RN/69

8. Punkt

Bericht des Ausschusses für innere Angelegenheiten über die Regierungsvorlage (308 d.B.): Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2026 – NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden (354 d.B.)

Präsidentin Doris Bures: Damit gelangen wir zum 8. Punkt der heutigen Tagesordnung.

Auf eine mündliche Berichterstattung wurde verzichtet.

Ich begrüße Herrn Bundesminister Karner und Herrn Staatssekretär Leichtfried im Hohen Haus und erteile Herrn Abgeordneten Gernot Darmann das Wort.

RN/70

13.28

Abgeordneter Mag. Gernot Darmann (FPÖ): Besten Dank, Frau Präsident! Herr Bundesminister! Herr Staatssekretär! Hohes Haus! Gegen ein Mehr an Cybersicherheit wird wohl niemand etwas einzuwenden haben, aber, werte Kolleginnen und Kollegen, es geht um das Wie: um die Abbildung dieser Cybersicherheit in Strukturen und Maßnahmen. Gegen dieses NIS-Gesetz sprechen wir Freiheitliche uns vehement aus, werte Kollegen. *(Beifall bei der FPÖ.)*

Ich hätte mir im Zuge dieser Debatte ja gewünscht, dass auch der sogenannte Deregulierungsstaatssekretär Schellhorn anwesend wäre, denn vorige Woche

hat er mit zwei Pressekonferenzen und seiner Verliererampel wortreich eine Show, ein Vorgaukeln von Deregulierungsmaßnahmen in einer Anzahl von 113, die in Wahrheit nichts Wirkliches bewegen, zum Besten gegeben. Mit diesem NIS-Gesetz werden aber tatsächlich – man halte sich fest, insbesondere die Vertreter der Wirtschaft, der Industrie und auch 18 weiterer Branchen! – 4 000 österreichische Unternehmen mit deren Lieferketten mit neuer Bürokratie, mit neuer Ineffizienz und in weiterer Folge mit Kostentreiberei belastet. Das ist der Ausfluss dieses NIS-Gesetzes und wie es schlussendlich in der Wirtschaft aufschlagen wird. Das Vorschieben des Begriffs Sicherheit ist in diesem Fall ein Frevel, denn mehr Sicherheit wird damit bei Gott nicht geschaffen, werte Kolleginnen und Kollegen. *(Beifall bei der FPÖ.)*

Herr Bundesminister, Herr Staatssekretär, Sie peitschen dieses NIS-Gesetz aufgrund der selbstverantworteten Versäumnisse der letzten Jahre durch dieses Parlament, um im alten Jahr noch irgendwelchen Strafmaßnahmen der Europäischen Union zu entkommen. Ich muss Ihnen schon sagen, die Vorgehensweise sucht ihresgleichen.

Wir haben im letzten Jahr hier ein laut Fachausschuss annähernd gleiches Gesetz – manche sagen wieder, ein absolut abgeändertes Gesetz – beraten. Im letzten Jahr haben noch NEOS und SPÖ massiv Kritik geäußert. Sie haben deutlich klargemacht: unmöglich, diesem Gesetz zuzustimmen. Und siehe da: Nunmehr stimmt man in diesen Parteien diesem Gesetz zu, weil es notwendig sein soll, diese Belastungen durchzuziehen.

Deswegen die Frage nicht nur an die ÖVP, sondern vor allem an die NEOS: Wie kann es sein, dass man derartige Belastungslawinen auf die österreichische Wirtschaft ausrollt, bis hin zu 10-Millionen-Euro-Strafen, darüber hinaus Strafen in der Höhe von bis zu 2 Prozent des globalen Unternehmensumsatzes des Vorjahrs, und zwar – der Geschäftsführung entsprechend zur Haftung

zugeleitet – mit dem Auftrag, in diesen Unternehmen der 18 Branchen dann auch noch eigene Teams einzurichten, die das Audit durch das Innenministerium abarbeiten werden? In weiterer Folge wird dort dann auch noch sicherzustellen sein, dass alle Maßnahmen, die vom Innenministerium aufgetragen werden, umgesetzt werden. Diese Unternehmen – das ist auch noch einmal spannend, und das hat mir auch im Fachausschuss keiner beantworten können – werden beauftragt, in ihrer Lieferkette sicherzustellen, dass auch die in der Lieferkette befindlichen Unternehmen – wurscht ob im Inland oder Ausland – all das abzubilden haben, was sich das Innenministerium einbildet.

Da frage ich mich – und diese Frage habe ich auch gestellt –, ob man im Ernst glaubt, dass das in der Realität abzubilden sein wird: Wenn ein österreichisches Unternehmen zur drittletzten Unternehmerposition in der Lieferkette hingeht und sagt: Liebe Leute, sagt uns eure Sicherheitsrisiken! Wie habt ihr euch gegen Cybersicherheitseinbrüche gerüstet? Wir möchten das gerne wissen, denn das Innenministerium fragt das ab!, dann würde ich als Unternehmen, das auf seine eigene Sicherheit schaut, natürlich eben nicht diese Information weitergeben, denn ansonsten ist man ja angreifbar.

Darüber hinaus kommt der nächste Wahnsinn in diesem ganzen Gesetz: All diese sicherheitsrelevanten, hochsensiblen Informationen der 4 000 österreichischen Unternehmen samt Lieferkette werden dann in einem eigenen Bereich des Innenministeriums zusammengeführt, in jenem Innenministerium, das auf der anderen Seite natürlich ein Interesse daran hat, hochsensible Cyberlücken zu kennen, weil man dieses Wissen ja auch für die Messengerdienstüberwachung braucht. Da gibt es einen Zielkonflikt, der haarsträubend ist und normalerweise jedem Abgeordneten hier herinnen, der seiner Kontrollpflicht gegenüber der Exekutive, der höchsten Exekutive, nämlich der Bundesregierung, nachkommt, auffallen müsste.

Verehrte Kolleginnen und Kollegen, ich bin wirklich verwundert, wie man dieses Gesetz so locker durchschütteln kann. Darüber hinaus wurde auch noch festgeschrieben – das wundert mich ja auch –, dass über die vorhin genannten hohen Strafen für unsere Wirtschaft die Bezirkshauptmannschaften quer durch Österreich entscheiden werden, die ja höchste Cyberkompetenz haben, die ja so viel Personal haben, um all das abzuarbeiten, was nunmehr vom Innenministerium, vom Gesetzgeber, von der Verliererampel beauftragt wird.

Dann schaue ich mir nämlich wirklich an, ob nicht tatsächlich – und das müsstet ihr auch wissen – die allermeisten dieser Unternehmen schon aufgrund der eigenen Fürsorge fürs Unternehmen ja um Welten mehr Cybersicherheitskompetenz haben als so manche Bezirkshauptmannschaft, die erst die Beamten auszubilden hat, die es ja anderseits gar nicht gibt, um dann diesen Unternehmen zu sagen, dass sie ihre eigene Cybersicherheit nicht im Griff haben.

Da beißt sich die Katze in den Schwanz! Das ist wie dem Dreck eine Watsche zu geben, was uns praktisch von diesem Ministerium als der Weisheit letzter Schluss im Bereich der Cybersicherheit zugeleitet wurde. Ich kann mich nur darüber wundern, dass hier im Ausschuss schon eine Mehrheit gegeben war, darüber hinaus aber auch hier im Nationalrat, im hohen Plenum vermutlich diese große Mehrheit über vier Parteien hinweg zustande kommen wird.

Werte Kolleginnen und Kollegen, normalerweise sollten Sie in sich gehen, denn zum Abschluss möchte ich schon noch etwas sagen, das ja fast zum Schmunzeln wäre, wäre es nicht so traurig: Das Innenministerium, das nunmehr im wahrsten Sinne des Wortes die Hoheit über dieses einzurichtende Cybersicherheitsamt hat, ist in Zukunft dafür zuständig oder macht sich selbst dafür zuständig, auf die Cybersicherheit von rund 4 000 Unternehmen zu achten. Es sammelt all diese hochsensiblen Informationen und war heuer, in diesem Jahr nicht in der

Lage, den eigenen Stall sauber zu halten. Es ist durch einen Cyberangriff attackiert worden. Auch die Republik Österreich ist im Bereich des Außenministeriums im letzten Jahr ganz massiv Angriffen ausgesetzt gewesen und hat sich selber nicht schützen können.

