ENTSCHLIESSUNGSANTRAG

der Bundesrätinnen Elisabeth Kittl, Simone Jagl, Claudia Hauschildt-Buschberger

betreffend Cybersicherheits-Richtlinie NIS 2 unverzüglich umsetzen

eingebracht im Zuge der Debatte zum Beschluss des Nationalrates vom 16. Oktober 2025 betreffend ein Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 und das Allgemeine Sozialversicherungsgesetz geändert werden (413/A und 243 d.B.) (TOP 17)

BEGRÜNDUNG

Die NIS-2-Richtlinie der EU ist von zentraler Bedeutung für die Cybersicherheit in Europa und in Österreich, ganz besonders auch im Hinblick auf Gesundheitstelematik und den Schutz von Gesundheitseinrichtungen und -daten.[1] Die Richtlinie legt europaweit einheitliche Mindeststandards für die Cybersicherheit kritischer Sektoren (etwa Energie, Verkehr, Bankwesen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur, öffentliche Verwaltung etc) sowie wesentlicher und wichtiger Einrichtungen fest. Ziel ist es, die Widerstandsfähigkeit gegenüber Cyberangriffen deutlich zu stärken und ein hohes gemeinsames Sicherheitsniveau in der EU zu schaffen. Die Richtlinie erweitert den Anwendungsbereich deutlich im Vergleich zur Vorgängerversion (NIS-1) – betroffen sind nun deutlich mehr Sektoren und Unternehmen. Mit NIS-2 wird Cybersicherheit zur Pflichtaufgabe – inklusive klarer Anforderungen an Risikomanagement, Meldepflichten und Unternehmensführung.

Die NIS-2-Richtlinie wäre bis 17. Oktober 2024 umzusetzen gewesen. Ein Gesetzesentwurf wurde in der türkis-grünen Regierungszeit ausgearbeitet. Dennoch hat bis heute keine Umsetzung stattgefunden, ein überarbeiteter Entwurf wurde wiederholt angekündigt, ist aber bis heute nicht vorgelegt worden. Im November 2024 hat die EU bereits ein Vertragsverletzungsverfahren gegen Österreich eingeleitet[2], aber weder das noch jüngste Cybersicherheitsvorfälle in österreichischen Ministerien können die Bundesregierung offenbar dazu bewegen, den Turbo in Sachen Cybersicherheit einzulegen. Dabei wäre das angesichts der wachsenden Bedrohungslage und auch der hybriden Kriegsführung Russlands dringend nötig.

Erst Ende August 2025 wurde ein Hackerangriff (eines mutmaßlich staatlichen Akteurs) auf das BMI bekannt, bei dem rund 100 Outlook-Postfächer kompromittiert wurden und Server offline genommen werden mussten.[3] Neben den massiven

---

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1674579731975&from=EN

[2] https://austria.representation.ec.europa.eu/news/europaische-kommission-startet-neue-vertragsverletzungsverfahren-2024-11-28_de?prefLang=et

[3] https://orf.at/stories/3404000/

Angriffen auf Ministerien, wie dem BMI oder dem BMEIA sehen wir auch sonst, dass sich die Bedrohungslage in Quantität und Qualität ständig verschärft:

- Im 2. Quartal 2025 gab es durchschnittlich 1.717 Cyberangriffe pro Woche auf österreichische Organisationen – ein Anstieg um 6% gegenüber dem Vorquartal.[4]
- In den letzten fünf Jahren war jedes dritte österreichische Unternehmen Ziel eines erfolgreichen Cyberangriffs.[5]
- Mehr als jeder 4. Angriff (28 Prozent) ist auf staatlich unterstützte Akteure zurückzuführen.[6]

Die NIS-2-Richtlinie ist ein dringend notwendiger Schutzschild. Ihre vollständige Umsetzung ist für Unternehmen, Institutionen und unsere kritische Infrastruktur existenziell.

Zuletzt hatte Innenminister Karner anlässlich des Cybersicherheitsvorfalls im BMI Anfang September erklärt, der Gesetzesentwurf sei bereits überarbeitet und in Abstimmung mit SPÖ und NEOS.[7] Am „Tag der kritischen Infrastruktur", einem Vernetzungstreffen von Vertretern der kritischen Infrastruktur und Sicherheitsexperten Mitte September erklärte der Innenminister, es liefen bereits „intensive Gespräche mit der Opposition".[8] Im Widerspruch zu diesen Presse-Statements wurde aber bis heute kein überarbeiteter Gesetzesentwurf vorgelegt. Auf der WKO-Website ist von einem „NISG 2026" die Rede[9] – offenbar plant die Regierung also mit ihrer Säumigkeit bei Cybersicherheit ins nächste Jahr zu gehen.

Die unterfertigenden Bundesrätinnen stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Bundesrat wolle beschließen:

„Die österreichische Bundesregierung wird aufgefordert, die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) unverzüglich umzusetzen."

ELISABETH AITTL

[4] https://www.austriainnovativ.at/woechentlich-1717-cyber-angriffe-auf-oesterreichische-organisationen-im-q2-2025/
[5] https://www.ey.com/de_at/newsroom/2025/09/ey-cybersecurity-2025

[6] https://www.onlinesicherheit.gv.at/Services/Publikationen/Sicherheitsstudien-und-Analysen/2025-Cyber-Security-in-Oesterreich.html
[7] https://www.oe24.at/oesterreich/politik/cyber-attacke-auf-ministerium-eu-richtlinie-nicht-umgesetzt/646879220
[8] https://www.puls24.at/news/chronik/neue-herausforderungen-fuer-staatsschuetzer-durch-ki/438015
[9] https://www.wko.at/it-sicherheit/nis2-uebersicht

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-23T23:29:02+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	