INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

NISG-2026-Leitfaden für Internet Service Provider

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Inhaltsverzeichnis

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Einleitung

Mit der Kundmachung des Netz- und Informationssystemsicherheitsgesetzes 2026 (NISG 2026) im Bundesgesetzblatt treten für wesentliche und wichtige Einrichtungen der digitalen Infrastruktur neue, verbindliche Sicherheitsanforderungen in Kraft. Ziel dieses Leitfadens ist es, unseren Mitgliedern eine praxisnahe Orientierung zu bieten und das NISG 2026 systematisch vorzubereiten. Dabei geben wir Hilfestellung bei der Umsetzung zentraler Anforderungen wie **Betroffenheit, Risikomanagement, Verantwortlichkeiten, Sicherheit der Lieferkette, Meldepflichten sowie Sanktionen.**

Zentrale Fristen im Überblick:

- **23.12.2025**: Kundmachung des NISG 2026 im Bundesgesetzblatt
- **01.10.2026:** Inkrafttreten des NISG 2026; bisheriges NISG tritt außer Kraft
- **01.01.2027:** Frist für die Registrierung der betroffenen Einrichtungen
- **01.10.2027:** Frist für die Abgabe der Selbstdeklaration
- **01.10.2028:** Frühester Termin, zu dem eine **wesentliche Einrichtung** auf Aufforderung die operative und organisatorische Umsetzung der Risikomanagementmaßnahmen nachweisen muss.
- **30.09.2030:** Frühester Termin, zu dem eine **wesentliche Einrichtung** die technischen Risikomanagementmaßnahmen oder **wichtige Einrichtung** auf Aufforderung einen Prüfbericht hinsichtlich der technischen, operativen und organisatorischen Risikomanagementmaßnahmen einer unabhängigen Stelle vorlegen muss.
  Beachte: Die Nachweispflicht für wichtige Einrichtungen besteht nur bei begründeten Hinweisen.

Zuständige Behörde: Einrichtung eines Bundesamts für Cybersicherheit

1. direkt dem Bundesminister für Inneres unterstellt
2. organisatorisch eigenständig, außerhalb der Generaldirektion für öffentliche Sicherheit
3. bundesweite Zuständigkeit

Der **Strafvollzug** und die Verhängung von Verwaltungsstrafen obliegt den Bezirksverwaltungsbehörden.

Die **Meldung von Cybersicherheitsvorfällen** sowie die **Selbstdeklaration** sind über das Unternehmensserviceportal (https://www.usp.gv.at/) vorgesehen und derzeit in Planung. Sobald konkrete Informationen vorliegen, wird diese Information entsprechend aktualisiert.

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Betroffenheit

Im Rahmen des NISG 2026 ist für jede Einrichtung zunächst zu klären, ob Sie von den gesetzlichen Anforderungen betroffen ist und ob Sie als wesentliche oder wichtige Einrichtung einzustufen ist, um darauf aufbauend Pflichten wie Registrierung, Risikomanagement und Meldepflichten korrekt umzusetzen.

Wesentliche Einrichtungen nach der NIS2-Richtlinie sind große Unternehmen aus besonders kritischen Sektoren wie Energie, Verkehr, Bankwesen, Finanzmarkt, Gesundheit, Trinkwasser, Abwasser, Verwaltung von IKT-Diensten, **digitaler Infrastruktur** und Weltraum (Anhang I).

Wichtige Einrichtungen sind mittlere Unternehmen dieser Sektoren sowie große und mittlere Unternehmen aus weiteren Sektoren wie Post und Kurier, Abfall, Chemie, Lebensmittel, Produktion, digitale Dienste und Forschung (Anhang II).