Jetzt sammelt man die ganzen sensiblen Daten in jenem Ministerium, das gerade heuer diesem Cyberangriff ausgesetzt war, und meint, damit nicht ein weiteres Risiko zu schaffen, das in Wahrheit erneut haarsträubend ist. Wenn eine organisierte Kriminalität, irgendwelche Cyberverbrecher meinen, schnell zu umfassenden Daten kommen zu wollen, dann ist es doch das Einfachste, jetzt nicht quer durch 4 000 Unternehmen auf die Suche zu gehen, sondern sich gleich ans Innenministerium zu wenden, um dort alle Daten auf einmal abzusaugen und zu wissen, wie die Wirtschaft, hochsensible Bereiche unserer Branchen aufgestellt sind. *(Beifall bei der FPÖ.)*

Alles zusammenfassend, werte Kolleginnen und Kollegen, wird es von unserer Seite für diesen Irrsinn namens NIS-Gesetz keine Zustimmung geben, weil es im höchsten Maße verantwortungslos ist, wie da mit dem Thema Cybersicherheit umgegangen wird. Wie gesagt, der Kreis soll sich schließen: Ohne Zweifel ist Cybersicherheit auch uns ein hohes Anliegen, aber nicht mit einem solchen Machwerk. *(Beifall bei der FPÖ.)*

13.36

Präsidentin Doris Bures: Nächster Redner: Herr Abgeordneter Friedrich Ofenauer.

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 Informationssystemen (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.

RN/72

13.45

Abgeordnete Irene Eisenhut (FPÖ): Danke, Frau Präsidentin! Herr Innenminister! Herr Staatssekretär! Liebe Zuseherinnen und Zuseher! Wir diskutieren heute neuerlich das sogenannte NIS2-Gesetz – ein Gesetz für die Cybersicherheit Österreichs, die Umsetzung einer EU-Richtlinie. Da dieses Gesetz Verfassungsbestimmungen enthält, ist hier im Parlament die notwendige Zweidrittelmehrheit erforderlich. Bereits Anfang 2023 trat eine EU-Richtlinie in Kraft, welche die Cyber- und Informationssicherheit von systemrelevanten

Unternehmen und Institutionen unionsweit regelt. Unternehmen sollen auf Cyberattacken vorbereitet sein und in Fällen von Cybercrime wissen, an wen sie sich wenden können und wie sie damit umzugehen haben. Es gibt ja bereits eine bestehende Meldestelle.

Da ich im Vorjahr noch nicht hier im Parlament war, habe ich mir natürlich die Abläufe, Meinungen und Äußerungen der einzelnen Fraktionen zu diesem Thema angesehen. Mich hat natürlich interessiert: Was hat die Fraktionen dazu bewogen, ihre Meinung vom Vorjahr zum jetzigen Regierungsentwurf zu ändern? 2024 – die Abstimmung war im Juli –: FPÖ, SPÖ und NEOS haben damals aufgrund erheblicher Sorgen und Bedenken im Hinblick auf Massendatenspeicherung, aber auch im Hinblick auf Massenüberwachung durch die Hintertür gegen die damalige Regierungsvorlage gestimmt. Weiterer Kritikpunkt war die Machtkonzentration im Innenministerium, verbunden mit Zielkonflikten, weil diese Stelle gleichzeitig auch Kontrollorgan war.

Seit der Abstimmung im Vorjahr gab es überdies keine Ausschussbegutachtung. Kollege Ofenauer – ich sehe ihn gerade nicht – hat gesagt - - *(Abg.* ***Ofenauer*** *[ÖVP] – mit beiden Händen aus der ersten Reihe der ÖVP-Fraktion winkend –: Ausschussbegutachtung ist ja nicht vorgesehen normalerweise im Gesetzgebungsverfahren …!)* Es hat vielleicht interne Gespräche *(Abg.* ***Ofenauer*** *[ÖVP]: Nein, …!)* zwischen den Regierungsfraktionen gegeben, es gab definitiv keine Ausschussbegutachtung. Im letzten Ausschuss wollten wir diese noch einmal beantragen, das wurde aber leider abgelehnt. Ich weiß nicht, mit wem Sie gesprochen haben, mit den Oppositionsparteien, zumindest mit der FPÖ hat es seit dem Juli des Vorjahres keine weiteren Gespräche und keine Begutachtung gegeben. Es fehlten Gespräche mit Stakeholdern aus Wirtschaft und Zivilgesellschaft, Einbindung von Experten; das wurde auch in den Stellungnahmen zu der jetzt vorliegenden Regierungsvorlage kritisiert. Der Kollege von der ÖVP hat weiters im Ausschuss behauptet, es gab keine

wesentlichen Änderungen und somit wäre auch eine weitere Ausschussbegutachtung nicht notwendig gewesen. *(Abg. **Zorba** [Grüne]: Das stimmt!)*

Für SPÖ und NEOS hingegen gab es so wesentliche Änderungen, dass sie auch ihre Meinung des Vorjahres revidiert haben und jetzt voraussichtlich der bestehenden Regierungsvorlage zustimmen werden. In der Rede der SPÖ vom Vorjahr wurde von drei großen Kritikpunkten gesprochen: von der Kritik an alle Macht im Innenministerium, von Zielkonflikten dahin gehend, dass jene Stelle, welche bei den Cybervorfällen Hilfestellungen leistet, auch gleichzeitig als Kontrollorgan agieren soll. Diese Befürchtung wurde angeblich *(Abg. **Köllner** [SPÖ]: Nein, nicht angeblich!)* durch mehr Transparenz beschwichtigt.

Die NEOS sahen 2024 noch die große Gefahr einer anlasslosen Massenüberwachung. Es gab jetzt eine Ausweitung der Berichtspflichten und gleichzeitig wollen aber die NEOS – so wurde es zumindest im Ausschuss geäußert – keine zusätzliche Belastung der Unternehmen. Sehr geehrte Damen und Herren, ich weiß nicht, wie das funktionieren soll *(Abg. **Holzegger** [NEOS]: Ich erklär's Ihnen dann!):* mehr Berichtspflichten und weniger Belastungen für die Unternehmen, aber ich freue mich schon *(Abg. **Holzegger** [NEOS]: Ja!)* auf die Erklärungen, vielleicht kann man das dann besser nachvollziehen.

Für uns steht auf alle Fälle fest: Es hat sich im Vergleich zum Vorjahr an dieser Regierungsvorlage so gut wie nichts geändert. Die Befürchtungen liegen nach wie vor im Raum; es gibt keinen wesentlichen Unterschied – und auch ein Weisungsrecht des Innenministers zu der neu einzurichtenden Stelle ist noch zu erwähnen. Ich glaube, Kollege Ofenauer hat es auch im Ausschuss gesagt, dass die Stelle ja nicht der Generaldirektion für die öffentliche Sicherheit untergeordnet ist, sondern dass eine eigene Stelle im Bereich des Innenministeriums eingerichtet wird. Nur: Es macht ja keinen Unterschied, ob

das die Sektion II betreut oder der Sektion II untergeordnet ist oder als eigenes Bundesamt untergeordnet ist – es ist und bleibt dem Innenminister untergeordnet. Und darum – nochmals – werden wir dieser Regierungsvorlage in der Form nicht zustimmen. *(Beifall bei der FPÖ.)*

13.50

Präsidentin Doris Bures: Nächster Redner: Herr Abgeordneter Maximilian Köllner.

