NIS2-Betroffenheits-Matrix

Autor: Dietmar Csitkovics
Datum/Version: 31.07.2024, V2

Matrix

Diese NIS2-Matrix bietet einen Überblick zur Einordnung der Betroffenheit von Unternehmen je nach Unternehmensgröße in Abhängigkeit der Branche laut der NIS2-Richtlinie:
https://loesungsagentur.at/NIS2-Richtlinie-2022-2555

	von NIS2/NISG betroffen (**wesentlich**)	von NIS2/NISG betroffen (**wichtig**)
große Unternehmen = mind. 250 Mitarbeiter (VZÄ) ODER 50 Mio Jahresumsatz UND 43 Mio Jahresbilanz	A1, DD1 - DD4	A2
mittlere Unternehmen = mind. 50 Mitarbeiter (VZÄ) ODER 10 Mio Jahresumsatz UND Jahresbilanz	DD1 + DD2	A1 + A2, DD3 + DD4
kleine Unternehmen = unter 50 Mitarbeiter (VZÄ) + bis 10 Mio. Jahresumsatz ODER Jahresbilanz	X	DD2 + DD3
Töchter/Partner = verbundenen Unternehmen über 50% Beteiligungen + Partner ab 25 bis 50% Beteiligungen	LK	LK
Bundeseinrichtungen = Behörden/Verwaltung ausg. Militär, Gericht, Gesetzgebung, Unis/FH und Einrichtungen für nationale/öffentliche Sicherheit	A1	X
Landeseinrichtungen = Landesregierung und Bezrikshauptmannschaften	X	A1
Große Gemeinden ab 50 DN nur als Verwalter/Betreiber wesentliche Einrichtungen (RKE-Richtlinie = Resilient Kritischer Einrichtungen)	A1	X

Abbildung 1: NIS2-Betroffenheits-Matrix

Legende

A1 = Anhang 1	Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten (B2B), öffentliche Verwaltung, Weltraum
A2 = Anhang 2	Post- und Kurierdienste, Abfallbewirtschaftung, Chemie (Herstellung und Handel), Lebensmittel (Großhandel, ind. Produktion und Verarbeitung), verarbeitendes Gewerbe/Herstellung von Waren, Anbieter digitaler Dienste, Forschung
DD1 = Digitale Dienste 1	TLD-Namenregister (qualifizierte Vertrauensdiensteanbieter), DNS-Dienstanbieter
DD2 = Digitale Dienste 2	Anbieter öffentlicher elektronischer Kommunikationsnetze oder wesentlich elektronischer Kommunikationsdienste
DD3 = Digitale Dienste 3	Vertrauensdiensteanbieter
DD4 = Digitale Dienste 4	Betreiber von Internet-Knoten, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks (CDN), Verwaltung von IKT-Diensten
LK = Lieferkette	Verbundene oder Partner-Unternehmen, Digitale Infrastruktur, Lieferkette (indirekt über Kunden betroffen), wesentlich/wichtig eingestuft oder kritische Einrichtung

Lösungsagentur GmbH | Eisenstädter Straße 76, Tür 2 | A-7350 Oberpullendorf | Austria | office@loesungsagentur.at
IBAN: AT24 3306 5000 0013 1193 | BIC: RLBBAT2E065 | UID: ATU 73431958 | FN: 494321v | www.loesungsagentur.at

Maßnahmen

Aus der Einordnung über die Matrix, der NIS2-RL und dem NISG (Netz-Informations-Sicherheits-Gesetz in Österreich) ergeben sich diese wichtigsten Handlungsempfehlungen, Strafen und Pflichten:

Was ist zu tun?	Leitungsorgane (verantwortlich laut § 31 NISG 2024): - Risikomanagement sicherzustellen (10 Maßnahmen) - Haftung für verursachte Schäden - Cybersecurity/Awareness-Schulungen für User und Leitungsbene - Lieferkette prüfen und ADV+
Strafen und Sanktionen	wesentlich: - 10 Mio EUR oder 2% des weltweiten - Jahresumsatzes (Sanktionen § 45 NISG 2024) wichtig: - 7 Mio EUR oder 1,4% des weltweiten - Jahresumsatzes (Sanktionen § 45 NISG 2024) - Verwaltungsstrafen der Bezirksverwaltungsbehörden
Pflichten	wesentlich/wichig: - Gültigkiet nach Inkraftreten NISG, also 27. Oktober 2024 - Registrierung §29 NISG nach spät. 3 Monaten - Risikomanagementmaßnahmen §32 NISG - binne 6 Monaten nach Aufforderung: Aufstellung Risikomanagementmaßnahmen §33 NISG - Meldung erheblicher Vorfälle §34 NISG - Governance-Maßnahmen §31 NISG + innerhalb von 3 Jahren nach Aufforderung: Prüfung durch unabhängige Stelle §33

Fazit und Status

Die NIS-Richtlinie betrifft aktuell ca. 500 Unternehmen in Österreich. Durch die NIS2 werden laut Experten ca. um den Faktor 10 mehr Unternehmen betroffen sein, also rund 5.000 Betriebe, die sich direkt und dringend mit dem Thema beschäftigen sollten. Durch die Lieferkette werden wohl mehr als 10.000 Betriebe direkt oder indirekt betroffen sein.

Wie schon in DSGVO-Zeiten sollte man sich entsprechend des Risikos, also Eintrittswahrscheinlichkeit zu Schadensausmaß, von Sicherheitsvorfällen und Datenschutzpannen vorbereiten. Dazu sollte der aktuelle Status geprüft und danach eine Strategie für einen nachhaltigen Prozess der IT-Security-Optimierung entwickelt werden. Unseren Kund:innen kennen diesen Prozess als DocuSec. Diese Methode der „dokumentierten Security" bietet auf die Firmengröße angepasste Audits, Reviews, Retrospektiven und Awareness-Maßnahmen.

Gerne beraten wir zu passenden Förderungen und Maßnahmen zur NIS2-Umsetzung.

Lösungsagentur GmbH | Eisenstädter Straße 76/2 | 7350 Oberpullendorf
office@loesungsagentur.at | www.Lösungsagentur.at
Bitte beachten Sie unsere Datenschutzerklärung