Für den Sektor **„Digitale Infrastruktur“** (gemäß Anhang I der NIS2-Richtlinie) gelten besondere Ausnahmeregelungen hinsichtlich des Anwendungsbereichs und der Einstufung der Einrichtungen:

<table>
<tr><th>Sektor</th><th>Art der Einrichtung</th><th>groß</th><th>mittel</th><th>klein</th></tr>
<tr><td rowspan="9">Digitale Infrastruktur</td><td>TLD-Namenregister, qualifizierte Vertrauensdiensteanbieter</td><td colspan="3" rowspan="2">wesentlich</td></tr>
<tr><td>DNS Diensteanbieter (ausgenommen Betreiber von Root-Nameserver)</td></tr>
<tr><td>Anbieter öffentlicher elektronischer Kommunikationsnetze oder elektronischer Kommunikationsdienste</td><td colspan="2">wesentlich</td><td>wichtig</td></tr>
<tr><td>Vertrauensdiensteanbieter</td><td>wesentlich</td><td colspan="2">wichtig</td></tr>
<tr><td>Betreiber von Internet-Knoten</td><td rowspan="4">wesentlich</td><td rowspan="4">wichtig</td><td rowspan="4"></td></tr>
<tr><td>Anbieter von Cloud-Computing-Diensten</td></tr>
<tr><td>Anbieter von Rechenzentrumsdiensten</td></tr>
<tr><td>Betreiber von Content Delivery Networks (CDN)</td></tr>
<tr><td>Verwaltung von IKT-Diensten</td><td></td><td>wesentlich</td><td>wichtig</td><td></td></tr>
</table>

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Ob ein Unternehmen als „wesentliche“ oder „wichtige“ Einrichtung im Sinne der NIS2-Richtlinie eingestuft wird, spielt **für die Umsetzung der geforderten Sicherheitsmaßnahmen keine Rolle** - diese Anforderungen gelten für beide Gruppen gleichermaßen.

Allerdings bestehen Unterschiede bei der behördlichen Überwachung und bei möglichen Sanktionen:

Wesentliche Einrichtungen	Wichtige Einrichtungen
Unterliegen einer intensiven Aufsicht, einschließlich regelmäßiger und gezielter Prüfungen, auch ohne konkreten Anlass („ex-ante“) sowie bei Verdachtsfällen („ex-post“). **Es sind keine fixen Prüfzyklen vorgesehen**	Werden nur bei konkretem Verdacht auf Verstöße kontrolliert („ex-post“).
Es können Stichprobenkontrollen sowie Vor-Ort-Inspektionen durchgeführt werden.	Vor-Ort-Kontrollen sind ebenfalls möglich.
Die Behörden können nachträgliche Maßnahmen anordnen.	Auch hier sind nachträgliche Maßnahmen zulässig.
Im Falle eines Verstoßes drohen Geldbußen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Wert höher ist).	Hier liegt der Bußgeldrahmen bei maximal 7 Millionen Euro oder 1,4 % des weltweiten Jahresumsatzes.

Wesentliche und wichtige Einrichtungen unterliegen den Bestimmungen des NISG 2026, wenn sie in Österreich niedergelassen sind. Abweichend davon gelten die Bestimmungen dieses Hauptteils für folgende Einrichtungen nur unter den nachstehenden Voraussetzungen:

1. Für Anbieter öffentlicher Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, sofern sie ihre Leistungen in Österreich bereitstellen;

2. Für DNS-Diensteanbieter, TLD-Namensregister, Stellen die Registrierungsdienste für Domänennamen erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltsübermittlungsnetzen (Content Delivery Networks), Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder sozialen Netzwerkplattformen, wenn sie in Österreich Dienste anbieten und
   a) sich ihre Hauptniederlassung in Österreich befindet oder
   b) sie weder in Österreich noch in einem anderen Mitgliedstaat der Europäischen Union einen Vertreter gemäß Absatz 4 benannt haben.

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Die **Einstufung einer Einrichtung nach Größe** als „mittleres Unternehmen“ oder als „großes Unternehmen“ richtet sich nach der Anzahl der Mitarbeiter, dem Jahresumsatz und der Jahresbilanzsumme.