RN/73

13.50

Abgeordneter Maximilian Köllner, MA (SPÖ): Danke, Frau Präsidentin! Geschätzter Herr Bundesminister! Werter Herr Staatssekretär! Meine sehr geehrten Damen und Herren! Netz- und Informationssystemsicherheitsgesetz: Man muss gestehen, es ist ein etwas sperriger Begriff, aber vielleicht zur Veranschaulichung ein einfaches Beispiel, das jede und jeden von uns betrifft und auch, um zu zeigen, worum es da eigentlich geht: Ich gehe in den Supermarkt, gehe mit meinem Einkauf an die Kasse und zahle nicht in bar, sondern vielleicht mit der Karte oder mit dem Handy, und dann hoffe ich natürlich, dass diese Zahlung auch klappt und dorthin kommt, wo sie hin soll und nicht durch etwaige Sicherheitslücken irgendwo landet. Da kommt eben dieses Gesetz ins Spiel, da kommen Banken ins Spiel, die wie Energieversorger, wie Flughäfen oder wie Spitäler zur kritischen Infrastruktur zählen.

Wir müssen darauf schauen, dass diese kritische Infrastruktur durch hohe Sicherheitsstandards geschützt wird, und das machen wir, indem wir umfassende Sicherheitsmaßnahmen in wichtigen Einrichtungen, in großen Unternehmen umsetzen. Das machen wir, indem wir Mitarbeiterinnen und Mitarbeiter schulen und sensibilisieren, und das machen wir natürlich auch im

Anlassfall, wenn es einen Cybervorfall gibt, indem es eine umgehende Meldung dieses Vorfalls gibt.

Kollege Ofenauer hat es angesprochen: Wir leben in einer sehr dynamischen Zeit. Es gibt hybride Angriffsformen, vielfältige Bedrohungslagen auf unsere Gesellschaft, und Angriffe sind auch von überall aus möglich. Jemand, der uns schaden möchte, der eine wichtige Einrichtung in Österreich zerstören möchte, der kann das von überall auf der Welt aus machen. Ich glaube, deswegen – weil Cyberkriminalität eben keine nationalen Grenzen hat – ist es auch wichtig, dass wir diese Vorgaben EU-weit umsetzen, dass es EU-weite, einheitliche und verbindliche Sicherheitsstandards gibt. Um auch darauf einzugehen, weil die FPÖ ja immer wieder die Europäische Union kritisiert: Ohne Gold-Plating zu betreiben, machen wir das, was notwendig ist – und nicht mehr. *(Beifall bei SPÖ, ÖVP und NEOS.)*

Und weil die FPÖ schon ganz interessiert war – was hat sich seit den Entwürfen der letzten Bundesregierung geändert? *(Abg. **Darmann** [FPÖ]: Ihr seids in der Regierung!)* – und auch, um dem Verfolgungswahn der FPÖ ein bisschen entgegenzutreten: Wir wollten eine eigene Cybersicherheitsbehörde als zentrale Anlaufstelle für sämtliche Cyberangelegenheiten. Wenn ich bedroht werde, wenn ich überfallen werde, dann werde ich auch in Zukunft die Polizei rufen. Wenn ein Unternehmen aber digital angegriffen wird, dann wird das zukünftig der Cybersicherheitsbehörde gemeldet. Und ja, sie ist im BMI angesiedelt, aber – und das ist schon wesentlich – außerhalb der Generaldirektion für öffentliche Sicherheit, außerhalb der Polizeisektion. Das ist im Sinne einer klaren Abgrenzung und im Sinne eines unabhängigen Arbeitens schon wichtig zu betonen: wenn Weisungen, dann schriftlich und mit Berichterstattung an das Parlament. *(Beifall bei der SPÖ, bei Abgeordneten der ÖVP sowie der Abg. **Holzegger** [NEOS].)*

Wenn wir schon bei den Berichtspflichten sind: Im Sinne der Transparenz haben wir gefordert, dass es erweiterte Berichtspflichten ans Parlament gibt. Der Direktor, die Direktorin der neuen Behörde wird auch den Fragen der Parlamentarier Antworten geben, wird für Auskünfte zur Verfügung stehen.

Wenn wir über Sicherheit generell sprechen, dann sprechen wir immer auch über einen durchaus herausfordernden Spagat zwischen Sicherheit und Freiheit, Sicherheit und Datenschutz. Im Sinne des Datenschutzes wird es einen Datenschutzbeauftragten geben, der nicht nur jährlich, sondern einen halbjährlichen Bericht über die Datenverarbeitungen auf der BMI-Website veröffentlichen wird, weil es eben auch um umfangreiche Befugnisse zur Verarbeitung von Daten – im Anlassfall auch von personenbezogenen Daten – geht. Zu guter Letzt haben wir im Sinne der Entlastung auch darauf geschaut, dass kleinere und mittlere Unternehmen von diesen Bestimmungen weitestgehend ausgenommen sind.

Zusammenfassend möchte ich sagen: Diese Bundesregierung hat in einer sehr schwierigen Zeit übernommen. Es ist nicht populär, wenn man sparen muss. Es gibt auch vielfältige Herausforderungen im Sicherheitsbereich, die nicht angenehm sind, um das auch einmal in aller Deutlichkeit anzusprechen. Wir haben aber bereits in dieser kurzen Zeit, seit März, geliefert, vor allem im Sicherheitsbereich. Wir haben das Asylgesetz verschärft. *(Abg.* ***Belakowitsch*** *[FPÖ]: Woran erkennt man das?)* Wir haben die Gefährderüberwachung, die Überwachung von Terroristen, beschlossen. Wir haben für das strengste Waffenrecht seit dem Bestehen dieses Gesetzes gesorgt. Und das Pendant zu diesem Netz- und Informationssystemsicherheitsgesetz ist das Resilienz kritischer Einrichtungen-Gesetz – auch ein sperriger Begriff –, auch das haben wir bereits beschlossen. Das RKEG schützt uns physisch, das NIS schützt uns digital. *(Beifall bei der SPÖ.)*

Es ist ein Riesengesetz, es hat lange gedauert, das stimmt, aber jetzt steht es vor dem Abschluss, und weil es lange gedauert hat, kann es gar kein Schnellschuss gewesen sein. – Danke an alle, die sich da aktiv und konstruktiv eingebracht haben; danke auch an die Grünen für die Vorarbeit in der Vorgängerbundesregierung – das muss man auch einmal ansprechen –, auch an Digitalisierungssprecher Süley Zorba. *(Beifall bei der SPÖ sowie des Abg.* ***Zorba*** *[Grüne].)*

An die FPÖ kann ich nur noch einmal appellieren – ein bisschen Zeit ist ja noch bis zur Abstimmung –: Das eine ist über Sicherheit zu reden, das andere ist für Sicherheit zu sorgen. Sie haben es in der Hand, ob Sie wieder einmal aus Prinzip dagegen sind oder im Sinne der Sicherheit für ganz Österreich mit dabei sind. – Danke schön. *(Beifall bei SPÖ, ÖVP, NEOS und Grünen.)*

13.57

Präsidentin Doris Bures: Herr Abgeordneter Köllner, ich ersuche Sie, den Begriff „Verfolgungswahn“ zurückzunehmen. *(Abg.* ***Köllner*** *[SPÖ]: Nehm' ich zurück!)* – Danke vielmals.

Dann ist der nächste Redner Abgeordneter Reinhold Maier.

RN/74

13.57

Abgeordneter Reinhold Maier (FPÖ): Geschätzte Frau Präsident! Herr Minister! Herr Staatssekretär! Werte Damen und Herren! Wie wir bereits gehört haben, sprechen wir heute über die NIS2-Richtlinien, ein Gesetz, das angeblich die Cyber- und Informationssicherheit verbessern soll. Doch eines darf nicht vergessen werden: NIS2 wurde im Jahr 2024 vom Verfassungsgerichtshof aufgehoben und ist jetzt in der hier vorliegenden Form in nur wenigen Punkten abgeändert. Damals waren SPÖ und NEOS wirklich strikt dagegen. Und was

machen sie heute? – Richtig, sie fallen im Liegen um und stimmen diesem Gesetz einfach zu. Offenbar reichen ein paar Regierungssessel aus, um einen Sinneswandel zu vollziehen. *(Beifall bei der FPÖ.)* Das ist aber nichts Neues und wirklich bezeichnend für diese Bundesregierung.

