – das ist zu tun

Die Umsetzung der NIS-2-RL wird das derzeit gültige österreichische NIS-Gesetz stark ausweiten. Die für Unternehmen relevanten Ergänzungen bringen einige neue Anforderungen, während bestehende erweitert bzw. angepasst werden. Hier ein kurzer Überblick, welche Bereiche Sie beachten sollten:

- **Leitungsorgane:** Fokus auf Rollendefinitionen und Zuweisung von Verantwortlichkeiten
- **Sicherheitsrichtlinien:** Erstellung und Überwachung von Sicherheitsrichtlinien und Verantwortlichkeiten
- **Risikomanagement:** Richtlinien und Prozesse, Effektivitätsbeurteilung, Überwachung und unabhängige Überprüfungen
- **Verwaltung von Vermögenswerten:** Inventarisierung und Klassifikation von Assets
- **Personalwesen:** Sicherheitsaspekte, Hintergrundüberprüfungen, Verfahren bei Beschäftigungswechsel und Disziplinarmaßnahmen
- **Cyberhygiene und -schulungen:** Bewusstseinsschaffung und Schulungen zur Cybersicherheit
- **Lieferkettensicherheit:** Sicherheitsrichtlinien und Lieferantenmanagement
- **Zugangssteuerung:** Richtlinien, Verwaltung von Berechtigungen und privilegierten Benutzerkonten, Identifikations- und Authentifizierungsmaßnahmen
- **Beschaffung, Entwicklung und Wartung:** Management von Konfigurationen, Änderungen, Schwachstellen, Sicherheitstests, Patchmanagement, Netzwerksegmentierung und Netzwerksicherheit
- **Kryptographie:** Richtlinien zur Kryptographie
- **Cybersicherheitsvorfälle:** Richtlinien, Überwachung, Ereignismeldung, Reaktion und Erkenntnisgewinnung
- **Betriebskontinuität und Krisenmanagement:** Kontinuitätsmanagement, Backup- und Krisenmanagement, Wiederherstellung
- **Physische und umgebungsbezogene Sicherheit:** Perimeter- und Zutrittskontrollen, Schutz vor Gefährdungen, Versorgungseinrichtungen

Ablauf der Nachweise/Prüfungen



Pflichten von wesentlichen und wichtigen Einrichtungen sowie Sanktionen

Pflichten

- Meldung an die Behörde, dass man eine wesentliche oder wichtige Einrichtung ist (Deadline: 3 Monate nach Inkrafttreten der NIS Gesetz Novelle)
- Erfüllen der Anforderungen durch technische und organisatorische Schutzmaßnahmen, um die ungestörte Erbringung der Dienste der wichtigen/wesentlichen Einrichtung sicherzustellen
- Meldepflicht von erheblichen Cybersicherheitsvorfällen an das zuständige Computer-Notfallteam (CSIRT)
- Durchführung einer Selbsteinschätzung der Umsetzung der Anforderungen (innerhalb von 6 Monaten nach Aufforderung durch Behörde)
- Überprüfung der Schutzmaßnahmen von wesentlichen Einrichtungen durch unabhängige Stelle wie CANCOM Austria (innerhalb von 3 Jahren nach Aufforderung zur Selbsteinschätzung)
- Überprüfung der Schutzmaßnahmen von wichtigen Einrichtungen durch unabhängige Stelle wie CANCOM Austria (nur bei begründeter Aufforderung der Behörde, Frist: 3 Jahre)

Sanktionen

- Persönliche Haftung der Leitungsorgane
- Geldbußen:

  10 Millionen Euro/2 % des weltweiten Umsatzes für **wesentliche** Einrichtungen

  7 Millionen Euro/1,4 % des weltweiten Umsatzes für **wichtige** Einrichtungen

Unser Angebot im Bereich NIS für Sie

Unterstützung bei der Umsetzung der NIS-2-RL-Anforderungen:

- **NIS-2-Gap-Analyse:** Standortbestimmung für Unternehmen; Analyse des Reifegrads der technischen und organisatorischen Maßnahmen und Ermittlung, welche Verbesserungsmaßnahmen noch notwendig sind
- **Security-Architektur-Review:** Überprüfung der technischen Infrastruktur und Systeme auf Erfüllung des Stands der Technik
- **Erstellung und Einführung eines Risikomanagements sowie von Dokumenten und Prozessen:** Unterstützung bei der Einführung eines ISMS und der technischen und organisatorischen Schutzmaßnahmen durch unsere Expertise
- **Durchführung von Audits, Risikoanalysen und Notfallübungen:** Unterstützung bei der Umsetzung des ISMS und der technischen sowie organisatorischen Schutzmaßnahmen durch unsere Expertise
- **NIS-Überprüfung:** Durchführung einer Überprüfung der Umsetzung der Anforderungen, wie im Gesetz für wesentliche (und bei Aufforderung für wichtige) Einrichtungen gefordert
- **Cyber Risk Rating:** Überschaubare Ist-Analyse mit Aufzeigen von Abweichungen und Handlungsempfehlungen. Darüber hinaus wird ein Mindeststandard in der Informationssicherheit unterstützt und bei Erfüllung mit einem Zertifikat honoriert. Die herausfordernde Sicherstellung der Informationssicherheit für Lieferanten gemäß § 17 NIS-Gesetz lässt sich mit dem Cyber Risk Rating effizient und effektiv prüfen sowie sicherstellen.
- **Business Continuity Management (BCM):** Unterstützung beim Aufbau eines BCM/IT-Notfallmanagements nach BSI-Standard 200-4 und/oder ISO 22301, um regulatorische Anforderungen zu erfüllen und als präventiver und reaktiver Schutz vor Schadensereignissen, welche den Fortbestand des Unternehmens bzw. der Organisation gefährden

Road to NIS2 für betroffene Einrichtungen

Der NIS2-Aktionsplan: Umfangreiche Anforderungen machen ein strukturiertes Vorgehen bei Umsetzung notwendig

	Kurzfristige Ziele (30-90 Tage)	Mittelfristige Ziele (bis 120 Tage)	Bis Inkrafttreten der NISG Novelle
People	→ Awareness bei Geschäftsführung schaffen → HR, Rechtsabteilung, etc. über die neuen Anforderungen informieren → Frühzeitige Einbindung von Abteilungsleitern	→ Verantwortliche in den Abteilungen definieren → Laufende Information der Stakeholder → Einrichtung eines abteilungsübergreifenden Teams zur Koordination	→ Laufende Zusammenarbeit der Abteilungen koordinieren → Schulungen in betroffenen Abteilungen durchführen → Etablierung eines kontinuierlichen Verbesserungsprozesses
Prozesse	→ Betroffene Prozesse und Abläufe identifizieren → Gap-Analyse gelebter Prozesse und externer Abhängigkeiten → Priorisierung von Maßnahmen basierend auf Risikobewertungen	→ Berichts- und Meldewege einrichten → Änderungen in Notfallprozessen und BCM identifizieren → Überarbeitung der Risikomanagement- und Auditprozesse	→ Kontinuierliche Verbesserung → Dokumentation und Überwachung der Compliance sicherstellen → Implementierung regelmäßiger interner Audits und Überprüfungen
Technologien	→ Gap-Analyse eingesetzter Tools und Roadmap zur Behebung erstellen Identifizierung kritischer Systeme und Datenflüsse → Schnelle Anpassungen und Upgrades wo möglich (Quick Wins)	→ Maßnahmen in bestehenden Systemen umsetzen → Überwachungs- und Reaktionswege planen → Änderungen in der IT-Infrastruktur planen	→ Integration neuer Technologien → Kontinuierliche Bewertung und Anpassung der IT-Infrastruktur → Laufende technologische Verbesserungen

Weiterführende Dienstleistungen und Produkte von CANCOM Austria

- Technische Audits (intern/extern): Penetration Tests der technischen Schutzmaßnahmen durch das CANCOM Red Team
- unterstützende Services bis zum Managed Service für den Betrieb ihrer technischen Infrastruktur (Server, Netzwerk, Firewall und Endpoint Security Lösungen)
- SOC-Dienstleistungen: Erkennen und Analyse von Sicherheitsvorfällen durch die Expertise des CANCOM Defense Center
- Risikomanagementwerkzeuge: Vertrieb der Risikomanagementsoftware CRISAM und Einführungsberatung
- Architektur, Design und Implementierung von technischen Maßnahmen nach Stand der Technik

Unsere Unterstützungsdienstleistungen

Bewertung

CANCOM Austria bewertet die bestehenden technischen und organisatorischen Schutzmaßnahmen des auftraggebenden Unternehmens aus der Sicht einer qualifizierten Stelle nach der geltenden Rechtslage (NISG, NISV, NIS Factsheets, NIS-2-Richtlinien-Umsetzung).