Unternehmensgröße	**Mitarbeiterzahl**	**Jahresumsatz**	**Jahresbilanzsumme**	**NIS2-Anwendung**
Kleines Unternehmen	< 50	≤ 10 Mio. €	≤ 10 Mio. €	Fällt **nicht** unter NIS2, außer in bestimmten Ausnahmefällen (siehe unten)
Mittleres Unternehmen	≥ 50	**ODER** > 10 Mio. €	**UND** > 10 Mio. €	Fällt unter NIS2
Großes Unternehmen	≥ 250	**ODER** > 50 Mio. €	**UND** > 43 Mio. €	Fällt unter NIS2

Unabhängig von der Unternehmensgröße fallen folgende Unternehmen unter NIS2:

1. Vertrauensdiensteanbieter
2. Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste
3. TLD-Namenregister
4. DNS-Diensteanbieter (ausgenommen Betreiber von Root-Namenservern).

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

NIS2-Governance

1. **Klärung der Relevanz**
   Prüfen Sie, ob Ihr Unternehmen von den Anforderungen der NIS2-Richtlinie betroffen ist. Berücksichtigen Sie dabei die Branche, die Unternehmensgröße sowie die angebotenen Dienste.

2. **Ressourcenplanung**
   Stellen Sie sicher, dass ausreichend personelle, finanzielle und technische Ressourcen für die Umsetzung der NIS2-Anforderungen zur Verfügung stehen.

3. **Verantwortlichkeiten festlegen**
   Bestimmen Sie klare Zuständigkeiten und benennen Sie Ansprechpersonen für die Umsetzung und Überwachung aller NIS2-relevanten Maßnahmen. Leitungsorgane und Mitarbeitende sollten regelmäßig zu ihren Aufgaben und zum sicheren Umgang mit IT-Systemen geschult werden.

4. **Unternehmensziele definieren**
   Verankern Sie die NIS2-Anforderungen in den strategischen Zielen des Unternehmens und sorgen Sie für eine angemessene Priorisierung der Cybersicherheit.

5. **Asset- und Dienstmanagement**
   Identifizieren Sie die für Ihr Unternehmen kritischen Dienste und Assets. Bewerten Sie deren Bedeutung für das Unternehmen und ordnen Sie ihnen eine Kritikalitätsstufe zu.

6. **Risikomanagement**
   Führen Sie eine Risikoanalyse durch: Identifizieren Sie anhand der kritischen Assets und dafür relevante Bedrohungen konkrete Risiken. Bewerten Sie in einem zweiten Schritt die Eintrittswahrscheinlichkeit dieser Risiken und mögliche Auswirkungen.

7. **Maßnahmenplanung und Umsetzung**
   Leiten Sie geeignete technische und organisatorische Maßnahmen ab, um identifizierte Risiken zu behandeln, und setzen Sie diese konsequent um.

8. **Identifikation und Behandlung von Schwachstellen**
   Definieren Sie Prozesse um Schwachstellen laufend zu identifizieren und diese zeitnahe zu behandeln.

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

9. **Kontinuitäts- und Notfallmanagement**
   Etablieren Sie Prozesse zur Aufrechterhaltung des Geschäftsbetriebs und zur Bewältigung von Notfällen, einschließlich regelmäßiger Überprüfung und Aktualisierung der Notfallpläne.

10. **Meldewesen und Berichtspflichten**
    Implementieren Sie ein System zur rechtzeitigen Meldung von Sicherheitsvorfällen an die zuständigen Behörden und stellen Sie sicher, dass alle Berichtspflichten eingehalten werden.

Hinweis:
Dieser Leitfaden bietet eine strukturierte Orientierung für die Umsetzung der NIS2-Richtlinie in Ihrem Unternehmen. Detaillierte Maßnahmen und Prozesse sollten individuell an die spezifischen Anforderungen und Gegebenheiten Ihres Unternehmens angepasst werden.

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Allgemeines Risikomanagement

Gemäß § 32 Abs 2 NISG sind Einrichtungen verpflichtet, ihre Netz- und Informationssysteme sowie deren physische Komponenten risikobasiert abzusichern und dabei ein dem jeweiligen Gefahrenpotenzial angemessenes Sicherheitsniveau durch einen **ganzheitlichen, gefahrenübergreifenden Ansatz** zu gewährleisten.

Welche Risikomanagementmaßnahmen sind umzusetzen?