Was passiert jetzt wirklich? – Aus ursprünglich sieben Sektionen werden 18 gemacht. Weiters werden 4 000 Unternehmen verpflichtet, eine Fülle an technischen, operativen und organisatorischen Maßnahmen umzusetzen, und das alles unter einer Strafandrohung von bis zu 10 Millionen Euro. Ich wiederhole es: bis zu 10 Millionen Euro. Allein diese Strafandrohung schadet unserem Wirtschaftsstandort und wird Investoren abschrecken, bei uns zu investieren.

Der nächste Punkt interessiert mich als Polizist natürlich ganz besonders, Herr Innenminister – vielleicht können Sie jetzt zuhören, es ist speziell an Sie gerichtet –: Im Innenministerium soll ein Bundesamt für Cybersicherheit geschaffen werden. Das ist ein neuer Behördenapparat, der bis 2029 auf 172 Planstellen anwachsen soll und somit personell und budgetär wieder zulasten der Basispolizei geht. Und da ist es ganz egal, Herr Kollege Köllner und Herr Ofenauer, wo das angesiedelt ist – nicht in der Generaldirektion –, es ist Herrn Innenminister Karner unterstellt. Die Sektionen I, II, IV und V sind ja auch dem Herrn Innenminister unterstellt. Deshalb ist das – unter Anführungszeichen – keine „Ausrede“ und keine Bereinigung Ihrer Zustimmung. *(Beifall bei der FPÖ.)*

Wie gesagt, personell und budgetär geht das zulasten der Basispolizei. Das ist bezeichnend, denn während hier eine neue Behörde geschaffen und aufgebaut wird, werden bei der Polizei aufgrund des Sparzwanges Dienststellen an Wochenenden geschlossen, Überstunden gestrichen und Zuteilungen aufgehoben. Herr Innenminister, das passiert auch bei Spezialeinheiten und

Sondereinheiten wie bei der Cobra, und das in Zeiten einer erhöhten Terrorgefahr – das ist wirklich unverantwortlich. *(Beifall bei der FPÖ.)*

Man kann also wirklich zusammenfassen: Für einen neuen Behördenaufbau, der wahrscheinlich wieder mit schwarzen Schäfchen gespickt werden wird, ist Geld da, aber meinen Kollegen und Kolleginnen wird im gleichen Atemzug die Weihnachtsbelohnung gestrichen. Weiters zwingt man uns – wir haben jetzt eine Besprechung gehabt – auch ein neues Dienstzeitmodell auf, das wieder Gehaltseinbußen für meine Kolleginnen und Kollegen bedeuten wird. Sie wissen, es gibt da Berechnungen – und wenn Sie es nicht wissen, ist es ja noch schlimmer. *(Beifall bei der FPÖ.)* Aus unserer Sicht, der Sicht der FPÖ, ist das eine falsche und unverantwortliche Prioritätensetzung in Ihrem Ressort, Herr Innenminister.

Reden wir noch über den zusätzlichen Mehraufwand und Bürokratieaufbau, der mit diesem Gesetz verbunden ist. Da frage ich mich wirklich: Wo ist der Deregulierungs-Sepp eigentlich? Da hätte er nämlich wirklich tätig werden müssen. Er hat ja erst vor Kurzem versucht, mit 113 Scheinmaßnahmen seine Daseinsberechtigung – sage ich jetzt einmal – zu machen. Jetzt schaut er wieder tatenlos und still zu und es passiert das Gegenteil: mehr Regulierung, mehr Aufwand und mehr Belastung für unsere Unternehmen.

Ein weiteres Problem sehe ich darin, dass die neue Cybersicherheitsbehörde Unternehmen künftig vorschreiben kann, welche IKT-Produkte, -Dienste und -Prozesse sie verwenden müssen. Das ist Bevormundung und Zentralisierung, meine Damen und Herren, das ist ein direkter Eingriff in die wirtschaftliche Freiheit. *(Beifall bei der FPÖ.)*

Als Höhepunkt kommt ein sicherheitspolitischer Widerspruch: Das Gesetz soll im Cyberbereich Sicherheitslücken schließen, während dieselbe Regierung die Messengerüberwachung beschlossen hat, die von Sicherheitslücken lebt. Also

was wollt ihr jetzt: Wollt ihr Lücken schließen oder wollt ihr sie nutzen? Denn beides geht sich nicht aus. Aus meiner Sicht ist das sicherheitspolitische Schizophrenie. *(Beifall bei der FPÖ.)*

Fakt ist, zusammenfassend: Die Sicherheit wird mit diesem Gesetz sicher nicht erhöht werden. Im BMI werden erneut falsche Prioritäten gesetzt und unser Wirtschaftsstandort wird durch die neuen Auflagen, durch neue Bürokratie und staatliche Bevormundung weiter beschädigt.

Meine Damen und Herren, die Regierung hat es im gesamten abgelaufenen Jahr und auch in den letzten drei Tagen wieder bewiesen: Sie kann es einfach nicht. Mein Appell an die Bundesregierung: Machen Sie den Österreichern ein Weihnachtsgeschenk und machen Sie den Weg frei für Neuwahlen und einen Volkskanzler Herbert Kickl. – Danke. *(Beifall bei der FPÖ.)*

14.03

Präsidentin Doris Bures: Herr Abgeordneter Maier, ich ersuche auch Sie, den Ausdruck „sicherheitspolitische Schizophrenie“ zurückzunehmen. *(Abg. **Maier** [FPÖ]: Es stimmt, aber ich nehme ihn zurück!)* – Nein, Sie können ihn nur zurücknehmen. Tun Sie das? *(Abg. **Maier** [FPÖ]: Ja!)* – Dann danke ich dafür. *(Abg. **Köllner** [SPÖ]: Brav ist er!)*

Die nächste Rednerin ist Frau Abgeordnete Ines Holzegger.

RN/75

14.03

Abgeordnete Ines Holzegger (NEOS): Danke, Frau Präsidentin! Werter Herr Minister! Herr Staatssekretär! Hohes Haus! Liebe Zuseherinnen und Zuseher! Heute ist ein guter Tag für die Cybersicherheit. Ja, es ist kein Geheimnis, dass es länger gedauert hat, bis wir am heutigen Tag angekommen sind, und ja, ich habe auch vollstes Verständnis, dass es in der Branche schon wirklich Ungeduld

gegeben hat, auch wegen der Unsicherheit und der Unklarheit – bis jetzt. Heute können wir endlich Klarheit geben; denn eines ist sicher: Wir werden angegriffen, täglich – in der Verwaltung, in der Wirtschaft, alle sind davon betroffen. Oft laufen aber solche Angriffe fernab von der öffentlichen Wahrnehmung ab. Genau deshalb brauchen wir ganz wichtige Schritte hin zu mehr Awareness und mehr Cybersicherheit.

Ich habe Ihnen, Herr Kollege Darmann, ja auch schon im Ausschuss erklärt, warum wir NEOS uns jetzt anders positionieren werden als letztes Jahr, aber ich sage es gerne noch einmal, vielleicht hält es dann: Letztes Jahr waren wir noch gegen den NIS2-Vorschlag, seither hat sich aber auch einiges geändert. Viele wertvolle Stellungnahmen sind eingebunden worden und damit sind auch viele Bedenken ausgeräumt worden. *(Abg. **Stefan** [FPÖ]: Glauben Sie das wirklich oder ist das jetzt da eine …?)*

Kollege Ofenauer hat es schon richtig gesagt: Die künftige NIS-Behörde ist eine eigenständige Behörde *(Abg. **Darmann** [FPÖ]: Aber weisungsgebunden!),* die lediglich vom Direktor geführt wird – davor wäre sie direkt beim Herrn Innenminister verortet gewesen. *(Zwischenruf des Abg. **Petschnig** [FPÖ]. – Abg. **Darmann** [FPÖ]: … verlass ich mich nicht!)* Darüber hinaus ist ein wichtiger Punkt auch die Weisungsfreiheit – und Weisungen des Ministers an den Direktor können ausschließlich schriftlich erfolgen und müssen in einen Weisungsbericht inkludiert werden. *(Abg. **Schnedlitz** [FPÖ]: Weisungsfreiheit … schriftliche Weisungen! Den Satz bitte schreiben wir raus! – Abg. **Stefan** [FPÖ]: Mündliche Weisungs…!)*

Jetzt möchte ich auch noch einen Punkt zum Bereich Bürokratievermeidung einbringen. Wissen Sie, ich komme aus dem Bereich, ich komme aus der Wirtschaft, deswegen kann ich da auch aus Erfahrung sprechen. *(Zwischenruf des Abg. **Schnedlitz** [FPÖ].)* Wir haben es geschafft, dass da unnötige Bürokratie

vermieden wird. *(Abg. **Stefan** [FPÖ]: Durch eine neue Behörde!)* Wie? – Das kann ich Ihnen gerne erklären: Viele Unternehmen haben schon einschlägige Zertifikate, das ist Usus da draußen, und wir haben es geschafft, dass diese einschlägigen Zertifikate auch als NIS-Zertifizierung gelten. ISO 27001 ist draußen kein Novum, das haben so viele Unternehmen, und damit brauchen sie keine zusätzliche Zertifizierung, sparen sich Zeit und Kosten. Das ist ein wirklicher Faktor für Sicherheit und für den Wirtschaftsstandort. *(Beifall bei den NEOS, bei Abgeordneten der ÖVP sowie des Abg. **Zorba** [Grüne].)*

Außerdem – und das ist auch schon erwähnt worden – wird es statt des jährlichen einen halbjährlichen Bericht zum Thema Cybersicherheit geben, denn im digitalen Bereich finden Dinge einfach schneller statt, auf Bedrohungen muss schneller reagiert werden, und kürzere Abstände sind einfach wichtig, weil die Uhren im digitalen Raum einfach schneller gehen.

Ich hoffe, dass sich die Kolleginnen und Kollegen von der FPÖ das vielleicht doch noch einmal überlegen – Sie haben jetzt mehrmals die Argumente gehört *(Ruf bei der FPÖ: Schriftliche Weisungen ...!)*, im Ausschuss, hier vom Rednerpult aus – und dass sie doch noch zustimmen werden. Sie schreiben sich ja selber immer Sicherheit auf die Fahnen, aber wenn es dann darauf ankommt *(Abg. **Stefan** [FPÖ]: Dann sind wir für die Freiheit!)*, ducken Sie sich scheinbar weg. *(Abg. **Stefan** [FPÖ]: Nein, wirklich!)* Ich kann Ihnen eines sagen: Vom einfach nur Warten wird es nicht sicher. *(Abg. **Stefan** [FPÖ]: Sie schreiben was auf die Fahnen? Und was machen Sie jetzt? Liberal?)* Sie, Herr Darmann, sagen: Es ist unverantwortlich, dem zuzustimmen. Ich sage: Es ist unverantwortlich, heute hier dagegenzustimmen. *(Beifall bei den NEOS sowie des Abg. **Köllner** [SPÖ]. – Abg. **Darmann** [FPÖ]: Das täuscht Sicherheit vor! Die es nicht gibt!)*

14.08

Präsidentin Doris Bures: Bitte, Herr Abgeordneter Süleyman Zorba.

RN/76

14.08

Abgeordneter Süleyman Zorba (Grüne): Danke, Frau Präsidentin! Sehr geschätzte Kolleginnen und Kollegen! Werte Zuseherinnen und Zuseher! Herr Innenminister! Herr Staatssekretär! Dass ich das noch erleben darf, dass wir das NIS-Gesetz hier im Parlament beschließen! *(Heiterkeit bei den Grünen. – Ruf bei der SPÖ: Bist ja noch gar nicht so alt!)*

Es ist eines der wichtigsten, zentralen europäischen Cybersicherheitsgesetze der letzten Jahre, und ich glaube, es ist wirklich an der Zeit gewesen, das in Österreich umzusetzen. Ich bin sehr froh, dass wir das mit vier demokratischen Parteien heute durch den Nationalrat bringen werden. *(Beifall bei Grünen und NEOS sowie des Abg.* ***Ofenauer*** *[ÖVP].)*

Das NIS-Gesetz begleitet mich ja quasi von Anfang an, seit ich im Nationalrat bin. Machen wir gleich mit dieser Zeitreise weiter: Dieser Entwurf war ja schon einmal hier, 2024 – das ist schon einige Zeit her –, und der Text war ja nahezu identisch mit dem, den wir heute beschließen werden. Damals hat uns die notwendige Zweidrittelmehrheit gefehlt, weil die Kolleginnen und Kollegen von der SPÖ und von den NEOS der Meinung waren, dass das nicht in Ordnung ist. Heute wird quasi derselbe Text durchgebracht.

Könnte man jetzt genüsslich auf diesem Umstand herumreiten, auf diese Wendung hinweisen? – Ja. Könnte ich die gleichen Argumente bringen, die Sie damals gebracht haben, und heute gegen diesen Entwurf stimmen? – Ja. Aber was würde es uns bringen? Was bringt es? Wozu? Wenn es um den Schutz unserer kritischen Infrastruktur geht, ist, glaube ich, parteipolitisches Klein-Klein fehl am Platz. *(Beifall bei den Grünen.)*

Wir haben heute schon öfter über die geopolitische Lage gesprochen und darüber, was hybride Kriegsführung bedeutet. Kritische Infrastruktur wird angegriffen – wir haben es schon gehört: Ministerien, Krankenhäuser, Energieanbieter, Verkehrsanbieter, alles Mögliche wird Ziel von Sabotage, der Kontinent ist auch Ziel von absichtlicher Desinformation. Auf all das sollten wir ja reagieren, und am besten europäisch und gemeinsam.

Aber was heißt das jetzt konkret für den einzelnen Österreicher, die einzelne Österreicherin? – Stellen Sie sich vor, Sie liegen in einem Krankenhaus, erwarten eine sehr, sehr wichtige Operation und auf einmal funktioniert nichts mehr – keine Patientenakte, keine Befunde, kein OP-Plan, die Operation kann nicht durchgeführt werden. Das ist in Barcelona passiert. Nach einem Hackerangriff wurden Hunderte Operationen abgesagt. Und das ist nicht Science-Fiction, das ist Realität, und genau deshalb braucht es eben Gesetze für mehr Cybersicherheit. *(Beifall bei den Grünen und bei Abgeordneten der SPÖ.)*

Es ist klar, dieses NIS-Gesetz 2026 ist jetzt keine leichte Materie. Zwei Regierungen haben daran gearbeitet, unzählige Mitarbeiterinnen und Mitarbeiter. Es ist eine Mammutaufgabe, aber es ist wichtig, dass hier ein gemeinsames Fundament geschaffen wird mit besserer Zusammenarbeit, schnellerer Reaktion auf Vorfälle. Und das Wichtigste: Europa zieht hier an einem Strang, und Österreich ist jetzt endlich, mit etwas Verspätung, ein Teil davon.

Wir haben in der Debatte ja auch kritische Stimmen gehört – hier im Nationalrat, aber auch von Stakeholdern und NGOs außerhalb. Ich glaube, diese Bedenken muss man auch ernst nehmen. Es stimmt auch, dass das eine Abwägung zwischen verschiedenen Interessen ist. Das Wichtige dabei ist halt, das große Ganze nicht aus dem Blick zu verlieren.

Cybersicherheit ist eben eine Mammutaufgabe. Es braucht Eingriffsmöglichkeiten, und deshalb sind klare Kontrollmechanismen wichtig, und die sind in diesem Gesetzesvorschlag gegeben.

Als Parlament haben wir eine ganz, ganz wichtige Kontrollfunktion. Und ganz ehrlich: Aus Gerhard Karner werden wir jetzt keinen großen Datenschützer machen. Darum ist es umso wichtiger, dass wir ganz genau darauf schauen, was der Herr Innenminister mit diesen Befugnissen macht. Da gibt es ja auch diese Berichte, die entsprechend in einer nahen Zeitabfolge hier im Nationalrat diskutiert werden. Und ich glaube, das ist nicht nur wichtig für die Kontrollfunktion, die wir auszuüben haben, sondern vielleicht gibt es auch Erkenntnisse, Sicherheitslücken, über die wir sprechen, und Vorfälle, die einen Mehrwert für die Bevölkerung bringen, damit sie sich darüber informiert. *(Beifall bei den Grünen.)*

Aber ist dieses NIS-2 jetzt das Ende der Fahnenstange? Haben wir nachher keine sicherheitsrelevanten Probleme mehr im digitalen Raum? – Nein. Es ist aber ein wichtiger europaweiter Standardisierungsschritt, und wir werden auch weiterhin daran arbeiten müssen, die Sicherheit hochzuhalten, egal ob es jetzt offline oder online ist. Dieses Gesetz ist also kein Abschluss, sondern quasi der Beginn einer neuen Sicherheitsarchitektur im Cybersicherheitsbereich. *(Beifall bei den Grünen.)*

Wir haben jetzt gehört, es ist ein riesengroßes Gesetz. Jetzt ist es wichtig, dieses Gesetz auch mit Leben zu füllen. Wir müssen die Unternehmerinnen und Unternehmer unterstützen, die jetzt einige Dinge haben, die sie umsetzen sollen.

Auf der anderen Seite braucht es, wie wir schon gehört haben, ausreichend Personal in den Behörden, Menschen, die mit diesem Gesetz arbeiten. Da

müssen wir auch darauf schauen, dass wir genug Fachkräfte haben, denn gute Cybersicherheitsexperten fallen für gewöhnlich nicht vom Himmel.

Das heißt, wir werden noch weiter investieren müssen. Und da erwarte ich mir auch Schritte von der Bundesregierung, dass wir in Ausbildung investieren, in Fachhochschulen, in die Lehre. Es muss eben auch eine bildungspolitische Priorität haben, in diesem Bereich gutes Personal hervorzubringen.

Zum Schluss: Konstruktive Oppositionsarbeit bedeutet eben, in den wichtigen Punkten auch zuzustimmen, auch Verbesserungen reinzuverhandeln. Wir haben diesem Entwurf, den wir ja von der letzten Gesetzgebungsperiode sehr gut kennen, im Ausschuss zugestimmt und wir werden dem auch hier im Nationalrat zustimmen. So funktioniert eben konstruktive Politik: Dass man dort, wo es problematische Auswüchse gibt, hinschaut, hinweist, vielleicht Verbesserungen reinverhandelt und dann, wenn es darauf ankommt, sich nicht vor der Verantwortung drückt, sondern auch zustimmt. *(Beifall bei den Grünen sowie bei Abgeordneten von ÖVP und SPÖ.)*

Ich möchte einen Dank aussprechen: Es gab in den letzten dreieinhalb, vier Jahren viele Mitarbeiterinnen und Mitarbeiter im Innenministerium, im Bundeskanzleramt, bei uns im Klub, Jessica Grün, Referentin in unserem Klub. Unzählige Mitarbeiterinnen und Mitarbeiter, sehr viele Leute haben da viel Zeit reingesteckt. Ihnen allen gebührt ein riesengroßes Danke.

Wir haben jetzt hier ein NIS-2, das wir auf den Weg bringen können. Danke auch an die Kolleginnen und Kollegen von SPÖ, NEOS und ÖVP dafür, dass wir jetzt doch am Ende noch ein paar Verbesserungen reinbringen konnten. Ich glaube, das ist heute ein guter Tag für die Cybersicherheit. – Danke schön. *(Beifall bei den Grünen sowie bei Abgeordneten von ÖVP, SPÖ und NEOS.)*

14.15

Präsidentin Doris Bures: Nun hat sich Herr Bundesminister Gerhard Karner zu Wort gemeldet. – Bitte.

RN/77

14.15

Bundesminister für Inneres Mag. Gerhard Karner: Sehr geehrte Frau Präsidentin! Geschätzte Damen und Herren Abgeordnete! Werte Zuseherinnen und werte Zuseher! Es wurde ja in dieser Debatte schon zu Recht mehrfach erwähnt, dass dieser Gesetzesvorschlag, dieses NIS2-Gesetz, schon sehr, sehr lange sehr intensiv debattiert und diskutiert wurde und wahrscheinlich eines jener Gesetze ist, das offensichtlich besonders viel Vorarbeit benötigt hat und auch gebraucht hat.

Beim SNG, beim Thema Gefährderüberwachung, haben wir vielleicht ähnlich lange debattiert, wenn nicht sogar länger. Faktum ist: Das NIS2-Gesetz wurde sehr intensiv und sehr lange erörtert. Und was ich für besonders wichtig halte: Dieses Gesetz wurde auch mit den Betroffenen oder, wie man neudeutsch sagt, mit den sogenannten Stakeholdern, besonders oft erörtert.

Es war ja im Jänner 2023, als die EU-Richtlinie letztendlich beschlossen wurde. Mit einem klaren Ziel ist diese EU-Richtlinie damals aufs Tapet gekommen, nämlich die Widerstandsfähigkeit im Cyberbereich zu stärken, die Reaktionszeit auf Cyberangriffe zu verkürzen und – wahrscheinlich, und das wurde auch zu Recht mehrmals angesprochen, der wichtigste Punkt in diesem Bereich – um resilient, widerstandsfähig zu sein, um einheitliche Standards festzulegen, damit man sich aufeinander verlassen kann, dass man, wenn man mit öffentlichen Institutionen, mit Unternehmen der kritischen Infrastruktur zu tun hat, weiß, wer welche Standards, welche Sicherheitsstandards, welche Sicherheitsresilienz anwendet.

Und weil es eben so ist, dass es ein für die Widerstandsfähigkeit unserer kritischen Infrastruktur enorm wichtiges Gesetz ist, wurde unmittelbar nach dem Beschluss der EU-Richtlinie im Jahr 2023 ein breiter Einbindungsprozess gestartet, eine Tour durch die Bundesländer, gemeinsam mit der Industriellenvereinigung, der Wirtschaftskammer, vielen anderen Betroffenen, die sich da intensiv beteiligt haben. Es ging um die Frage: Was kommt, was ist notwendig, was müssen wir tun, um uns selber zu schützen, um widerstandsfähig, resilient zu sein?

Auch an dieser Stelle möchte ich mir wirklich herzlich bedanken, nämlich bei allen Mitarbeiterinnen und Mitarbeitern aus dem Innenministerium, die in dieser Zeit massiv unterwegs waren, aber auch bei den vielen anderen in der Industriellenvereinigung, in der Wirtschaftskammer, in den Bezirksorganisationen. Auch viele aus dem Hohen Haus und auch aus dem Bundeskanzleramt haben an der Umsetzung dieses Gesetzes letztendlich gearbeitet.

Ich habe es auch im Ausschuss gesagt: Mir ist bewusst, dass die Umsetzung dieses Gesetzes für die Betroffenen natürlich einen Aufwand bedeutet. Aber – ich habe versucht, es zu erklären und tue es nochmals – dieser Aufwand ist notwendig, und das wissen ja letztendlich auch die Organisationen, Institutionen und auch Unternehmen.

Gerade größere Konzerne tun das ja bereits sehr umfangreich. Es ist vor allem die Struktur der Mittelbetriebe, die da in vielen Bereichen mehr Beratung benötigen, damit sie gegen Angriffe von außen sicher sind, damit sie ihre Geschäfte letztendlich machen können.

Gute Vorbereitung, Resilienz verhindert, vermindert Attacken und vor allem die möglichen Auswirkungen solcher Attacken, die letztendlich sogar existenzgefährdend sein können. Daher war – und das wurde auch von einigen

Mandatarinnen und Mandataren angesprochen – der Ansatz dieses Gesetzes immer und vor allem jetzt: Beraten statt Strafen! Das ist ganz entscheidend, damit dieses Gesetz umgesetzt wird, die nötige Akzeptanz und, das ist der entscheidende Punkt, auch die entsprechende Wirksamkeit erreicht: Beraten statt Strafen!

