Cybersicherheit

Sicherheit von Netz- und Informationssystemen (NIS)

Cybersicherheits-Richtlinie NIS2 – NISG 2024

Barbara Streimelweger

Inhaltsverzeichnis

Cybersicherheit

1. Cybersicherheit in Europa und Österreich

Cyber Incidents, Cyber-Vorfälle, wie beispielsweise Cybercrime, Unterbrechungen von IT-Netzwerken und IT-Diensten, Malware, Ransomware und Datenschutzverletzungen führen mit 36% die Liste der wichtigsten Geschäftsrisiken global für 2024[1] an. In Österreich[2] zählen Cyber-Vorfälle wie Datenpannen, Angriffe auf kritische Infrastruktur oder Vermögenswerte und vermehrte Ransomware-Attacken mit 40% zu den größten Risiken.

IT-Systemen wird eine zentrale Rolle in der Gesellschaft zugeschrieben und sowohl Verlässlichkeit als auch Sicherheit sind für wirtschaftliche und gesellschaftliche Tätigkeiten sowie das Funktionieren des Binnenmarkts entscheidend. Die Europäischen Union (EU) fordert ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen und veröffentlichte im EU-Amtsblatt als ersten Rechtsakt über Cybersicherheit in der EU mit 19.07.2016 die EU-Richtlinie 2016/1148, bekannt als NIS-Richtline. Diese wurde mit 28.12.2018 mit dem NIS-Gesetz in Österreich umgesetzt und betrifft vorwiegend Unternehmen der kritischen Infrastruktur und Anbieter digitaler Dienste, wie Online-Marktplätze, Online-Suchmaschinen und Cloud Computing-Dienste. Mit 17.07.2019 wurde die NIS-Verordnung (NISV) im Bundesgesetzblatt veröffentlicht.

Die Forderung nach mehr Cybersicherheit wächst stetig: Einerseits sind Maßnahmen notwendig und zu setzen, um der Entwicklung der Bedrohungslandschaft und steigenden Cyberkriminalität entgegenzuwirken. Die zunehmende Digitalisierung fordert andererseits ebenfalls die Umsetzung von Maßnahmen für mehr Sicherheit. Dies führte dazu, dass die EU-Richtlinie 2016/1148 durch die EU-Richtline 2022/2555 vom 14.12.2022 (Cybersicherheits-Richtlinie NIS2, NIS-2-Richtline), veröffentlicht im EU-Amtsblatt am 27.12.2022, aufgehoben wurde.

Die Cybersicherheits-Richtlinie NIS2 muss spätestens bis 17.10.2024 in nationales Recht umgesetzt sein. Weitere Übergangsfristen sind nicht vorgesehen. Nun liegt seit 03.04.2024 der erste Begutachtungsentwurf, das Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024), für vier Wochen zur Begutachtung vor. Die Regelungen gelten für die betroffenen Einrichtungen mit Inkrafttreten des Gesetzes. Da es sich beim NISG 2024 um einen offiziellen Begutachtungsentwurf handelt, der im parlamentarischen Gesetzgebungsprozess noch abgeändert werden kann, sind die genannten Anforderungen noch nicht fix definiert. Ebenso ist der Zeitpunkt des Inkrafttretens noch offen.

2. Cybersicherheits-Richtlinie NIS2

2.1. Zielsetzung der NIS-2-Richtline

Die Ziele und Forderungen der EU sind einerseits der Schutz kritischer Einrichtungen und Infrastrukturen in der EU vor Cyberbedrohungen und andererseits das Erreichen eines einheitlichen hohen Sicherheitsniveaus in der EU und damit eine Steigerung der Cyber-Resilienz.

Die NIS-2-Richtline kann als regulatorische Antwort auf die Forderung nach mehr Cybersicherheit in der EU sowie als Reaktion auf die eskalierenden Cyberbedrohungen und Cyberkriminalität gesehen werden und stützt sich dabei auch auf die Erfahrungen der NIS-Richtline (NIS1).

[1] Quelle: Allianz Risk Barometer 2024, Allianz Commercial | Pressemitteilung
[2] Quelle: Allianz Risk Barometer 2024 – Top 10 Geschäftsrisiken in Österreich in 2024

2.2. Änderungen im Rahmen der NIS-2-Richtline

Zur Harmonisierung und Verbesserung des Sicherheitsniveaus in den Mitgliedsstaaten verschärft die NIS-2-Richtlinie einerseits die Anforderungen an die Cybersicherheit sowie Sanktionen und andererseits legt sie für verschiedene Sektoren strengere Anforderungen fest. Darüber hinaus werden Themen wie Cyber-Risikomanagement, Geschäftskontinuität, Kontrolle und Überwachung und Reaktion auf Vorfälle behandelt. Ein wesentlicher Punkt ist sicherlich, dass die Verantwortung beim Management liegt und nicht einfach vom Leitungsorgan an Mitarbeitende wie dem CISO oder „NIS-Verantwortlichen“ abgeschoben werden kann. Durch die Ausweitung des Anwendungsbereichs der NIS-2-Richtlinie auf mehr Organisationen gelten nun auch strengere Haftungsregeln für das Management der betroffenen Organisationen.

Die wesentlichen Ziele der Cybersicherheits-Richtlinie NIS2 umfassen unter anderem:

- Harmonisierung und Verbesserung des Sicherheitsniveaus in den Mitgliedsstaaten
- Angleichen von Sicherheitsanforderungen und Anforderungen an die Cybersicherheit verschärfen
- Abdecken mehrere Sektoren und Konzentration auf größere, mittlere und kritische Akteure
- Verschärfte Sanktionen bei Verstößen
- Straffen der Berichtspflichten
- Angleichen von Aufsicht und Durchsetzung
- Intensivieren und Ausbauen der operativen Zusammenarbeit (inkl. EU-Cyber-Krisenmanagement)

2.3. Anwendungsbereich der NIS-2-Richtline

Der Anwendungsbereich ist in Artikel 2 geregelt:

*„(1) Diese Richtlinie gilt für **öffentliche oder private Einrichtungen** der in den **Anhang I oder II genannten Art**, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben. […]“*

2.4. Betroffenheit & Prüfschema

Wer ist nun eigentlich von NIS2 betroffen? Als betroffen gelten mittlere und große Unternehmen bestimmter Sektoren sowie die Digitale Infrastruktur. Darüber hinaus sind Dienstleister (über vertragliche Vereinbarungen) und Lieferanten von NIS2-betroffenen Unternehmen indirekt betroffen (Schlagwort: Lieferkettengesetz).

Zur Evaluierung betroffener Einrichtungen ist eine Zuordnung des Unternehmens einerseits über die Unternehmensgröße und den Jahresumsatz und andererseits über die Sektoren-Zugehörigkeit zu treffen.

Die Klassifizierung der Unternehmensgröße basiert auf Empfehlungen und Definitionen der Kommission für KMU[3].

Größenklasse	**Beschäftigte (VZÄ)**		**Jahresumsatz [€]**		**Jahresbilanz [€]**
Kleines Unternehmen | KU	< 50	**und**	≤ 10 Mio.	**oder**	≤ 10 Mio.
Mittleres Unternehmen | MU	≥ 50 bis < 250	**und**	≤ 50 Mio.	**oder**	≤ 43 Mio.
Großes Unternehmen | GU	≥ 250	**oder**	> 50 Mio.	**und**	> 43 Mio.

