Kurztitel

Netz- und Informationssystemsicherheitsgesetz 2026

Kundmachungsorgan

BGBl. I Nr. 94/2025

Typ

BG

§/Artikel/Anlage

§ 34

Inkrafttretensdatum

01.10.2026

Abkürzung

NISG 2026

Index

41/01 Sicherheitsrecht

Text

Berichtspflichten

§ 34. (1) Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen sektorspezifischen CSIRT oder den für sie zuständigen sektorspezifischen CSIRTs, in Ermangelung eines solchen dem nationalen CSIRT, unverzüglich jeden erheblichen Cybersicherheitsvorfall (§ 35) zu melden. Das CSIRT leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter.

(2) Für die Zwecke der Meldung gemäß Abs. 1 haben die betroffenen Einrichtungen dem CSIRT Folgendes zu übermitteln:

1. unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Cybersicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Cybersicherheitsvorfall auf rechtswidrige und schuldhafte Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;
2. unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Cybersicherheitsvorfalls, eine Meldung über den Cybersicherheitsvorfall, in der gegebenenfalls die unter Z 1 genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Cybersicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;
3. auf Ersuchen eines CSIRTs oder gegebenenfalls der Cybersicherheitsbehörde einen Zwischenbericht über relevante Statusaktualisierungen;
4. spätestens einen Monat nach Übermittlung der Meldung des Cybersicherheitsvorfalls gemäß Z 2 einen Abschlussbericht, der Folgendes enthält:
   a) eine ausführliche Beschreibung des Cybersicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

b) Angaben zur Art der Bedrohung und zu den zugrundeliegenden Ursachen, die wahrscheinlich den Cybersicherheitsvorfall ausgelöst haben;

c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Cybersicherheitsvorfalls;

5. soweit der Cybersicherheitsvorfall zum Zeitpunkt der Fälligkeit der Vorlage des Abschlussberichts gemäß Z 4 noch andauert, haben die betreffenden Einrichtungen bis zu diesem Zeitpunkt einen Fortschrittsbericht zu übermitteln, wobei der Abschlussbericht bis spätestens einen Monat nach Beendigung der Vorfallsbehandlung übermittelt werden muss.

Abweichend von Z 2 unterrichtet ein Vertrauensdiensteanbieter das CSIRT in Bezug auf erhebliche Cybersicherheitsvorfälle, die sich auf die Erbringung seiner Vertrauensdienste auswirken, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Cybersicherheitsvorfalls. Zusätzlich haben die betroffenen Einrichtungen alle Informationen zu übermitteln, die es dem CSIRT und der Cybersicherheitsbehörde ermöglichen zu ermitteln, ob der Cybersicherheitsvorfall grenzübergreifende Auswirkungen hat.

(3) Soweit ein erheblicher Cybersicherheitsvorfall die Erbringung des jeweiligen Dienstes der betroffenen Einrichtung beeinträchtigt, hat die Einrichtung die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Cybersicherheitsvorfall zu unterrichten und, soweit möglich, alle Maßnahmen oder Abhilfemaßnahmen mitzuteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können.

(4) Das CSIRT hat der meldenden Einrichtung spätestens 24 Stunden nach Eingang der Frühwarnung gemäß Abs. 2 Z 1 eine Antwort zu übermitteln, einschließlich einer ersten Rückmeldung zu dem erheblichen Cybersicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung für die Durchführung möglicher Abhilfemaßnahmen. Auf Ersuchen der betreffenden Einrichtung leistet das CSIRT zusätzliche technische Unterstützung. Wird bei dem erheblichen Cybersicherheitsvorfall ein strafrechtlich relevanter Hintergrund vermutet, gibt das CSIRT ferner Orientierungshilfen für die Meldung des Cybersicherheitsvorfalls an die Strafverfolgungsbehörden.

(5) Wenn der erhebliche Cybersicherheitsvorfall zwei oder mehr Mitgliedstaaten der Europäischen Union betrifft, hat die Cybersicherheitsbehörde im Wege der zentralen Anlaufstelle unverzüglich die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten und die ENISA über den erheblichen Cybersicherheitsvorfall zu unterrichten. Diese Mitteilung hat die gemäß Abs. 2 erhaltenen Informationen zu enthalten.

(6) Nach Anhörung der von einem erheblichen Cybersicherheitsvorfall betroffenen Einrichtungen kann die Cybersicherheitsbehörde personenbezogene Daten nach erfolgter Interessenabwägung bezüglich der Auswirkungen auf die Betroffenen veröffentlichen, um die Öffentlichkeit über erhebliche Cybersicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von erheblichen Cybersicherheitsvorfällen erforderlich ist, oder die Offenlegung des erheblichen Cybersicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt. Bei der Interessenabwägung ist darauf zu achten, dass nur jene personenbezogenen Daten veröffentlicht werden, die zum vorgenannten Zweck unbedingt erforderlich sind. Es ist auf den Verhältnismäßigkeitsgrundsatz gemäß § 1 Abs. 2 DSG und auf den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO Bedacht zu nehmen.

(7) Die Cybersicherheitsbehörde hat jener Behörde, die in Umsetzung des Art. 9 der Richtlinie (EU) 2022/2557 national als zuständige Behörde benannt oder eingerichtet wurde, Informationen über erhebliche Cybersicherheitsvorfälle, erhebliche Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung zu stellen, die gemäß Abs. 1 von Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen gelten, gemeldet wurden. Dasselbe gilt für freiwillige Meldungen gemäß § 37.

(8) Die Cybersicherheitsbehörde hat der Regulierungsbehörde gemäß § 194 TKG 2021 und der KommAustria gemäß § 199 TKG 2021 Informationen über erhebliche Cybersicherheitsvorfälle, erhebliche Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung zu stellen, die gemäß Abs. 1 von Anbietern öffentlicher elektronischer Kommunikationsnetze oder Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste gemeldet wurden. Dasselbe gilt für freiwillige Meldungen gemäß § 37.

(9) Die Cybersicherheitsbehörde hat dem Bundesminister für Inneres halbjährlich über eingetretene erhebliche Cybersicherheitsvorfälle einschließlich der gemäß den Abs. 1, 5, 7 und 8 sowie gemäß § 8a Abs. 3 des Gesundheitstelematikgesetzes 2012 (GTelG 2012), BGBl. I Nr. 111/2012, zur Verfügung gestellten Informationen und über freiwillige Meldungen gemäß § 37 zu berichten.

(10) Die Cybersicherheitsbehörde hat der ENISA im Wege der zentralen Anlaufstelle alle drei Monate einen zusammenfassenden Bericht über gemäß Abs. 1 gemeldete erhebliche Cybersicherheitsvorfälle sowie gemäß § 37 gemeldete erhebliche Cyberbedrohungen sowie Beinahe-Cybersicherheitsvorfälle zu übermitteln.

Zuletzt aktualisiert am

30.12.2025

Gesetzesnummer

20013065

Dokumentnummer

NOR40273895