Angesprochen wurde auch – und das halte ich auch für notwendig und wichtig –: Die Unabhängigkeit der Behörde ist eben sichergestellt. Ja, es gibt eine Weisungsbefugnis unter klaren Regelungen. Ich denke, das ist auch notwendig. Warum? – Weil sich eben ein Innenminister, ein Mitglied der Bundesregierung auch zu einer Verantwortung bekennen muss und sich auch nicht abputzen sollte. Daher halte ich es für sinnvoll, sich zu dieser Verantwortung zu bekennen – und das tue ich, daher: Bundesamt statt einer Gruppe im BMI unter Federführung der Generaldirektion für die öffentliche Sicherheit. *(Beifall bei der ÖVP sowie des Abg.* ***Bernhard*** *[NEOS].)*

Daher gibt es auch von mir an dieser Stelle wirklich ein Danke für diese intensiven Gespräche mit allen Beteiligten im Rahmen der Koalitionsgespräche – an den Herrn Staatssekretär, aber natürlich auch bei den NEOS, und jetzt zuletzt auch bei den Grünen, denn wir haben ja in der vorigen Regierung schon intensiv darüber beraten. – Schön; und es ist gut, dass wir jetzt endlich diese breite Mehrheit schaffen, die ich einfach für notwendig halte.

Ja, dieses Gesetz bedeutet Aufwand und Arbeit, aber es bedeutet vor allem auch eines: Es bedeutet Schutz und Sicherheit für die betroffenen Institutionen, für die betroffenen Organisationen, für die betroffenen Unternehmen. Es bedeutet Schutz und Sicherheit für die Bevölkerung. Es bedeutet Schutz und Sicherheit für unser Land. Daher bitte ich Sie, diesem Gesetzesvorschlag auch

zuzustimmen. – Vielen herzlichen Dank. *(Beifall bei der ÖVP sowie bei Abgeordneten von NEOS und Grünen.)*

14.21

Präsidentin Doris Bures: Nächster Redner: Herr Abgeordneter Robert Laimer.

RN/78

14.21

Abgeordneter Robert Laimer (SPÖ): Vielen Dank, Frau Präsidentin! Herr Bundesminister! Staatssekretär! Hohes Haus! Geschätzte Kolleginnen und Kollegen! Liebe Zuseherinnen und Zuseher! Beim Netz- und Informationssystemsicherheitsgesetz, kurz NIS2, geht es nicht um taxative Aufzählung von Paragrafen, sondern darum, ob in unserem Land morgen Strom, Wasser, medizinische Versorgung und Datenzugänge funktionieren oder eben nicht.

Wir leben in einer Zeit, in der Kraftwerke, Spitäler, Verkehrsnetze, Verwaltungsserver genauso bedroht sind wie ein Tresor oder auch eine Grenze, nur dass der Angriff heute nicht mehr mit Sprengstoff erfolgt, sondern mit Schadsoftware, Erpressungsalgorithmen und Hackergruppen.

Cyberangriffe treffen nicht irgendwen im System. Sie treffen Patienten, sie treffen Pendler, Familien, Unternehmen. Wenn ein Krankenhaus erpresst wird – es wurde schon ausgeführt –, dann steht nicht eine Firewall still, sondern die Notaufnahme. Das muss uns bewusst sein. Digitale Ausfälle in der Spitzenmedizin führen unweigerlich zu menschlichen Tragödien.

Darum ist unsere Zustimmung heute auch kein Jubelakt, sondern staatliche Pflicht und Verantwortung. Die EU fordert zu Recht die Umsetzung. Europa ist im Fadenkreuz hybrider Angriffe, und Österreich kann es sich schlicht und einfach nicht erlauben, länger zuzuwarten und weiter aufzuschieben.

Zugegeben, als SPÖ haben wir im Vorjahr Nein gesagt, weil der Gesetzentwurf Schwächen hatte, erhebliche Schwächen sogar, und wir haben jetzt Ja gesagt, weil diese Schwächen nun gemeinsam ausgemerzt wurden. Von ehemaligen Machtkonzentrationen im Bundesministerium für Inneres ist er nun sozusagen in die Balance gerückt: Die Berichtspflichten sind präzisiert, die Abläufe transparenter, die Rolle der Behörden klar definiert – das war uns besonders wichtig – **und** das Parlament wurde eingebunden.

Wir beschließen keine Überwachung per se, sondern Schutzmechanismen in konsequenter Form auf europäischem Niveau. Wir müssen ehrlich sein: Tausende Unternehmen sind mittlerweile betroffen. Cybersicherheit kostet Budget, ja, es kostet Personal und es bedarf Know-hows. Keine Cybersicherheit kostet Arbeitsplätze, Infrastruktur und, ganz besonders bitter, am Ende Vertrauen, nämlich in die Schutzfunktion unseres Staates.

Deshalb haben wir auch darauf gedrängt, dass die neue Cybersicherheitsstelle nicht nur mahnt, sondern auch begleitet, nicht nur straft, sondern auch Lösungen vorgibt, nicht nur Vorgaben macht, sondern erklärt, trainiert und unterstützt, zu unser aller digitaler Sicherheit, denn es hilft niemandem, im Ernstfall Excel-Listen zu aktualisieren. *(Heiterkeit und Beifall bei der ÖVP sowie Beifall bei SPÖ und Grünen.)* Und glauben Sie mir, damit haben wir unsere Erfahrungen gemacht, während Server kollabieren.

Die Sicherheitsarchitektur muss funktionieren, simpel, klar und schnell erreichbar. Hybride Angriffe, Cyberkriminalität, digitale Spionage – das ist längst Alltag, und genau darum geht es. Wir bringen Österreich digital in die Lage, sich selbst zu verteidigen, ohne Grundrechte abzubauen und ohne Unternehmen in Bürokratie zu verfangen. Wir schaffen sozusagen Resilienz für den digitalen Zukunftsraum, für starke Infrastruktur, für starke Grundrechte.

Abschließend Dank an die Grünen für die seriöse Mitarbeit, besonders an ihren Experten Kollegen Zorba. Ich hoffe, zu viel Lob schadet nicht in der eigenen Partei. – Vielen Dank. *(Heiterkeit und Beifall bei den Grünen sowie Beifall bei der SPÖ und bei Abgeordneten der ÖVP.)*

14.25

Präsidentin Doris Bures: Nun hat sich Herr Staatssekretär Jörg Leichtfried zu Wort gemeldet. – Bitte.

RN/79

14.25

Staatssekretär im Bundesministerium für Inneres Mag. Jörg Leichtfried: Vielen Dank, Frau Präsidentin! Herr Bundesminister! Geschätzte Damen und Herren Abgeordnete! Sehr geehrte Damen und Herren Zuseherinnen und Zuseher! Dann werde ich mich mit dem Lob etwas zurückhalten, damit es dem Kollegen Zorba nicht doch vielleicht intern schadet *(Heiterkeit bei den Grünen)*, und werde meine Rede anders beginnen. Ich habe das nämlich vorgehabt, aber Kollege Laimer hat mich rechtzeitig davor gewarnt.

Ich möchte aber schon auf die Situation eingehen, vor der wir stehen. Die Bedrohungslage, sehr geehrte Damen und Herren, ist auch für Österreich deutlich komplexer und deutlich anspruchsvoller geworden. Hybride Bedrohungen, Spionage und Desinformation haben oft ihre Ursprünge im Ausland, gefährden aber unmittelbar Staat, Gesellschaft und Wirtschaft hier in Österreich, und das sind genau die, die wir schützen möchten: Staat, Gesellschaft und Wirtschaft, insgesamt die Menschen in Österreich, gilt es zu schützen.

Weil das Thema Gefährderüberwachung einige Male angesprochen wurde: Das Gegenteil gilt für Terroristen! Die wollen wir mit allen Mitteln, die uns unser

Rechtsstaat bietet, bekämpfen, um Österreich sicherer zu machen, sehr geehrte Damen und Herren! *(Beifall bei der SPÖ und bei Abgeordneten der ÖVP.)* Die Wahrscheinlichkeit, dass in Österreich ein Terroranschlag passiert, zu reduzieren, ist unsere wichtigste oder eine der wichtigsten Aufgaben, die wir haben.

Mit dem Netz- und Informationssystemsicherheitsgesetz ist uns ein wichtiger Schritt zu einem zeitgemäßen, umfassenden und aktuellen Gesetz als Antwort auf die rasch steigenden Herausforderungen gelungen. Das Ziel ist klar: Weiterentwicklung der österreichischen Cybersicherheitsarchitektur, Schutz der kritischen Infrastruktur und rasche, effiziente Reaktion auf Cybersicherheitsfälle.

Einige von Ihnen haben gefragt, was der Unterschied zum letzten Gesetzentwurf war – Herr Kollege Maier, das wurde übrigens nicht vom Verfassungsgerichtshof aufgehoben, sondern es hat keine Verfassungsmehrheit im Nationalrat gefunden, wenn Sie mir diese leichte Korrektur erlauben. Aber was ist der Unterschied? – Der Unterschied ist: Stärkung des Datenschutzes, Entlastung von kleineren und mittleren Unternehmen, Einrichtung einer unabhängigen, entpolitisierten Behörde, Berichtspflichten an den Nationalrat und Bundesrat sowie Auskunftserteilung an den Nationalrat, Änderung der maßgeblichen Berichtspflichten von jährlich auf halbjährlich. – Das ist nicht nichts, das sind wesentliche Änderungen.

Weil das NIS2-Gesetz auch in Kompetenzen der Länder eingreift, braucht es eine Verfassungsmehrheit, und ich möchte die Gelegenheit nützen, mich bei allen zu bedanken, die diesen Weg jetzt gegangen sind. Es war ein langer, schwieriger Weg. Ich möchte mich auch ganz besonders bei den Grünen für die sehr, sehr konstruktive Verhandlungsführung in diesem Bereich bedanken, die eine Verfassungsmehrheit ermöglicht haben. Wir sind auf dem richtigen Weg,

um für mehr Sicherheit in Österreich für alle zu sorgen. – Herzlichen Dank.

(Beifall bei SPÖ und ÖVP sowie bei Abgeordneten der Grünen.)

14.28

Präsidentin Doris Bures: Nächste Rednerin: Frau Abgeordnete Agnes Sirkka Prammer.

RN/80

14.29

Abgeordnete Mag. Agnes Sirkka Prammer (Grüne): Vielen Dank, sehr geehrte Frau Präsidentin! Sehr geehrter Herr Bundesminister! Sehr geehrter Herr Staatssekretär! Liebe Kolleginnen und Kollegen! Liebe Zuseherinnen und Zuseher! Wir haben jetzt über das NIS-Gesetz schon sehr viel gehört. Allerdings, was wir immer gehört haben, ist: Wir brauchen das, damit wir sicher sind. – Wir dürfen uns nicht der Illusion hingeben, dass wir dadurch immer vor allem geschützt sind; aber wir erreichen damit, dass wir die höchsten Sicherheitsstandards einhalten können, die wir haben. Ich glaube, das ist das Wesentliche und das ist das, was man tun kann und was man tun muss, um Sicherheit zu gewährleisten.

Für alle, die nicht immer alle Folgen vom Nationalrat im Fernsehen oder online mitverfolgen: Wir haben in der letzten Sitzung über die Drohnenabwehr gesprochen. Wir haben darüber gesprochen, wie gefährlich Drohnen sind, wie gefährlich Angriffe mit Drohnen sind und dass wir uns davor schützen müssen. Wir haben über Flughäfen gesprochen und wir haben darüber gesprochen, was für eine große Gefahr das für die Flughäfen ist. Nun ist das etwas, das sich jeder gut vorstellen kann: Die sieht man, man sieht sie am Himmel, man sieht sie kommen, man kann sie physisch beseitigen, man kann sich physisch davor schützen. – Das ist bei der Datensicherheit anders; es ist aber um nichts weniger gefährlich.

Bleiben wir beim Beispiel des Flughafens: Wenn man sich in die Netzwerke eines Flughafens reinhackt, könnte man zum Beispiel die Schiebetüren beim Duty-free-Shop auf- und zumachen. – Wurscht, oder? Ist jetzt halb so wild. Man kann aber genauso gut zum Beispiel die Gepäckabfertigung manipulieren. Dann kommen halt die Koffer alle irgendwo anders an, wo man sie vielleicht nicht haben will, und dort, wo man sie braucht, sind sie nicht. – Das ist sehr, sehr unangenehm, aber trotzdem noch einigermaßen handelbar. Man könnte sich aber auch in das Betriebssystem des Towers einhacken, und da schaut es dann schon ganz anders aus, denn dann kriegen wir wirklich die größten Probleme: wenn plötzlich zig Flugzeuge im Luftraum über Österreich ungelenkt sind, also keine Ahnung mehr haben, was ober ihnen, unter ihnen ist, was ihnen entgegenkommt, worauf sie zufliegen. – Deshalb ist es wichtig, dass wir Strukturen schaffen, die uns auch vor diesen Gefahren schützen, und das machen wir mit diesem Gesetz. *(Beifall bei den Grünen sowie bei Abgeordneten von ÖVP und SPÖ.)*

Ja, natürlich ist es unangenehm. Auf viele Unternehmen kommt ein Aufwand zu, den sie vorher nicht hatten. Ja, das ist nicht angenehm, aber es ist ein Sicherheitsmechanismus und es muss sein. Gewisse Sicherheitsvorkehrungen muss man einfordern und muss man einfordern können, weil es für uns alle, weil es für unsere gesamte Gesellschaft wichtig ist. Kinder mögen es auch nicht immer, wenn sie Schwimmflügerl angezogen bekommen. Aber ehrlich: Würden sie ihre Nichtschwimmerkinder ohne Schwimmflügerl ins Wasser lassen? – Nein. *(Abg. **Stefan** [FPÖ]: Das sagt eh alles! Genau so werden wir auch gesehen!)*

Genau dasselbe machen wir mit der Datensicherheit. Deshalb brauchen wir dieses Gesetz, und ich bin sehr froh, dass es so gut funktioniert hat, das gemeinsam umzusetzen. – Vielen Dank. *(Beifall bei den Grünen sowie bei Abgeordneten von ÖVP und SPÖ.)*

14.32

Präsidentin Doris Bures: Zu Wort ist dazu nun niemand mehr gemeldet. Damit ist die Debatte geschlossen.

Wünscht der Herr Berichterstatter ein Schlusswort? – Das ist nicht der Fall.

RN/81

Abstimmung

Präsidentin Doris Bures: Wir gelangen nun zur Abstimmung über den Gesetzentwurf in 308 der Beilagen.

Hiezu haben die Abgeordneten Friedrich Ofenauer, Maximilian Köllner, Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen einen Zusatz- beziehungsweise Abänderungsantrag eingebracht.

Ich werde daher zunächst über die vom erwähnten Zusatz- beziehungsweise Abänderungsantrag betroffenen Teile und schließlich über die restlichen, noch nicht abgestimmten Teile des Gesetzentwurfes abstimmen lassen.

Da der vorliegende Gesetzentwurf Verfassungsbestimmungen enthält, stelle ich zunächst im Sinne des § 82 Abs. 2 Z 1 der Geschäftsordnung die für die Abstimmung erforderliche Anwesenheit der verfassungsmäßig vorgesehenen Anzahl der Abgeordneten fest.

Die Abgeordneten Ofenauer, Köllner, Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben einen Zusatz- beziehungsweise Abänderungsantrag betreffend die Artikel 1 bis 3 eingebracht.

Wer dem zustimmt, den bitte ich um ein Zeichen. – Das ist mit Mehrheit so angenommen.

Schließlich kommen wir zur Abstimmung über die restlichen, noch nicht abgestimmten Teile des Gesetzentwurfes samt Titel und Eingang in der Fassung

der Regierungsvorlage.

Wer sich dafür ausspricht, den bitte ich um ein zustimmendes Zeichen. – Das ist mehrheitlich angenommen.

Ausdrücklich stelle ich die verfassungsmäßig erforderliche Zweidrittelmehrheit fest.

Wir kommen sogleich zur dritten Lesung.

Ich bitte jene Damen und Herren, die in der dritten Lesung zustimmen, um ein Zeichen. – Der Gesetzentwurf ist in dritter Lesung, wiederum mit der verfassungsmäßig erforderlichen Zweidrittelmehrheit, **beschlossen.**