[3] Benutzerleitfaden der EU-Kommission zur Definition von KMU, Empfehlung der Kommission Definition von KMU

Sektoren mit hoher Kritikalität (NIS-2-Richtline, Anhang I)

- Energie (1)
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen (1)
- Trinkwasser
- Abwasser (2)
- Digitale Infrastruktur (1)
- Verwaltung von IKT-Diensten (B2B) (2)
- Öffentliche Verwaltung (2)
- Weltraum (2)

Sektoren mit sonstiger Kritikalität (NIS-2-Richtline, Anhang II) Post- und Kurierdienste (2)

- Abfallbewirtschaftung (2)
- Produktion, Herstellung und Handel mit chemischen Stoffen (2)
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln (2)
- Verarbeitendes Gewerbe/Herstellung von Waren (2)
- Anbieter digitaler Dienste (1)
- Forschung (2)

Anmerkung: (1) Ergänzungen im Sektor | (2) neu gegenüber NIS1

Prüfschema

Folgende Prüfschritte dienen zur Feststellung der unmittelbaren Betroffenheit eines Unternehmens:

(1) Liegt die betreffende Einrichtung in der EU?

(2) Ist das Unternehmen eine Einrichtung entsprechend Spalte 3 des Anhangs I oder II?

(3) Handelt es sich um ein mittleres oder großes Unternehmen?
(Beachte etwaige Sonderregeln für Digitale Infrastruktur oder wenn das Unternehmen als kritisch eingestuft wird.)

(4) Handelt es sich um eine wesentliche oder wichtige Einrichtung?

NIS-2 betroffene Unternehmen

Wesentliche Einrichtungen	Wichtige Einrichtungen	Digitale Infrastruktur
▪ große Einrichtungen Anhang I ⇓ strengere Aufsicht (ex-ante) und höhere Strafdrohung	▪ mittlere Einrichtungen Anhang I ▪ große und mittlere Einrichtungen Anhang II	

2.5. Bußgelder und rechtliche Konsequenzen bei Nichteinhaltung der NIS-2-Richtline

Halten Unternehmen die Anforderungen der NIS-2-Richtline nicht ein beziehungsweise setzen die NIS-2-Richtline nicht korrekt um, können sie, in Abhängigkeit ihrer Einstufung als wesentliches oder wichtiges Unternehmen, mit erheblichen Strafen belegt werden.

- Wesentliche Unternehmen – belegt mit einer Geldbuße von mindestens 10 Mio. EUR oder 2 % des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr
- Wichtige Unternehmen – belegt mit einer Geldbuße von mindestens 7 Mio. EUR oder 1,4 % des gesamten weltweiten Jahresumsatzes

Neben den möglichen Bußgeldern können Leitungsorganen (Geschäftsführer:innen, Vorständ:innen, Prokurist:innen, Aufsichtsrät:innen) auch rechtliche Konsequenzen in Form der persönlichen Haftung drohen.

2.6. Wesentliche Anforderungen der NIS-2-Richtline

Die Anforderungen aus der NIS-2-Richtline heraus lassen sich in vier Hauptbereiche

- Unternehmerische Verantwortlichkeit,
- Cybersicherheit – Risikomanagement,
- Berichtspflichten und
- Zertifizierungsregelungen

unterteilen.

(1) Unternehmerische Verantwortlichkeit

Die Aufgaben der unternehmerischen Verantwortlichkeit umfassen neben der Verantwortung zur Einhaltung und Umsetzung der NIS-2-Richtline sowie Vorschriften im Allgemeinen auch die Verantwortung von Konsequenzen bei deren Nichteinhaltung sowie die Beaufsichtigung der Umsetzung des Risikomanagements im Bereich der Cybersicherheit. Zudem umfasst sie die Teilnahme an Schulungen zur Risikoerkennung und Risikobewertung der Cybersicherheit sowie die Organisation regelmäßiger Cybersicherheitsschulungen für Mitarbeitende.

(2) Cybersicherheit – Risikomanagement

Ziel des Cybersicherheit-Risikomanagements ist die Umsetzung von Strategien zur Risikominderung. Schwerpunktmäßig ist die Reaktion auf Zwischenfälle, die Sicherheit der Lieferkette und die Stärkung des Netzwerks zu legen. Darüber hinaus sind Zugangskontrollen und der Einsatz von Verschlüsselung zu verbessern.

