RN/56

8. Punkt

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 Informationssystemsicherheitsgesetz 2026 – NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden (308 d.B. und 354 d.B. sowie 11725/BR d.B. und 11726/BR d.B.)

Vizepräsident Michael Wanner: Wir gelangen nun zu Punkt 8 der Tagesordnung.

Dazu begrüße ich Herrn Staatssekretär Leichtfried recht herzlich bei uns: Herzlich willkommen! *(Beifall bei ÖVP und SPÖ sowie der Bundesrätinnen **Jagl** [Grüne/NÖ] und **Deutsch** [NEOS/W].)*

Berichterstatter ist Herr Bundesrat Ernest Schwindsackl. – Ich bitte um den Bericht.

RN/57

Berichterstatter Ernest Schwindsackl: Herr Vizepräsident! Geschätzter Herr Staatssekretär! Werte Kolleginnen und Kollegen! Ich berichte 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 erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden.

Der Bericht liegt Ihnen in schriftlicher Form vor, ich komme daher gleich zur Antragstellung:

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 Art. 44 Abs. 2 B-VG die verfassungsmäßige Zustimmung zu erteilen.

Herzlichen Dank.

Vizepräsident Michael Wanner: Wir gehen in die Debatte ein.

Zu Wort gemeldet ist Herr Bundesrat Werner Gradwohl.

RN/58

13.10

Bundesrat Werner Gradwohl (FPÖ, Steiermark): Danke, Herr Präsident! Sehr geehrter Herr Bundesminister! Herr Staatssekretär! Werte Kollegen im Bundesrat! Sehr geehrte Damen und Herren im Saal und vor den Bildschirmen via Livestream! Ich begrüße die jungen Zuhörer *(Bundesrat* ***Reisinger*** *[SPÖ/OÖ]: … ausschließlich Zuhörer!)* im Hintergrund recht herzlich! – Danke, dass Sie so ein Interesse für den Bundesrat haben.

Wir beraten heute das Netz- und Informationssystemsicherheitsgesetz 2026 – ein Gesetz, das laut Regierung die Cybersicherheit in Österreich stärken soll. Ich sage gleich zu Beginn ganz klar: Niemand in diesem Haus stellt die Bedeutung von Cybersicherheit infrage. Cyberangriffe sind real, sie betreffen Staaten,

Unternehmen und Bürger gleichermaßen. Gerade deshalb braucht es Gesetze, die wirksam, verhältnismäßig und klar sind. *(Beifall bei der FPÖ.)*

Was wir heute vorliegen haben, ist jedoch ein Entwurf, der nicht aus Überzeugung entsteht, sondern aus Druck. Die NIS2-Richtlinie ist seit Anfang 2023 in Kraft. Die Umsetzungsfrist ist im Oktober 2024 abgelaufen. Österreich ist säumig und jetzt – Jahre später – wird uns gesagt, wir müssen das beschließen, sonst droht ein Vertragsverletzungsverfahren. Zeitdruck ersetzt keine Qualität. Ein schlechtes Gesetz wird nicht besser, nur weil man es zu spät beschließt.

Die Regierung spricht von rund 4 000 betroffenen Einrichtungen. Das ist keine Randnotiz, das ist ein massiver Eingriff in unsere Wirtschafts- und Verwaltungsstruktur. Doch niemand kann heute seriös beantworten, wie viele Betriebe konkret pro Sektor, pro Bundesland und entlang der Lieferketten betroffen sein werden, denn dieses Gesetz endet nicht bei den unmittelbar erfassten Einrichtungen. Durch die Verpflichtung zur Absicherung der Lieferkette werden auch zahlreiche kleine und mittlere Unternehmen erfasst – Betriebe, die weder vorbereitet noch informiert wurden. Das ist keine Transparenz, das ist Unsicherheit per Gesetz.

Besonders gravierend ist die Kostenfrage. Die Regierung legt keine nachvollziehbare Gesamtkostenabschätzung vor – weder für die Unternehmen noch für die öffentliche Hand. Internationale Vergleiche zeigen: Die einmaligen Implementierungskosten reichen von 10 000 Euro bis weit über 1 Million Euro. Dazu kommen laufende Kosten von 100 000 Euro pro Jahr – für zusätzliches Personal, externe Prüfungen, technische Sicherheitsmaßnahmen und umfassende Dokumentationspflichten. Diese Kosten verschwinden nicht, sie werden weitergegeben: an Konsumentinnen und Konsumenten, an Patientinnen und Patienten, an die gesamte Bevölkerung.

Kommen wir zu den Sanktionen: Geldstrafen von bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes. Das ist kein pädagogischer Zeigefinger, das ist eine existenzielle Bedrohung. *(Beifall bei der FPÖ.)*

Gleichzeitig bleiben die gesetzlichen Pflichten erstaunlich unklar. Es ist die Rede von geeigneten Maßnahmen, von Verhältnismäßigkeit, von gebührender Berücksichtigung von Risiken. Was das konkret bedeutet, soll eine Behörde per Verordnung festlegen können. Das Parlament gibt Kompetenzen ab und das Risiko bleibt bei den Unternehmern.

Besonders problematisch ist auch die institutionelle Konstruktion: Die neue Cybersicherheitsbehörde wird direkt dem Innenminister unterstellt. Gleichzeitig ist dieses Ressort für Überwachungsinstrumente zuständig, die strukturell davon leben, dass Sicherheitslücken existieren. Wer Sicherheitslücken schließen soll, darf kein Interesse daran haben, sie offenzuhalten.

Mit diesem Gesetz schaffen wir einen großen neuen Apparat: ein Bundesamt, mehrere Computer-Notfallteams, Sondergremien, Koordinationsstellen im Gesundheitsbereich. Die Kosten für die öffentliche Hand werden sich in den nächsten fünf Jahren auf geschätzte 150 bis 200 Millionen Euro belaufen. Mehr Behörden bedeuten aber nicht automatisch mehr Sicherheit.

Der Bundesrat ist nicht dazu da, Gesetze einfach durchzuwinken. Er ist dazu da, dort Nein zu sagen, wo ein Gesetz aus dem Gleichgewicht gerät. *(Beifall bei der FPÖ.)*

Cybersicherheit darf kein Vorwand für Bürokratie, unklare Pflichten und Millionenstrafen sein. Sicherheit entsteht durch klare Regeln, nicht durch Angst.

Ein Gesetz, das Kosten verschweigt, Verantwortung abschiebt und Existenzen gefährdet, ist kein gutes Gesetz. Ein schlechtes Gesetz wird nicht richtig, nur

weil die EU Druck macht. Ein teures Gesetz wird nicht gerecht, nur weil man es Sicherheit nennt. Deshalb sage ich klar und verantwortungsvoll: Aus diesen Gründen können wir diesem Gesetz nicht zustimmen. *(Beifall bei der FPÖ.)*

13.16

Vizepräsident Michael Wanner: Als Nächster zu Wort gemeldet ist Bundesrat Klubvorsitzender Mag. Harald Himmer.

RN/59

13.17

Bundesrat Mag. Harald Himmer (ÖVP, Wien): Sehr geehrter Herr Präsident! Herr Staatssekretär! Hohes Haus! Sehr geehrte Damen und Herren hier im Saal und vor den Bildschirmen! Liebe Besuchergruppe! Wir besprechen ein sehr wichtiges Thema, nämlich die Cybersicherheit für unsere Unternehmen in Österreich. Mein Vorredner hat dankenswerterweise gesagt, dass er die Problemerkenntnis – nämlich dass Cybersicherheit eine wichtige Thematik ist – voll anerkennt. Offensichtlich sollte man dann eigentlich in diesem Punkt im Hohen Haus oder hier im Bundesrat keine zweite Meinung haben.

Was das Thema betrifft, dass man Gesetze immer umfassender oder länger diskutieren kann: Das kann man, glaube ich, zu jedem Gesetz sagen. Meiner Erinnerung nach haben wir dieses Gesetz in der vorhergehenden Gesetzgebungsperiode nicht durchgebracht, weil uns damals die Zweidrittelmehrheit gefehlt hat. Damals waren auch die SPÖ und die NEOS dagegen. Wenn sie heute zustimmen, dann ist in diesem Gesetz ja offensichtlich etwas überarbeitet worden. *(Bundesrat **Spanring** [FPÖ/NÖ]: Das glaubt's jetzt aber nicht selber!)*

Was ich nur zu den Argumenten meines Vorredners vorbringen möchte: Ich weiß nicht, was von den Argumenten durch eine längere Begutachtungsperiode

ausräumbar wäre. Tatsache ist natürlich, dass die Abwehr von Cyberangriffen überwacht werden muss und dass es dazu auch gesetzliche und institutionelle Regelungen geben muss. Klar ist auch, dass – wenn man danach ruft, dass das alles ganz präzise sein soll, Herr Kollege – wir alle wissen, dass es bei Definitionen wie kritische Unternehmen, größere Unternehmen, kleinere Unternehmen und so weiter wohl sehr aufwendig wäre, taxativ alle Unternehmen in Österreich in einem solchen Gesetz abzubilden. Gleichzeitig ist es natürlich, was die Kostenseite betrifft, auch nicht so einfach, das in das Gesetz hineinzuschreiben – völlig abgesehen davon, dass ja gerade die Kostenstruktur im Technologie- und Datenbereich äußerst volatil ist.

Tatsache ist aber auch, dass kein Weg daran vorbeiführt. Die Annahme, dass wir uns vorstellen könnten, dass es irgendwann einmal keine Cyberattacken mehr geben wird, ist sehr unwahrscheinlich. Also diese Entwicklung bleibt, die ist nicht mehr umkehrbar.

Natürlich ist es richtig, dass größere Unternehmen mehr Möglichkeiten haben, sich gegen Cyberangriffe zu wehren, in dem Sinn, dass sie größere Organisationen, größere IT-Organisationen, mehr Fachleute haben et cetera, allerdings ist es eben auch so, dass auch kleine Unternehmen sich wehren müssen, und dabei ist es dann wiederum der Fall, dass nicht jedes kleine Unternehmen ein eigenes Security-Operation-Center wird etablieren können. Also dass jetzt in dieser Form kleinere Unternehmen Unterstützung brauchen, das ist ja wohl ganz klar, und das ist ja auch das, was hier angedacht vonseiten des Ministeriums ist: nicht, dass es die Überwachung ist, sondern dass die kleineren Unternehmen Unterstützung bekommen, dass man da mithilft, dass man die Summe der Cyberangriffe, die auf Österreich einprasseln und die mehrere und viele KMUs betreffen, gemeinsam abarbeitet und dass Experten dann im Ministerium auch gerade diesen Unternehmen helfen.

Ich bin überzeugt davon, dass der Herr Staatssekretär und auch der Herr Minister nichts daran ändern werden, dass sie ihre Beamten dahin gehend anweisen, dass es Unterstützung geben soll und dass nicht die prioritäre Absicht ist, dass jetzt bestraft werden soll. Und dass es jetzt in einem Gesetz auch immer wieder bestimmte Pönalen gibt für das Nichteinhalten von bestimmten Maßnahmen, okay, das ist halt auch etwas, das üblich ist, denn wenn wir jetzt zum Beispiel sagen würden, man soll 130 km/h auf der Autobahn fahren, aber es gibt keine Konsequenzen, dann werden halt wesentlich mehr Leute über 130 km/h fahren, wenn man dafür keine Strafe zahlen muss, wenn das einfach nur ein dezenter Hinweis ist.

Oder sagen wir, es gäbe zum Beispiel nur eine freiwillige Redezeitbeschränkung von 10 Minuten *(Heiterkeit bei der ÖVP):* Wenn es nur freiwillig ist, ohne Sanktionen, dann ist es etwas, das eingehalten wird oder eben auch nicht, weil es dazu keine Sanktionen gibt. Genauso ist es bei einem Gesetz: Wenn ein Gesetz nur unverbindlich wäre, dann wäre es für die Behörden natürlich auch schwierig, es zu exekutieren.

Aus diesen Gründen und aus vielen mehr werden wir dieser Gesetzesvorlage natürlich zustimmen. *(Beifall bei der ÖVP und bei Mitgliedern des Bundesrates von der SPÖ.)*

13.22

Vizepräsident Michael Wanner: Danke schön.

Als Nächste zu Wort gemeldet ist Frau Bundesrätin Sandra Jäckel.

RN/60

13.22

Bundesrätin Sandra Jäckel (FPÖ, Vorarlberg): Vielen Dank, Herr Vizepräsident! Herr Staatssekretär! Werte Kollegen im Bundesrat! Hallo, Besucher! Es sind

viele junge Leute hier bei uns im Plenarsaal, das freut mich sehr. Liebe Zuseher via Livestream! NIS 2 ist eine EU-Richtlinie aus Brüssel, die vorgibt, das Cybersicherheitsniveau - - *(Eine Besuchergruppe verlässt den Saal. – Bundesrat* ***Ruprecht*** *[ÖVP/Stmk.]: Ich glaube, die Besucher:innen haben sich nicht angesprochen gefühlt!)* – Das ist egal! Ich bin trotzdem höflich, ich bin gut erzogen *(Beifall bei der FPÖ):* Ein: Bitte!, ein: Danke!, ein: Grüß Gott!, und ein: Auf Wiedersehen!, ich glaube, das gehört in die Kinderstube.

Ich fange noch einmal von vorne an: NIS 2 ist eine EU-Richtlinie aus Brüssel, die vorgibt, das Cybersicherheitsniveau zu erhöhen, indem sie auch in Österreich Staaten und Tausende Unternehmen mit neuen Pflichten, Kontrollen und massiven Strafdrohungen überzieht: mehr Meldepflichten, mehr Auflagen und mehr Bürokratie. Ob das eine Garantie für die Sicherheit in Österreich ist, ist für mich fraglich.

Zweifellos: Cybersicherheit ist notwendig, das bestreitet niemand, auch wir Freiheitlichen nicht. Der Schutz kritischer Infrastruktur, von Daten, von Unternehmen und staatlichen Systemen ist unerlässlich; strittig ist nur, was die Regierung hier daraus macht.

Herr Staatssekretär, ich weiß nicht, ob Sie es mitbekommen haben oder ob der Kelch an Ihnen vorbeigezogen ist, denn auch das Ressort Innenministerium war bereits Ziel eines Cyberangriffs.

Jetzt frage ich mich: Warum wurde ein Gesetz, das bereits 2024 vom Verfassungsgerichtshof aufgehoben wurde, nun nahezu unverändert wieder vorgelegt? Und warum – das ist die größte Frage, die sich mir da stellt, liebe SPÖ und liebe NEOS – stimmen Sie, obwohl Sie dieses Gesetz damals strikt abgelehnt haben, nun einhellig zu? *(Beifall bei der FPÖ.)*

Da kommt mir natürlich auch gleich die Antwort: Ein paar Regierungssessel mehr und schon sind alle Bedenken vergessen! – Diese politische Beliebigkeit ist bezeichnend für diese Verliererregierung. *(Beifall bei der FPÖ.)*

Wie soll dieses Gesetz nun umgesetzt werden? – Ich sage es Ihnen: Aus sieben Sektionen werden 18. Über 4 000 Unternehmen werden verpflichtet, eine Flut an technischen, organisatorischen und operativen Maßnahmen umzusetzen – und das Größte an dem Ganzen: begleitet von Strafdrohungen von bis zu 10 Millionen Euro. Ich frage Sie: Wie soll das ein mittelständischer Betrieb bewältigen? Wie soll ein Investor bei solchen Haftungsrisiken noch Vertrauen in den Standort Österreich haben?

Diese Verliererregierung redet ständig von Entbürokratisierung, von Deregulierung, von wirtschaftlicher Vernunft, und zeitgleich wird hier ein Gesetz geschaffen, das die Bürokratie wieder einmal explodieren lässt. Die klassische Frage, die wir uns schon gestern und heute auch immer wieder gestellt haben, lautet: Wo ist der Deregulierungs-Sepp? Staatssekretär Schellhorn hat vor Kurzem 113 sogenannte Entlastungsmaßnahmen präsentiert. Für mich sind das reine Scheinmaßnahmen, um die eigene Daseinsberechtigung medial zu verkaufen. *(Beifall bei der FPÖ.)*

Wenn Schellhorn ernsthaft darüber nachdenkt – der Super-GAU heute in den Medien –, bei den Bundesländern von neun auf drei einzusparen, liebe Kollegen im Bundesrat, dann sage ich ganz klar: Den Schellhorn einzusparen, wäre ein Fortschritt und vermutlich die sinnvollste Einsparung dieser Regierung. *(Beifall bei der FPÖ. – Ruf bei der FPÖ: Bravo!)*

Kommen wir zurück zum Eigentlichen: Wie gesagt, von Staatssekretär Schellhorn hört man kein Wort, keinen Widerstand, keinen Einsatz für Betriebe. *(Ruf bei der SPÖ: Das ist ja nicht notwendig, das ist ja ein gutes Gesetz!)* Kollege Schellhorn begibt sich lieber nach Lech und macht dort Showkochen.

Parallel dazu plant das Innenministerium ein neues Bundesamt für Cybersicherheit – schon wieder ein neuer Behördenapparat, schon wieder Versorgungsposten für die Parteifreunde der ÖVP, statt für Sicherheit für die Bevölkerung zu sorgen. Bis 2029 sollen 172 Planstellen geschaffen werden. Ich als Polizistin sage Ihnen ganz klar: Diese 172 Planstellen fehlen draußen, sie fehlen in Inspektionen, bei der Bereitschaftseinheit, dort, wo Sicherheit nicht verwaltet, sondern durchgesetzt wird. *(Beifall bei der FPÖ.)*

Das, was Sie hier betreiben, ist für mich kein Sicherheitskonzept, das ist Postenschacher auf Kosten unserer Bevölkerung, ein weiteres klassisches Versagen des ÖVP-Innenministeriums. *(Bundesrat **Himmer** [ÖVP/W]: Aber jetzt redest du wirklich einen Topfen!)* – Nein, das stimmt nicht, Herr Kollege Himmer. *(Bundesrat **Himmer** [ÖVP/W]: Nein, jetzt redest du wirklich einen Topfen! Und wer soll sich um das kümmern?)* Ich habe das letzte Sitzung - - *(Bundesrat **Himmer** [ÖVP/W]: Wer kümmert sich um die Cybersicherheit?)* Es gibt externe - - *(Bundesrat **Himmer** [ÖVP/W]: Machen wir einfach - -!)* Schauen Sie, wir haben das ja im Ausschuss besprochen: Es gibt auch Externe, die das machen können. *(Bundesrat **Himmer** [ÖVP/W]: Ja, Externe, ja!)* Warum sollen wir immer nur die Basis dafür opfern, Kollege? *(Bundesrat **Himmer** [ÖVP/W]: Externe für ganz Österreich! Eine Firma - -!)* Ich glaube, Sie waren schon lange nicht mehr an der Basis beim exekutiven Außendienst. *(Beifall bei der FPÖ. – Neuerlicher Zwischenruf des Bundesrates **Himmer** [ÖVP/W].)*

Ich habe es bereits in der letzten Sitzung dieses Hauses unmissverständlich festgehalten: Die Personaldecke bei der Polizei schrumpft. *(Bundesrat **Himmer** [ÖVP/W]: Das ist ja kein Straßenpolizist ...!)* Es gibt immer weniger, vielen Dienststellen fehlen die Planstellen, Minimalbesetzungen, Überstundenkürzungen. Ich sage Ihnen eines: Besonderes - - *(Bundesrat **Himmer** [ÖVP/W]: Ja! Cybersicherheit gegen Straßenpolizisten!)* – Fängt auch auf den Straßen an. *(Bundesrat **Himmer** [ÖVP/W]: Aber diese zwei Themen zu vermischen,*

ist einfach so etwas von unsachlich, ja?) Ich sage Ihnen: Reden Sie mit der Basis und reden Sie nicht nur hier im Parlament!

Besonders verantwortungslos, Herr Staatssekretär, ist der Umgang mit unserer Spezialeinheit – das ist die Cobra –, denn ausgerechnet bei der Cobra – dort, wo es um Sekunden und Menschenleben geht – Personal und Ressourcen zu reduzieren, ist für mich ein sicherheitspolitischer Offenbarungseid und ein Risiko für unsere Bevölkerung. *(Beifall bei der FPÖ.)*

Zusammenfassend: Gerade in unserer Zeit – Terrorgefahr, Waffen, Messergewalt – wachsen die Unsicherheiten in ganz Österreich, und ich sage jetzt einfach zusammenfassend ganz klar: Dieses Gesetz steht für falsche Prioritäten – für ÖVP-Postenschacherei statt Schutz *(Bundesrat* ***Himmer*** *[ÖVP/W]: Nein! Das ist so ein Unsinn!)* der Bevölkerung –, und aus Sicht der FPÖ ist das eine unverantwortliche Politik.

Wer glaubt, mit neuen Behörden, neuen Posten und immer dickeren Gesetzesmappen Sicherheit zu schaffen, hat hier den Ernst der Lage nicht verstanden. *(Beifall bei der FPÖ.)*

13.29

Vizepräsident Michael Wanner: Als Nächster zu Wort gemeldet ist Herr Bundesrat Dominik Reisinger. – Bitte.

RN/61

13.29

Bundesrat Dominik Reisinger (SPÖ, Oberösterreich): Sehr geehrter Herr Präsident! Sehr geschätzter Herr Staatssekretär! Hohes Haus! Kolleginnen und Kollegen! Werte Zuhörerinnen und Zuhörer! Wir debattieren hier unter diesem Tagesordnungspunkt das Netz- und Informationssystemsicherheitsgesetz – ein

ein bisschen sperriger Begriff, aber wenn man sich damit beschäftigt, wird vieles plausibel und logisch.

Dieses Gesetz muss sozusagen neu geordnet werden, es braucht eine Adaption, und das ist wichtig und notwendig, weil der rasante technische Fortschritt, der Fortschritt der Technologien schier ungeahnte Möglichkeiten bietet. Dieser Fortschritt bietet Möglichkeiten im negativen wie im positiven Sinn. Mit im negativen Sinn meine ich, dass diese Technologien natürlich auch missbräuchlich verwendet und eingesetzt werden können, wenn kriminelle Energie zutage tritt.

Cyberkriminalität, Cyberangriffe sind leider allgegenwärtig. Daher müssen wir hier auch die gesetzlichen Rahmenbedingungen schaffen, nachschärfen und alles tun, um das Sicherheitsniveau aufrechtzuerhalten oder sogar zu heben. *(Beifall bei der SPÖ.)*

Ich bin mir nicht sicher, ob das allen bewusst ist: Diese neuen Kriminalitätsformen können jeden treffen, Private, größere Institutionen und vor allem die kritische Infrastruktur. Diese vielfältigen Angriffsflächen müssen wir eben bestmöglich schützen und das tun wir mit diesem Gesetz. Ein Teil- oder Totalausfall der kritischen Infrastruktur hätte nämlich fatale Folgen. Herr Kollege Gradwohl – er ist gerade nicht im Saal –, natürlich hat der Experte im Ausschuss Zahlen der Folgekostenabschätzung genannt, aber es ist eben schwierig, zum jetzigen Zeitpunkt auf Punkt und Beistrich Zahlen zu nennen. *(Präsident **Samt** übernimmt den Vorsitz.)*

Aber eine Frage zurück: Haben Sie schon einmal ausgerechnet, was es kosten würde, wenn solch kritische Infrastruktur total ausfallen würde, wenn Krankenhäuser, große Nahversorger, Verkehrsbetriebe, Wasserversorger, Banken nicht mehr funktionieren würden, tage-, wochenlang? Welche Kosten

würde das verursachen? – Diese Kosten und der Schaden wären um ein Vielfaches größer.

Leider reicht das Zahlenwerk der FPÖ hier nicht aus, und es ist schade, dass diese wichtige Maßnahme zur Anhebung unserer Sicherheit von Ihnen hier nicht mitgetragen wird. *(Beifall bei SPÖ und ÖVP.)*

Was sind jetzt, um es auf den Punkt zu bringen, die wesentlichen Maßnahmen? – Es wird, das haben wir schon gehört, eine eigenständige Cybersicherheitsbehörde, das Bundesamt für Cybersicherheit, geschaffen. Es geht darum, hier Maßnahmen zu setzen, um das Sicherheitsniveau zu heben. Dieses Bundesamt wird die zentrale Anlaufstelle sein. Es geht um die Meldung und die Behandlung von Sicherheitsvorfällen, und es geht natürlich auch, wie immer in diesem großen Bereich der Sicherheit, um den internationalen Austausch und um Kontaktpflege.

Eine wesentliche Aufgabe des Bundesamtes ist es aber vor allem auch, und das habe ich heute noch nicht gehört, dass es als Schnittstelle für den privaten und für den öffentlichen Sektor fungiert – wir wollen eben die Menschen nicht allein lassen. Und ganz wichtige und zentrale Punkte sind auch Bewusstseinsbildung und Prävention, um die gesamtstaatliche Resilienz in diesem Bereich hochzuhalten.

Zentral aus meiner Sicht ist auch die Ausweitung der Berichtspflichten, damit wird die parlamentarische Kontrolle sichergestellt. Weisungen des Innenministers müssen halbjährlich veröffentlicht werden und die Direktorin beziehungsweise der Direktor dieses Bundesamtes muss auch für Informationen zur Verfügung stehen, und zwar in den zuständigen Ausschüssen des Nationalrates. Darüber hinaus wird der Datenschutzbeauftragte des BMIs hier natürlich auch den Datenschutz, der ganz wichtig ist, im Auge behalten.

Alles in allem eine wichtige Gesetzesmaterie, die unsere Sicherheit erhöht. Ich danke der Regierung, ich danke allen, die bei diesem Gesetz mitziehen, und ich finde es sehr schade, dass die FPÖ wieder einmal gegen mehr Sicherheit in Österreich ist. – Danke für die Aufmerksamkeit. *(Beifall bei SPÖ und ÖVP sowie der Bundesrätin **Deutsch** [NEOS/W].)*

13.35

Präsident Peter Samt: Als Nächste zu Wort gemeldet ist Frau Bundesrätin MMag. Dr. *(Zwischenruf der Bundesrätin **Kittl** [Grüne/W])* – fast; aber das kommt ja vielleicht noch *(Bundesrätin **Kittl** [Grüne/W] – auf dem Weg zum Rednerinnen- und Rednerpult –: Das wäre schön!)* – Elisabeth Kittl. – Bitte, Frau Kollegin.

RN/62

13.35

Bundesrätin MMag. Elisabeth Kittl, BA (Grüne, Wien): Danke, Herr Präsident! Sehr geehrter Herr Staatssekretär! Liebe Kollegen und Kolleginnen! Liebe Besucher:innen, ich freue mich, dass Sie hier sind, dass ihr hier seid! Ja, das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus im digitalen Bereich ist grundsätzlich sehr, sehr begrüßenswert, denn es gibt heute so gut wie gar nichts mehr, und das wissen wir, das ohne digitale Struktur funktioniert. Und dass sie in jedem Bereich sicher funktioniert, ist umso wichtiger.

Wir brauchen nur daran zu denken, wie wir reagieren, wenn Computer oder Handy nicht mehr funktionieren, wie wir uns darüber ärgern und von wie vielen – extrem vielen – Informationen und Funktionen wir abrupt abgeschnitten sind.

Aber dass sich jemand Fremder in unser System oder unsere Privatsphäre einschleicht, ist zusätzlich extrem bedrohlich, und es ist natürlich beängstigend. Bedrohlich ist es vor allem dann, wenn es um Behörden und Unternehmen oder

eben Ministerien geht. Und wir haben es schon gehört, die kritische Infrastruktur ist da ein wesentlicher Punkt. Das ist das, was schon genannt wurde, plus die Bereiche Telefon, Internet, Wasserversorgung, Gesundheit, Energie, Verkehr, Post, Müll, öffentliche Verwaltung – eigentlich kann man gar nicht alles aufzählen, weil schon alles digital eingebettet in eine Struktur, eine sehr vernetzte Struktur, ist.

Das ist eben genau das Ding, diese Vernetzung ist ein wichtiger Punkt, der eben genau den Schutz braucht, denn wenn ein Unternehmen, eine Behörde betroffen ist, wirkt sich das auch auf andere aus.

Ja, es ist mühsam, für diese Sicherheit zu sorgen, aber es zahlt sich auf jeden Fall aus, und es zahlt sich auch für den Wirtschaftsstandort Österreich aus, denn Unsicherheit, und das habe ich schon öfters hier betont, ist nie ein Wirtschaftstreiber.

Cybersicherheit bedeutet Schutz vor privaten Hacker:innen, aber – leider muss man das jetzt auch ansprechen – auch vor hybrider Kriegsführung; das sind Angriffe, das sind Sabotage oder Spionage und die werden leider jeden Tag mehr. Daher ist eine staatliche Aufsicht hier ein guter und vor allem auch ein notwendiger Schritt, auch aus Sicht der EU, denn sie schreibt das in einer Richtlinie vor.

Aber es ist ein großer Eingriff, denn es ist ein staatlicher Zugriff auf private Daten beziehungsweise wird dadurch ein solcher ermöglicht. Die neu geschaffene zuständige Stelle heißt Cybersicherheitsbehörde und ist beim Innenministerium angesiedelt. Diese Stelle überprüft unter anderem, was Behörden und was Unternehmen tun, wenn bei ihnen ein Sicherheitsvorfall passiert.

Solch ein Vorfall muss dann auch gemeldet werden, und diese Meldung geht wiederum auch an die Europäische Union weiter, da er wie schon erwähnt Auswirkungen auch an anderen Orten haben kann. Und für den Fall, dass es notwendig ist, kommen dann private operative Computernotfallteams auch vor Ort.

Wenn die Unternehmen oder auch die Behörden aber nicht genügend Maßnahmen setzen, können den Unternehmen auch mit Bescheid solche Maßnahmen vorgeschrieben werden. Und wenn diesen nicht Folge geleistet wird, werden Ersatzmaßnahmen gesetzt.

Zudem wird auch eine Whistleblower-Stelle für Schwachstellen und Sicherheitslücken in Behörden oder Unternehmen eingerichtet.

Ja, das ist eben eine Menge an Befugnissen, durch die das Innenministerium bei Cybersicherheitsvorfällen Zugriff auf sehr viele und sehr kritische Daten bekommt. Und daher, ja, ist bei diesem Gesetz wohl auch ein Missbrauchsrisiko gegeben, vor allem, wenn wir bedenken, dass es den Bundestrojaner gibt und das Innenministerium mit Spionagesoftware nach Sicherheitslücken suchen soll. Und das am selben Ort, zumindest eben von der Spitze her gesehen, an dem man nun auch Sicherheitslücken sammeln wird. Das ist heikel, und wir sagen auch immer noch, dass wir gegen diese Verwendung dieser Spionagesoftware sind.

Wir Grünen haben auch mitverhandeln dürfen und haben zusätzliche Kontrollmechanismen gefordert und erfolgreich hineinverhandelt, nämlich dass zweimal im Jahr Berichte über diese Arbeit der Cybersicherheitsbehörde zeitnah, das heißt eben innerhalb von ein paar Monaten, ins Parlament kommen und nicht erst nach ein, zwei Jahren.

Das ist auch wichtig und das bedarf einer aufmerksamen Kontrolle durch uns. Ich denke, wir sollten da auch unbedingt mehr Expertise im IT-Bereich aufbauen.

Aber auch die Cybersicherheitsbehörde braucht entsprechendes Personal. Das werden – ich habe nachgefragt – an die 200 Leute sein, und da müssen wir natürlich schauen, dass es genügend Ausbildungsmöglichkeiten gibt; für die Cybersicherheitsbehörde, aber natürlich auch für uns.

Da diese Berichte ins Parlament kommen, sind sie natürlich auch öffentlich. Das ist total wichtig, denn es gibt Expert:innen aus der Zivilgesellschaft, entsprechende NGOs, die diese Berichte auch kontrollieren wollen und denen ich, wie zum Beispiel Epicenter Works, explizit für ihre Arbeit danken möchte.

Zusätzlich hätte man aber auch unabhängige Kommissionen oder Beiräte zur Kontrolle installieren können. An Einsprüchen gegen Bescheide der Sicherheitsbehörde oder Aufschreien gegen das operative Vorgehen vor Ort werden wir dann aber sehen, ob die Arbeit der Cybersicherheitsbehörde noch mehr an Kontrolle bedarf.

Wir werden es im Auge behalten, stimmen aber heute zu, da die positiven Aspekte des Gesetzes für mehr Cybersicherheit überwiegen. – Vielen Dank. *(Beifall bei den Grünen und bei Mitgliedern des Bundesrates von der ÖVP.)*

13.41

Präsident Peter Samt: Bevor wir den nächsten Redner hören, darf ich recht herzlich bei uns Besuch aus dem Burgenland begrüßen. Es ist eine Abordnung der FPÖ Güssing mit Landtagsabgeordneten Mag. Thomas Grandits. Herzlich willkommen! *(Allgemeiner Beifall.)*

Als Nächste zu Wort gemeldet ist Frau Bundesrätin Mag. Dr. Julia Deutsch. Jetzt stimmt das mit dem Doktor auch.

RN/63

13.41

Bundesrätin Mag. Dr. Julia Deutsch (NEOS, Wien): Vielen Dank, Herr Präsident! Sehr geehrter Herr Staatssekretär! Werte Kolleginnen und Kollegen! Liebe Zuseherinnen und Zuseher hier im Saal und natürlich auch vor den Bildschirmen zu Hause! Wir sprechen heute über NIS2 und somit sprechen wir ganz klar über Sicherheit – nicht abstrakt, nicht theoretisch, sondern wir sprechen ganz konkret über den Schutz unserer kritischen Infrastruktur, unserer Unternehmen und letztlich der Menschen in unserem Land.

Cyberangriffe sind längst keine Randerscheinung mehr. Sie treffen Verwaltungen, sie treffen Spitäler, sie treffen Energieversorger, Verkehrssysteme und Betriebe, und das auf täglicher Basis. Sie werden von der Öffentlichkeit nicht immer bemerkt, aber sie passieren, das ist Fakt, und sie verursachen Schäden in Milliardenhöhe. Wer jetzt glaubt, wir könnten uns Zeit lassen oder auf freiwillige Maßnahmen hoffen, der verkennt die Realität. *(Zwischenruf des Bundesrates **Reisinger** [SPÖ/OÖ].)*

Mit diesem Gesetzesbeschluss setzen wir nun europäische Standards um. Wir stärken die Widerstandsfähigkeit der österreichischen Cybersicherheitsinfrastruktur. Das ist notwendige Vorsorge in einer Zeit, in der digitale Angriffe Teil hybrider Bedrohungen geworden sind, und das auch und gerade durch staatliche Akteure.

Wichtig ist für uns NEOS aber auch: Sicherheit darf nicht mit Bürokratie verwechselt werden. Deswegen war für uns auch entscheidend, dass dieser Gesetzentwurf gegenüber der Vision von 2024 deutlich verbessert worden ist. *(Zwischenrufe bei der FPÖ.)* Zentrale Kritikpunkte aus der Wirtschaft und aus Fachkreisen wurden eingearbeitet und ernst genommen. Das Ergebnis ist ein

Gesetz, das klare Rahmenbedingungen schafft und gleichzeitig unnötige Belastungen vermeidet.

Konkret heißt das, bestehende Zertifizierungen wie zum Beispiel ISO-Normen werden anerkannt, Doppel- und Mehrfachprüfungen entfallen. Unternehmen erhalten auch ausreichend Übergangsfristen, um die Vorgaben umzusetzen. Statt neuer Hürden gibt es Unterstützung und Orientierung.

Ein weiterer wesentlicher Punkt für uns ist die institutionelle Ausgestaltung. Die NIS-Behörde – also das Bundesamt für Cybersicherheit – ist eigenständig organisiert und nicht mehr direkt beim Innenminister verankert. Das ist wirklich wesentlich, denn Weisungen dürfen auch nur schriftlich erfolgen und müssen transparent dokumentiert werden. *(Bundesrätin **Jäckel** [FPÖ/Vbg.]: Keine Ahnung!)* Das stärkt die Rechtsstaatlichkeit und das Vertrauen in die Arbeit der Behörde.

Was für uns in dieser Hinsicht auch relevant war, sind die halbjährlichen Lageberichte, sie sind ein wichtiger Fortschritt. Cyberbedrohungen entwickeln sich rasant, und wer nur einmal im Jahr draufschaut, der erkennt vielleicht Bedrohungen viel zu spät. Wir setzen da bewusst auf Aktualität und auf Handlungsfähigkeit. Für uns ist nämlich klar: Digitale Sicherheit bedeutet auch aktives Handeln, nichts tun oder verzögern erhöht nur das Risiko für Unternehmen, für die öffentlichen Einrichtungen und für die Gesellschaft insgesamt. