RN/71

13.36

Abgeordneter Mag. Friedrich Ofenauer (ÖVP): Vielen Dank, Frau Präsidentin! Sehr geehrter Herr Bundesminister! Herr Staatssekretär! Geschätzte Kolleginnen und Kollegen im Hohen Haus! Sehr verehrte Zuseherinnen und Zuseher! Man kann durchaus sagen, dass wir ein wenig unter Druck sind, was den Beschluss des Netz- und Informationssystemsicherheitsgesetzes betrifft, weil die Frist für die Umsetzung schon abgelaufen ist, auf der anderen Seite aber natürlich auch, was die allgemeine Sicherheitslage betrifft, denn – es wurde bereits angesprochen – vor allem hybride Angriffe nehmen zu und davor ist keiner gefeit, kein privater Betrieb, kein privater Computer und natürlich auch Behörden nicht.

Diese Cyberangriffe sind deswegen besonders tückisch, weil sie sehr subtil erfolgen. Sie hinterlassen kein aufgebrochenes Türschloss, keine aufgebrochene Tür, machen keinen lauten Knall, können aber sehr große Auswirkungen haben.

Die Hacker dringen in fremde Systeme ein, verändern Datensätze minimal, lösen damit vielleicht Kettenreaktionen aus oder sie stehlen sensible Informationen. Hinter diesen Angriffen stehen längst nicht mehr nur kriminelle Organisationen, sondern manchmal auch geopolitisch und staatlich aktivierte Akteure, manchmal sogar sogenannte Wegwerfagenten.

Eines ist klar: Diese Bedrohungslage ist genauso gefährlich wie physische Attacken oder kinetische Angriffe. Die Bedrohungslagen haben sich für unsere Gesellschaft massiv verändert. Sie sollen die Gesellschaft demoralisieren, die Gesellschaft destabilisieren, und deswegen müssen wir als gesamte Gesellschaft gegen solche Angriffe widerstandsfähig werden. Resilienz ist also nicht mehr nur ein Schlagwort, sondern eine Notwendigkeit, denn wir müssen unsere Krankenhäuser, die Energieversorgung, Kommunikationsnetzwerke, unsere

gesamte kritische Infrastruktur, die das Nervensystem unseres Landes ist, schützen.

Im Jahr 2024 konnte das dafür notwendige Netz- und Informationssystemsicherheitsgesetz nicht beschlossen werden, weil die Zweidrittelmehrheit gefehlt hat. Deswegen wurde gegen Österreich auch ein Vertragsverletzungsverfahren eingeleitet. 2024 ist schon eine Zeit lang her, deswegen kann ich der Argumentation des Kollegen Darmann gar nichts abgewinnen, wenn er von einem Durchpeitschen dieses Gesetzesvorhabens spricht, da es seit 2024 läuft. *(Abg.* ***Darmann*** *[FPÖ]: Ihr habt jahrelang nichts getan, um jetzt einen Blödsinn vorzulegen!)* Ja, wir nehmen nun einen neuen Anlauf, aber von einem Schnellschuss, meine Damen und Herren, kann keine Rede sein.

Dass keine Begutachtung stattgefunden hat, schwingt auch immer mit, wurde vor allem auch im Ausschuss releviert. Auch das stimmt nicht, weil das 2024 vorgelegte Gesetz auch entsprechend begutachtet wurde und im Wesentlichen auch den Inhalt dieses Gesetzes, das wir heute beschließen werden, darstellt. Auch dass Experten nicht eingebunden worden sein sollen, stimmt nicht. Im neuen Entwurf wurden Bundesländer, Wirtschaftskammer, Industriellenvereinigung und auch Experten eingebunden. Rückmeldungen sind in die Überarbeitung eingeflossen – auch jene der damaligen Oppositionsparteien SPÖ und NEOS – und vor allem die Grünen haben im letzten Innenausschuss nach entsprechender Überarbeitung und Aufnahme ihrer Vorschläge ihre Zustimmung gegeben. Dafür auch ein Dankeschön, dass da entsprechend mitgestimmt wird.

Das NIS 2026 übernimmt zentrale Teile des Entwurfs von 2024, wurde aber in entscheidenden Punkten nachgeschärft. Deswegen bringe folgenden Antrag ein:

RN/71.1

Abänderungsantrag

der Abgeordneten Friedrich Ofenauer, Maximilian Köllner, Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen zum Bericht des Ausschusses für innere Angelegenheiten über die Regierungsvorlage (308 d.B.) betreffend ein Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und lnformationssystemen (Netz- und Inforrnationssystemsicherheitsgesetz 2026 NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden (354 d.B.) – TOP 8.

Der Nationalrat möge in 2. Lesung beschließen, dass der vorliegende Gesetzentwurf wie folgt geändert wird – und ich darf jetzt die wesentlichen Punkte dieses Abänderungsantrages vortragen:

Es werden nämlich die im Entwurf vorgesehenen Berichtspflichten durch gesetzliche Festlegung von Veröffentlichungs- beziehungsweise Übermittlungsfristen präzisiert, nämlich in § 3b Abs. 6, in § 4 Abs. 3 und in § 42 Abs. 11 sowie ergänzende Ausführungen betreffend die inhaltliche Aufbereitung der Berichte in der Begründung.

Dann werden Fristen gemäß § 29 Abs. 4 NISG 2026 an die unionsrechtlichen Vorgaben angepasst.

Es werden unionsrechtlich vorgesehene Informationsverpflichtungen in § 29 Abs. 1 NISG 2026 sowie in § 34 Abs. 10 NISG 2026 im Sinne einer einfacheren Notifizierung gegenüber der Europäischen Kommission abgebildet; und es wird durch die Änderung von BMF auf BMWKMS ein redaktionelles Versehen im TKG 2021 beseitigt; und die redaktionelle Anpassung aufgrund der gestrigen Änderungen des Gesundheitstelematikgesetzes wird eingearbeitet.

Sie sehen, meine Damen und Herren: Parlamentarische Berichtspflichten wurden präzisiert, der Innenminister muss halbjährlich über die Cybersicherheitslage berichten, Übergangsfristen wurden praxistauglicher gestaltet und der Aufbau der neuen Cybersicherheitsbehörde wurde neu strukturiert. Das ist auch ein wesentlicher Punkt, weil dieser Kritikpunkt auch gekommen ist: Sie wird außerhalb der Generaldirektion für die öffentliche Sicherheit angesiedelt, was die Vorwürfe mit Sicherheitslücken, Messengerüberwachung und so weiter schon wieder einmal ad absurdum führt. Wichtig ist auch für uns als Parlament, dass der Direktor der Cybersicherheitsbehörde sowie sein Stellvertreter künftig den zuständigen Ausschüssen des Nationalrates für Auskünfte zur Verfügung stehen.

Meine Damen und Herren, das Ziel dieser neuen Cybersicherheitsbehörde ist Beraten statt strafen. Wichtig ist es, die Unternehmen bei der Risikoanalyse zu unterstützen – und das ist wichtig, um eben Aufmerksamkeit für die angesprochenen neuen Bedrohungslagen zu schaffen, die Awareness zu schärfen, wie man so schön sagt. Das ist bei größeren Betrieben schon vorhanden, weil diese ja bereits über entsprechende ISO-Zertifizierungen verfügen und für sie jetzt vielleicht die neuen NIS2-Anforderungen nicht ganz so überraschend kommen; aber vor allem muss natürlich bei kleineren Betrieben die Aufmerksamkeit für entsprechende Sicherheitsbedrohungen und Sicherheitsrisiken erhöht werden.

Ja, das mag vielleicht ein zeitlicher und auch ein finanzieller Aufwand sein, aber vor allem diese Berichtspflichten sind wichtig für die Republik – vor allem auch für das Innenministerium und für die Polizei, um ein Lagebild der Republik zu haben; aber auch für die Unternehmen, um ein eigenes Risikobild für die Bedrohungen, denen sie ausgesetzt sind, zu haben. Damit bedeutet das auch, in gewisser Weise einen Selbstschutz zu haben. Denn klar ist,

Cybesicherheitsrisiken – vor allem Cyberbedrohungen – können alle treffen; und Prävention ist sicherlich günstiger als die Wiederherstellung von Daten.

Umso wichtiger ist eine breite Zustimmung, die dieser Entwurf heute von ÖVP, SPÖ, NEOS und Grünen erhält, die sich zu mehr Sicherheit vor allem auch im digitalen Raum bekennen. Wenig überraschend, aber doch ist es so, dass die FPÖ, die sich zwar gerne als Sicherheitspartei inszeniert, aber dann wie so oft Maßnahmen, die der Sicherheit dienen, nicht mitträgt und nicht mitstimmt. *(Abg. **Lindner** [SPÖ]: Nicht überraschend!)* Danke schön. – Nicht überraschend, nicht überraschend. *(Heiterkeit des Abg. **Zarits** [ÖVP]. – Beifall bei der SPÖ, bei Abgeordneten der NEOS sowie des Abg. **Zorba** [Grüne].)*

13.44

Der Gesamtwortlaut des Antrages ist unter folgendem Link abrufbar:

RN/71.2

TOP8 Abänderungsantrag: AVISO-Dokument gescannt von Mag. Friedrich Ofenauer, Maximilian Köllner, MA, Douglas Hoyos-Trauttmansdorff

Präsidentin Doris Bures: Der Abänderungsantrag wurde in den Grundzügen erläutert, wurde bereits an alle Abgeordneten verteilt und steht daher auch mit in Verhandlung.

Nächste Rednerin: Frau Abgeordnete Irene Eisenhut.