Um den Schutz vor Cyberbedrohungen und die betriebliche Ausfallsicherheit zu gewährleisten, ist die Integration von IT- und OT-Sicherheit unerlässlich, da die Konvergenz von IT (Information Technology, Informationstechnologie) und OT (Operation Technology, Betriebstechnologie) eine erweiterte Angriffsfläche schafft.

Die Integration von IT- und OT-Sicherheit zur Einhaltung von NIS-2 ist damit eine der wesentlichen Anforderungen und bedeutet, dass Unternehmen ihre Sicherheitsstrategien für Informationstechnologie und Betriebstechnologie zusammenführen müssen und hier einen gesamtheitlichen Blick auf den Aspekt Sicherheit werfen.

Für die OT-Sicherheit kann der Standard IEC 62443, für IT-Sicherheit der Standard ISO 27001 herangezogen werden.

(3) Berichtspflichten

Im Rahmen der Berichtspflicht kann zwischen 3 Stufen unterschieden werden, wobei für jede die Erstellung von strikten Berichtsprotokollen zu beachten ist:

- 24h – Frühwarnung: Erster Alarm und Meldung an die Behörde (CERT/CSIRT);
  - Verdacht, ob Sicherheitsvorfall auf rechtswidriger oder böswilliger Handlung beruht und ob grenzüberschreitend;
- 72h – Meldung bis 72h nach Kenntnis des Sicherheitsvorfalls;
  - Detaillierter Bericht über Bewertung, Schweregrad und Auswirkungen und gegebenenfalls Indikatoren für eine Kompromittierung

- 1 Monat – Abschlussmeldung bis 1 Monat nach Meldung
  - Ausführliche Beschreibung, Angaben zur Art der Bedrohung, Ursachen, Abhilfemaßnahmen und gewonnener Erkenntnisse

Darüber hinaus tragen freiwillige Meldungen zu mehr Cybersicherheit bei!

- freiwillige Meldung von (Beinahe-)Cybersicherheitsvorfällen, und -bedrohungen an das CSIRT;
- Meldung von betrügerischen Nachrichten und Internetfallen an die Watchlist Internet;

(4) Zertifizierungsregelungen

Welche Unternehmen beziehungsweise Einrichtungen sich einer Zertifizierung / Audit in einem definierten Zeitrahmen unterziehen sollen oder müssen, wird durch die EU-Kommission festgelegt.

3. Conclusio und Ausblick

Die Forderung nach mehr Cybersicherheit in der EU in Folge der eskalierenden Cyberbedrohungen und steigenden Cyberkriminalität ist verständlich. Unternehmen müssen ihre Cyber-Resilienz steigern und demzufolge auf Cyber-Vorfälle bestens vorbereitet sein, um sich und seine Assets schützen zu können.

Je nachdem, wie das parlamentarische Gesetzgebungsverfahren ausgeht, wird sich zeigen, wie die Anforderungen der Cybersicherheits-Richtlinie NIS2 in welchem Umfang in nationales Gesetz übergeführt werden und ob beziehungsweise wo es ergänzende nationale Verschärfungen geben wird.

Bild: © iStock: metamorworks

Fachartikel: Sicherheit von Netz- und Informationssystemen (NIS)
NIS2-Richtlinie • NISG 2024
Ausgabe: 2024-04-30 v02 (1st Edition: 2024-04-18 v01)
Publiziert bei OVE: *Netz- und Informationssystemsicherheit* (www.ove.at, 2024-04-25)
Publiziert auf www.stragere.at (2024-05-02)

Stragere Management Consulting e.U.
Am Kirchenweg 8
3071 Böheimkirchen | Austria
office@stragere.at
www.stragere.at