1. Entwicklung von Konzepten zur Risikoanalyse und zur Absicherung von Informationssystemen, einschließlich klarer Definitionen von Rollen, Verantwortlichkeiten und Weisungsrechten

2. Maßnahmen zur Bewältigung und Reaktion auf Cybersicherheitsvorfälle

3. Sicherstellung des laufenden Betriebs, etwa durch ein effektives Backup- und Wiederherstellungsmanagement im Notfall sowie durch ein strukturiertes Krisenmanagement

4. Absicherung der Lieferkette, insbesondere im Hinblick auf unmittelbare Anbieter und Dienstleister

5. Umsetzung von Sicherheitsmaßnahmen beim Erwerb, der Entwicklung und Wartung von Netz- und Informationssystemen – inklusive Schwachstellenmanagement und Offenlegung von Sicherheitslücken

6. Entwicklung und Anwendung von Verfahren zur Evaluierung der Effektivität bestehender Risikomanagementmaßnahmen im Bereich Cybersicherheit

7. Implementierung grundlegender Verfahren für Cyberhygiene und Durchführung entsprechender Schulungen für Mitarbeitende

8. Erarbeitung und Anwendung von Richtlinien und Prozessen für den Einsatz von Kryptografie und, falls erforderlich, Verschlüsselung

9. Schutzmaßnahmen im Bereich Personalsicherheit, Konzepte für Zugriffsberechtigungen sowie das Management betrieblicher Anlagen

10. Nutzung von Multi-Faktor-Authentifizierung oder kontinuierlicher Authentifizierung, sichere Kommunikationssysteme für Sprache, Video und Text und, falls notwendig, zusätzlich abgesicherte Notfallkommunikationslösungen innerhalb der Einrichtung

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Bei der **Umsetzung von Risikomanagementmaßnahmen** sind zu berücksichtigen:

- Der Stand der Technik
- Einschlägige nationale, europäische und internationale Normen
- Best-Practices (bewährte Verfahren und Methoden)

Das NISG 2026 verfolgt im Risikomanagement einen risikobasierten Ansatz. **Risikobasiert** heißt, dass Maßnahmen zur Cybersicherheit gezielt an die tatsächlichen individuellen Risiken angepasst werden. Statt pauschaler Vorgaben werden Bedrohungen und Schwachstellen individuell bewertet, und die Schutzmaßnahmen richten sich nach dem jeweiligen Gefährdungspotenzial. Maßnahmen sollen regelmäßig überprüft und angepasst werden, sobald sich die Risikosituation verändert.

Risikomanagement für die Sektoren der digitalen Infrastruktur

Mit der neuen Regelung besteht nunmehr nach § 32 Abs 5 NISG 2026 eine ausdrückliche **Verordnungsermächtigung für das Bundesamt für Cybersicherheit (Cybersicherheitsbehörde)**, die es ermöglicht, die Anforderungen an das Risikomanagement für bestimmte Sektoren verbindlich festzulegen.

Für alle Sektoren der digitalen Infrastruktur – mit Ausnahme Anbieter öffentlicher elektronischer Kommunikationsnetze und –dienste – gelten ab Inkrafttreten des NISG 2026 die Vorgaben der EU-Durchführungsverordnung.

Für den Teilsektor der **Anbieter öffentlicher elektronischer Kommunikationsnetze und -dienste** wird noch eine nationale Verordnung zu den Risikomanagementmaßnahmen erlassen. Dabei stellt sich die Frage, ob es hierfür eine eigene Durchführungsverordnung geben wird oder ob die bereits bestehende EU-Durchführungsverordnung für den digitalen Sektor auch auf diesen Teilsektor ausgeweitet wird.

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Meldepflichten

Die Meldepflichten für **wesentliche und wichtige Einrichtungen** sind in § 34 NISG geregelt. Betroffene Einrichtungen müssen unverzüglich jeden **erheblichen Cybersicherheitsvorfall** (§ 35) melden.

Ein **erheblicher Cybersicherheitsvorfall** gilt gemäß § 35 Abs 1 als solcher, wenn er:

1. schwerwiegende Betriebsstörungen der erbrachten Dienste der Einrichtung oder schwerwiegende finanzielle Verluste für die Einrichtung verursacht hat oder verursachen kann, oder

2. andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Nachfolgend werden die konkreten Meldefristen für Sicherheitsvorfälle übersichtlich dargestellt.

