Kurztitel

Netz- und Informationssystemsicherheitsgesetz 2026

Kundmachungsorgan

BGBl. I Nr. 94/2025

Typ

BG

§/Artikel/Anlage

§ 32

Inkrafttretensdatum

01.10.2026

Abkürzung

NISG 2026

Index

41/01 Sicherheitsrecht

Text

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

§ 32. (1) Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu reduzieren und die Auswirkungen von Cybersicherheitsvorfällen auf die Nutzer ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

(2) Die Risikomanagementmaßnahmen haben zudem unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen nationalen, europäischen und internationalen Normen sowie bewährter Verfahren und der Kosten der Umsetzung ein Cybersicherheitsniveau zu gewährleisten, das dem bestehenden Risiko angemessen ist.

(3) Bei der Beurteilung der Verhältnismäßigkeit der Risikomanagementmaßnahmen sind das Ausmaß der Risikoexposition der Einrichtung sowie ihrer Dienste, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Cybersicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(4) Diese Risikomanagementmaßnahmen haben auf einem gefahrenübergreifenden Ansatz zu beruhen, der auf den Schutz der Netz- und Informationssysteme samt deren physischen Komponenten vor Cybersicherheitsvorfällen abzielt, und zumindest folgende Inhalte zu umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Cybersicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder

Diensteanbietern, unter Berücksichtigung der spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, der Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Dienstanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, sowie der Ergebnisse der gemäß Art. 22 Abs. 1 NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(5) Die Cybersicherheitsbehörde ist ermächtigt, durch Verordnung nähere Anforderungen an die Risikomanagementmaßnahmen gemäß Abs. 4 festzulegen. Dabei kann die Cybersicherheitsbehörde insbesondere anordnen, dass die von der Europäischen Kommission auf Grundlage des Art. 21 Abs. 5 NIS-2-Richtlinie hinsichtlich einzelner Sektoren oder bestimmter Arten von Einrichtungen erlassenen Durchführungsrechtsakte zur Festlegung technischer und methodischer Anforderungen an Risikomanagementmaßnahmen auch auf andere Sektoren oder Arten von Einrichtungen anwendbar sind, wobei sektorspezifische Besonderheiten Berücksichtigung finden können.

Schlagworte

Netzsystem, Sprachkommunikation, Videokommunikation

Zuletzt aktualisiert am

30.12.2025

Gesetzesnummer

20013065

Dokumentnummer

NOR40273893