

# Bericht

## des Ausschusses für innere Angelegenheiten

**über den Beschluss des Nationalrates vom 12. Dezember 2025 betreffend ein Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsystemsicherheitsgesetz 2026 – NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden**

Mit diesem Beschluss sollen das Netz- und Informationssystemsystemsicherheitsgesetz 2026 (NISG 2026) erlassen und das Telekommunikationsgesetz 2021 (TKG 2021), BGBl. I Nr. 190/2021, und das Gesundheitstelematikgesetz 2012 (GTelG 2012), BGBl. I Nr. 111/2012, geändert werden.

Die zunehmende Durchdringung nahezu aller Bereiche der Gesellschaft und des täglichen Lebens mit digitaler Technologie bietet erhebliche Chancen und Möglichkeiten. Gleichzeitig wird die Gesellschaft dadurch aber auch angreifbarer und abhängiger von der Vertraulichkeit, Verfügbarkeit und Integrität von digital verarbeiteten und gespeicherten Informationen, mit anderen Worten: von der Sicherheit im Cyberraum. Staaten, Gruppierungen, aber auch kriminellen Akteuren eröffnen sich immer neue Wege, die digitale Vernetzung für Spionage, Sabotage oder andere kriminelle Aktivitäten nutzbar zu machen. Dabei können schon die Fähigkeiten einzelner krimineller Individuen genügen, um Cyberangriffe mit im Vorfeld nicht abschätzbaren Folgen für die Sicherheit Österreichs durchzuführen. Immer mehr österreichische Unternehmen wurden in den vergangenen Jahren Opfer von Cyberattacken, wie insbesondere von Datenverschlüsselungsangriffen (Ransomware-Attacken) und Angriffen auf die Verfügbarkeit ihrer IT-Systeme (DDoS-Attacken) (für eine nähere Darstellung der Cyberlage im Jahr 2022 siehe den Bericht Cybersicherheit für das Jahr 2022). Im Lichte dieser Entwicklungen wird deutlich, dass moderne Demokratien ein entsprechendes organisatorisches, personelles und finanzielles Fundament benötigen, um die wachsende Bedeutung von Cybersicherheit gesamtstaatlich abbilden zu können.

Aufgrund der seit Jahren rapide zunehmenden Bedeutung von Cybersicherheit hat die Europäische Union (EU) mehrere Rechtsakte erlassen, die der unionsweiten Erhöhung der Cybersicherheit dienen. Mit der Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren, ABl. Nr. L 202 vom 08.06.2021 S. 1, wird das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit eingerichtet und sieht in diesem Zusammenhang die Benennung von nationalen Koordinierungszentren durch die Mitgliedstaaten vor. Mit der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 ABl. Nr. L 333 vom 27.12.2022 S. 80, CELEX-Nr.: 32022L2555, (im Folgenden: NIS-2-Richtlinie), welche am 16. Jänner 2023 in Kraft getreten ist, wird unter anderem eine erhebliche Steigerung der zu beaufsichtigenden Einrichtungen sowie eine erhebliche Ausweitung des Aufgabenspektrums der NIS-Behörden vorgesehen.

Das NISG 2026 errichtet das nationale Koordinierungszentrum für Cybersicherheit gemäß der Verordnung (EU) 2021/887 und setzt die NIS-2-Richtlinie um.

Ein im Zuge der Debatte im Plenum des Nationalrates eingebrachter und beschlossener Abänderungsantrag wurde wie folgt begründet:

**„Zu Z 1, 2 und 6:**

Mit den vorgeschlagenen Änderungen sollen die jeweils festgelegten Berichts- bzw. Veröffentlichungspflichten dahingehend präzisiert werden, dass diesen bis spätestens sechs Monate nach Ende des jeweiligen Berichtszeitraums nachzukommen ist. Dadurch soll einerseits die zeitgerechte Berichterstattung bzw. Veröffentlichung sichergestellt und andererseits eine strukturierte sowie qualitativ hochwertige Aufbereitung gewährleistet werden. Betreffend die Verpflichtungen zur Berichterstattung (etwa gegenüber dem Nationalrat sowie Bundesrat gemäß dem vorgeschlagenen § 4 Abs. 3) ist wesentlich, dass die zu übermittelnden Berichte im Sinne der Nachvollziehbarkeit eine klar definierte Struktur sowie eine kohärente Gliederung nach Themenschwerpunkten aufweisen sollen.