- **Unverzüglich, innerhalb von 24 Stunden**: Frühwarnung (ggf. Verdacht auf rechtswidrige und schuldhafte Handlung oder grenzüberschreitende Auswirkungen)
- **Unverzüglich, jedenfalls innerhalb von 72 Stunden**: Meldung (Schweregrad, Auswirkungen, etc.)
- **Spätestens einen Monat nach Frühwarnung**: Abschlussbericht (Beschreibung Vorfall, einschließlich Schweregrad und Auswirkungen, Art der Bedrohung, Ursachen, Abhilfemaßnahmen)
- Wesentliche, wichtige sowie Einrichtungen, die nicht in den Anwendungsbereich des NISG 2026 fallen, können gemäß § 36 NISG 2026 auf **freiwilliger Basis** relevante Cybersicherheitsinformationen (z. B. über Bedrohungen, Schwachstellen, Beinahe-Vorfälle und Abwehrmaßnahmen) austauschen, um die Prävention, Erkennung, Reaktion und Wiederherstellung bei Cybervorfällen zu unterstützen.
- Kommt es im Rahmen eines Cybersicherheitsvorfalls auch zu einer Verletzung des Schutzes personenbezogener Daten (Data Breach), sind zusätzlich die Melde- und Berichtspflichten nach der DSGVO sowie dem TKG 2021 einzuhalten.

Die **Meldung von Cybersicherheitsvorfällen** ist derzeit über das Unternehmens-Service-Portal (https://www.usp.gv.at/) vorgesehen. Sobald konkrete Informationen vorliegen, wird diese Information entsprechend aktualisiert.

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Pflichten wichtiger Einrichtungen

Zeitpunkt / Auslöser	**Verpflichtung**	**Gesetzliche Grundlage**
Ab Inkrafttreten 01.10.2026	Risikomanagementmaßnahmen umsetzen	§ 32 NISG
Ab Inkrafttreten 01.10.2026	Governance-Strukturen für Informationssicherheit etablieren	§ 31 NISG
Bei erheblichem Cybersicherheitsvorfall	Meldung an die zuständige Behörde (24h, 72h, 1 Monat)	§ 34 NISG
Innerhalb von 3 Monaten nach Inkrafttreten	Registrierung bei der zuständigen Behörde	§ 29 NISG
Innerhalb von 12 Monaten ab Registrierung	Selbstdeklaration der umgesetzten Risikomanagementmaßnahmen inkl. Sicherheit der Lieferkette (gemäß dem Formular der Behörde) einreichen	§ 33 NISG
Innerhalb von **2 Jahren** nach Aufforderung durch die Cybersicherheitsbehörde	Nachweis der technischen, operativen und organisatorischen Risikomanagementmaßnahmen durch externe Stellen, wobei operative und organisatorische Maßnahmen auch durch Zertifikate wie ISO 27001 nachgewiesen werden können	§ 33 NISG

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Pflichten wesentlicher Einrichtungen

Zeitpunkt / Auslöser	Verpflichtung	Gesetzliche Grundlage
Ab Inkrafttreten 01.10.2026	Risikomanagementmaßnahmen umsetzen	§ 32 NISG
Ab Inkrafttreten 01.10.2026	Governance-Strukturen für Informationssicherheit etablieren	§ 31 NISG
Bei erheblichem Cybersicherheitsvorfall	Meldung an die zuständige Behörde (24h, 72h, 1 Monat)	§ 34 NISG
Innerhalb von 3 Monaten nach Inkrafttreten	Registrierung bei der zuständigen Behörde	§ 29 NISG
Innerhalb von 12 Monaten ab Registrierung	Selbstdeklaration der umgesetzten Risikomanagementmaßnahmen inkl. Sicherheit der Lieferkette einreichen	§ 33 NISG
Innerhalb von **2 Monaten** nach Aufforderung durch die Cybersicherheitsbehörde	Nachweis der operativen und organisatorischen Risikomanagementmaßnahmen durch externe Stellen (kann auch durch Zertifikate wie ISO 27001 nachgewiesen werden)	§ 33 NISG
Innerhalb von **2 Jahren** nach Aufforderung durch die Cybersicherheitsbehörde	Nachweis der technischen Risikomanagementmaßnahmen durch externe Stellen	§ 33 NISG

