Kurztitel

Netz- und Informationssystemsicherheitsgesetz 2026

Kundmachungsorgan

BGBl. I Nr. 94/2025

Typ

BG

§/Artikel/Anlage

§ 33

Inkrafttretensdatum

01.10.2026

Abkürzung

NISG 2026

Index

41/01 Sicherheitsrecht

Text

Nachweis der Wirksamkeit von Risikomanagementmaßnahmen

§ 33. (1) Wesentliche und wichtige Einrichtungen haben innerhalb von zwölf Monaten nach Eintritt der Registrierungspflicht gemäß § 29 Abs. 2 der Cybersicherheitsbehörde Informationen hinsichtlich umgesetzter Risikomanagementmaßnahmen gemäß § 32, insbesondere betreffend die genutzten Netz- und Informationssysteme und die Sicherheit der Lieferketten sowie die Ergebnisse der durchgeführten Risikoanalyse, nach den Vorgaben der Cybersicherheitsbehörde in strukturierter Form zu übermitteln (Selbstdeklaration).

(2) Wesentliche und wichtige Einrichtungen haben innerhalb von zwei Jahren nach Aufforderung durch die Cybersicherheitsbehörde die technische, operative und organisatorische Umsetzung der Risikomanagementmaßnamen gemäß § 32 durch eine von einer unabhängigen Stelle nach den Vorgaben der Cybersicherheitsbehörde sowie auf Basis der von der jeweiligen Einrichtung durchgeführten Risikoanalyse oder einer aufgrund sonstiger Risikoabwägungen durchgeführten Prüfung, die nicht länger als zwei Jahre zurückliegt, nachzuweisen, wobei der Nachweis der operativen sowie organisatorischen Umsetzung auch durch einschlägige gültige Zertifikate möglich ist. Davon abweichend haben wesentliche Einrichtungen die operative sowie organisatorische Umsetzung der Risikomanagementmaßnahmen innerhalb von zwei Monaten nach Aufforderung durch die Cybersicherheitsbehörde nachzuweisen. Für Aufforderungen in Bezug auf wichtige Einrichtungen gilt § 38 Abs. 2 sinngemäß. Die erstmalige Aufforderung kann frühestens nach Ablauf von zwei Jahren ab Inkrafttreten dieses Bundesgesetzes erfolgen.

(3) Zum Nachweis der Umsetzung der Risikomanagementmaßnahmen durch eine von einer unabhängigen Stelle durchgeführte Prüfung gemäß Abs. 2 hat die jeweilige Einrichtung der Cybersicherheitsbehörde einen von ihren Leitungsorganen sowie den eingesetzten unabhängigen Prüfern unterzeichneten Prüfbericht über die Umsetzung der Risikomanagementmaßnahmen einschließlich

festgestellter Mängel und einen Maßnahmenplan zur Beseitigung der Mängel nach den Vorgaben der Cybersicherheitsbehörde in strukturierter Form zu übermitteln.

(4) Die Kosten von Prüfungen durch unabhängige Stellen sind von der geprüften Einrichtung zu tragen, es sei denn, die Cybersicherheitsbehörde trifft in hinreichend begründeten Fällen eine anderslautende Entscheidung.

(5) Wesentliche und wichtige Einrichtungen haben der Cybersicherheitsbehörde geplante Prüfungen durch unabhängige Stellen spätestens einen Monat im Voraus nach den Vorgaben der Cybersicherheitsbehörde durch Übermittlung eines Prüfplans, aus dem die Einzelheiten der beabsichtigten Prüfung hervorgehen, bekannt zu geben.

Schlagworte

Netzsystem

Zuletzt aktualisiert am

30.12.2025

Gesetzesnummer

20013065

Dokumentnummer

NOR40273894