Dies kann in der Form eines Gap Assessments, einer technischen Architekturanalyse und/oder eines internen oder externen Pentests geschehen.

Ziel ist es, ein möglichst genaues Bild der Erfüllung der NIS-Anforderungen zu erhalten und daraus Arbeitspakete und Projekte abzuleiten.

Beratung

CANCOM Austria unterstützt das auftraggebende Unternehmen bei der Umsetzung der Projekte und Arbeitspakete durch Informationen und Feedback sowie die Bereitstellung von Vorlagen und Anforderungsprofilen.

Die Umsetzung wird dabei primär vom auftraggebenden Unternehmen durchgeführt, während CANCOM Austria nur bei Bedarf bzw. auf Wunsch direkt tätig wird.

Ziel ist es, die interne Expertise für die Erfüllung der Anforderungen auf- bzw. auszubauen. CANCOM Austria fungiert als Multiplikator, der die Effizienz und die Effektivität der internen Ressourcen vergrößert.

Durchführung

Hier wird CANCOM Austria direkt für das auftraggebende Unternehmen tätig und liefert die Bausteine für die erfolgreiche Erfüllung von Anforderungen. Das auftraggebende Unternehmen gibt hier die Aufgaben bzw. das Ziel vor, setzt aber in der Regel nicht selbst um. CANCOM Austria stellt seine Expertise und Erfahrungen bereit, um die Aufgaben bzw. Ziele gut und effizient zu erfüllen.

Die Durchführung kann verschiedene Bereiche betreffen: Dokumentenerstellung, Prozessentwicklung, Risikoanalyse, Incident Response etc.

CANCOM Austria (vormals Kapsch BusinessCom) ist Österreichs führender ICT-Service Provider und Digitalisierungspartner. Als Hybrid IT Service Provider begleitet die CANCOM Gruppe Unternehmen in die digitale Zukunft. CANCOM unterstützt ihre Kunden dabei, die Komplexität ihrer IT zu reduzieren und ihren Geschäftserfolg durch den Einsatz modernster Technologie auszubauen. Um den IT-Bedarf von Unternehmen, Organisationen und dem öffentlichen Sektor ganzheitlich abzubilden, bietet CANCOM passgenaue IT von A bis Z aus einer Hand.

Das IT-Lösungsangebot der CANCOM Gruppe enthält Beratung, Umsetzung, Services sowie den Betrieb von IT-Systemen. Kunden profitieren dabei von der umfangreichen Expertise sowie einem ganzheitlichen und innovativen Portfolio, das die für eine erfolgreiche digitale Transformation notwendigen Anforderungen an die IT von Unternehmen abdeckt. Als führender IT Integrator und Service Provider bietet CANCOM ein breites Spektrum an Leistungen und Lösungen, darunter Business Solutions und Managed Services für Cloud Transformation, AI und Analytics, Workplace, Enterprise Mobility und IT-Security. Dies umfasst auch Hosting und As-a-Service-Modelle.

CANCOM Austria entwickelt darüber hinaus eigene Softwarelösungen und Plattformen für innovative Geschäftsmodelle. Als Digital Maker denken die Mitarbeiter von CANCOM Austria dabei stets end-to-end. Durch die Kapsch-Wurzeln verbindet CANCOM Austria 130 Jahre Innovationskraft mit der langjährigen Erfahrung als Marktführer für Netzwerk, Data Center, Security, Collaboration und Managed Services. Das CANCOM Cyber Defense Center gewährleistet dabei 24/7 Schutz vor Cyberangriffen.
Zusätzlich bietet die CANCOM a+d IT Solutions, die bereits seit 1994 in Österreich aktiv ist, smarte Workplace-Lösungen mit Geräte-Lifecycle-Management zur Erreichung von Nachhaltigkeitszielen und Employee Choice Programmen für Endgeräte verschiedenster Hersteller.

CANCOM Austria AG	GJ 22/23: rd. 520 Mio. Euro, 1.622 MA
CANCOM Gruppe	GJ 2023: 1,5 Mrd. Euro, 5.600 MA

Besuchen Sie uns auf ↗ cancom.at

CANCOM Austria // Wienerbergstraße 53 // 1120 Wien // Österreich // T +43 50 822-0 // office@cancom.com // www.cancom.at