Es besteht kein gesetzlich festgelegter Prüfzyklus für wesentliche Einrichtungen. Die zuständige Behörde kann Prüfungen flexibel und in Abhängigkeit von der aktuellen sektorspezifischen Bedrohungslage anfordern. Unabhängig davon muss die Sicherheit der Einrichtung jederzeit gewährleistet sein. Im Falle einer behördlichen Prüfung müssen die erforderlichen Nachweise innerhalb des gesetzlich vorgesehenen Zeitrahmens vorgelegt werden können.

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Sicherheit der Lieferkette

Die nachgelagerten Unternehmen in der Lieferkette sind gemäß NIS2 indirekt betroffen. Je nach Risikobewertung sind geeignete Maßnahmen bei der Auswahl und Steuerung von Lieferanten und Dienstleistern umzusetzen.

Empfohlene Maßnahmen:

- Entwicklung eines Konzepts zur Absicherung der Lieferkette, basierend auf einer Risikobewertung
- Überprüfung der Cybersicherheitsqualität und Resilienz von IKT-Produkten und -Diensten bei Lieferanten
- Definition risikobasierter Auswahlkriterien für Anbieter und Dienstleister
- Vertragsgestaltung mit klaren Cybersicherheitsanforderungen und Leistungsvereinbarungen
- Führen eines aktuellen Verzeichnisses aller relevanten Anbieter, Dienstleister, Produkte und Prozesse
- Einfordern von Nachweisen, z. B. bestehende ISO 27001-Zertifizierungen oder vergleichbare Standards
- Regelmäßige Überprüfung und Anpassung dieser Lieferantenbewertung entsprechend der aktuellen Risikolage

Im Rahmen der NIS2-Anforderungen sind Organisationen verpflichtet, nicht nur ihre eigenen Systeme und Prozesse, sondern auch die Sicherheit in der Zusammenarbeit mit externen Partnern, Zulieferern und Dienstleistern zu gewährleisten. Ziel ist es, Risiken, die durch die Einbindung Dritter entstehen können, frühzeitig zu erkennen und gezielt zu steuern. Bereits bei der Auswahl von Lieferanten sollten Sicherheitsaspekte berücksichtigt und bei Bedarf vertraglich festgelegt werden. Die Einhaltung dieser Anforderungen sollte regelmäßig durch Kontrollen, Audits oder andere geeignete Maßnahmen überprüft werden.

Als Orientierung für angemessene Nachweise innerhalb der Lieferkette empfiehlt die zuständige Behörde insbesondere Betreibern wesentlicher Dienste, sich an etablierten Standards und Leitlinien zu orientieren. Dazu zählen etwa:

- das österreichische Informationssicherheitshandbuch
- die internationale Norm ISO/IEC 27001, IEC 62443 2-1 mit Fokus auf Lieferkettensicherheit
- die CIS Controls in der aktuellen Version 8.0
- sowie das Cyber Risk Rating des KSÖ, insbesondere die Anforderungen für die Einstufungen A und B.

INTERNET SERVICE PROVIDERS AUSTRIA

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Verantwortlichkeit der Leitung nach NIS2

Verantwortung der Leitung

Die oberste Verantwortung für die Umsetzung der NIS2-Anforderungen liegt bei der Leitung des Unternehmens. Die Leitungsorgane wesentlicher und wichtiger Einrichtungen müssen an für diese spezifisch gestalteten Cybersicherheitsschulungen teilnehmen. Die Einrichtungen haben weiters ihren Mitarbeitern regelmäßigen Schulungen zu unterziehen, damit diese ausreichenden Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste erwerben können.

Wer zählt zur Leitung?

Zur Leitung gehören nunmehr der **Vorstand und die Geschäftsführung** (Aufsichtsräte gelten nicht (mehr) als Leitungsorgane).

Aufgaben der Leitung

- Gesamtverantwortung für Informationssicherheit und NIS2-Umsetzung
- Festlegung strategischer Ziele für Informationssicherheit und Krisenmanagement
- Bereitstellung notwendiger Ressourcen (Personal, Budget, Zeit)
- Ernennung und Unterstützung verantwortlicher Fachkräfte (z. B. IT-Sicherheitsbeauftragte, Risikomanager)
- Genehmigung von Sicherheitsrichtlinien und Notfallplänen
- Überprüfung und Freigabe von Risikobewertungen und Maßnahmen
- Förderung einer unternehmensweiten Sicherheitskultur
- Wahrnehmung der rechtlichen Verantwortung und Haftung

Währinger Straße 3/18
1090 Wien, Austria
+43 1 409 55 76
office@ispa.at | **www.ispa.at**

Sanktionen

Wesentliche Einrichtungen:
Bei einer Verwaltungsübertretung kann eine Geldstrafe von bis zu 10 Millionen Euro oder bis zu 2 % des gesamten weltweiten Umsatzes des Unternehmens im vorangegangenen Geschäftsjahr verhängt werden – maßgeblich ist der jeweils höhere Betrag.

Wichtige Einrichtungen:
Bei einer entsprechenden Verwaltungsübertretung droht eine Geldstrafe von bis zu 7 Millionen Euro oder bis zu 1,4 % des gesamten weltweiten Umsatzes des zugehörigen Unternehmens im vorangegangenen Geschäftsjahr – auch hier gilt der höhere Betrag.

Verhältnis zu anderen Gesetzen

RKEG: Das RKEG regelt die physische Resilienz kritischer Einrichtungen, während das NISG (bzw. die NIS2-Richtlinie) die Anforderungen an die Cybersicherheit vorgibt. Für digitale Infrastruktureinrichtungen sieht der Entwurf des RKEG ausdrücklich vor, dass zentrale Verpflichtungen wie Risikoanalyse (§ 14), Resilienzmaßnahmen (§ 15), Meldepflichten (§ 17), nicht doppelt anzuwenden sind, sofern die Anforderungen der NIS2-Richtlinie bereits vollständig und wirksam umgesetzt werden. Dadurch wird eine Doppelregulierung vermieden. Voraussetzung ist allerdings, dass auch im Rahmen der NIS2-Umsetzung die physische Sicherheit nach den Vorgaben des RKEG berücksichtigt wird.

TK-NSiV 2020: Die Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020) regelt spezifische Sicherheitsanforderungen für Betreiber elektronischer Kommunikationsnetze sowie Anbieter elektronischer Kommunikationsdienste in Österreich. Ziel der Verordnung ist es, ein angemessenes Sicherheitsniveau für elektronische Kommunikationsnetze und -dienste sicherzustellen und Risiken für den Netzbetrieb zu minimieren. Im Kontext der Umsetzung der NIS-2-Richtlinie ist derzeit noch nicht abschließend geklärt, wie sich diese sektorspezifische Verordnung künftig im Verhältnis zum NISG 2026 verhält. Insbesondere ist offen, ob die TK-NSiV 2020 aufgehoben, angepasst oder teilweise durch neue Regelungen im Rahmen der nationalen NIS-2-Umsetzung ersetzt wird. Daher ist mit möglichen Anpassungen oder einer Harmonisierung der bestehenden Anforderungen zu rechnen.

Anmerkung: Dieser Leitfaden bildet die aktuell geltende Rechtslage ab. Auf EU-Ebene ist eine Novellierung der NIS2-Richtlinie geplant, insbesondere zur Entlastung kleinerer und mittlerer Unternehmen durch die Einführung der Kategorie „Small Mid-Caps“. Zudem ist vorgesehen, dass DNS-Diensteanbieter künftig nicht mehr automatisch und unabhängig von ihrer Größe als wesentliche Einrichtungen erfasst werden. Sobald konkrete Änderungen vorliegen, informieren wir unsere Mitglieder und passen den Leitfaden entsprechend an.