**Zu Z 3 und 5:**

Mit den gegenständlichen Änderungen soll entsprechend den Vorgaben der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. Nr. L 333 vom 27.12.2022 S. 80, CELEX-Nr.: 32022L2555, (im Folgenden: NIS-2-RL), eine Präzisierung bzw. Abbildung bestimmter Verpflichtungen der Cybersicherheitsbehörde erfolgen.

Demnach soll – in Umsetzung des Art. 3 Abs. 3 NIS-2-RL – gemäß dem vorgeschlagenen § 29 Abs. 1 klargestellt werden, dass das von der Cybersicherheitsbehörde zu führende Register wesentlicher und wichtiger Einrichtungen einschließlich der Einrichtungen, die Domännennamen-Registrierungsdienste erbringen, regelmäßig, längstens jedoch alle zwei Jahre zu überprüfen und bei Bedarf anzupassen ist.

Gemäß dem vorgeschlagenen § 34 Abs. 10 soll die Cybersicherheitsbehörde in ihrer Funktion als zentrale Anlaufstelle entsprechend der unionsrechtlichen Vorgabe gemäß Art. 23 Abs. 9 NIS-2-RL verpflichtet sein, der ENISA alle drei Monate einen zusammenfassenden Bericht über die gemäß § 34 Abs. 1 sowie § 37 gemeldeten erheblichen Cybersicherheitsvorfälle, erheblichen Cyberbedrohungen sowie Beinahe-Cybersicherheitsvorfälle zu übermitteln. Wesentlich ist, dass dieser Bericht lediglich aggregierte sowie anonymisierte Daten enthalten soll.

**Zu Z 4:**

Mit der vorgeschlagenen Änderung soll ein redaktionelles Versehen beseitigt und entsprechend den Vorgaben des Art. 3 Abs. 4 UAbs. 2 NIS-2-RL vorgesehen werden, dass wesentliche und wichtige Einrichtungen einschließlich jener Einrichtungen, die Domännennamen-Registrierungsdienste erbringen, Änderungen der gemäß § 29 Abs. 2 Z 4 und 5 zu übermittelnden Angaben ehestmöglich, in jedem Fall jedoch innerhalb von zwei Wochen ab dem Tag der Änderung der Cybersicherheitsbehörde mitzuteilen haben.

**Zu Z 7:**

Mit der vorgeschlagenen Änderung soll ein redaktionelles Versehen bereinigt werden.

**Zu Z 8:**

Die vorgeschlagene Änderung soll aufgrund der jüngsten Novelle des Gesundheitstelematikgesetzes 2012 (GTelG 2012), BGBl. I Nr. 111/2012, vorgenommen werden.“

Der Ausschuss für innere Angelegenheiten hat den gegenständlichen Beschluss des Nationalrates in seiner Sitzung am 16. Dezember 2025 in Verhandlung genommen.

Berichterstatter im Ausschuss war Bundesrat Ernest **Schwindsackl**.

Gemäß § 30 Abs. 2 GO-BR wurde beschlossen, Bundesrätin MMag. Elisabeth **Kittl**, BA mit beratender Stimme an den Verhandlungen teilnehmen zu lassen.

An der Debatte beteiligten sich die Mitglieder des Bundesrates Dominik **Reisinger**, MMag. Elisabeth **Kittl**, BA und Werner **Gradwohl**.

Bei der Abstimmung wurde mehrstimmig beschlossen,

1. gegen den Beschluss des Nationalrates keinen Einspruch zu erheben (dafür: V, S, dagegen: F),
2. dem vorliegenden Beschluss des Nationalrates gemäß Artikel 44 Abs. 2 B-VG die verfassungsmäßige Zustimmung zu erteilen (dafür: V, S, dagegen: F).

Zum Berichterstatter für das Plenum wurde Bundesrat Ernest **Schwindsackl** gewählt.

Der Ausschuss für innere Angelegenheiten stellt nach Beratung der Vorlage mehrstimmig den **Antrag**,

1. gegen den vorliegenden Beschluss des Nationalrates keinen Einspruch zu erheben,
2. dem vorliegenden Beschluss des Nationalrates gemäß Artikel 44 Absatz 2 B-VG die verfassungsmäßige Zustimmung zu erteilen.

Wien, 2025 12 16

**Ernest Schwindsackl**

Berichterstatter

**Mag. Harald Himmer**

Vorsitzender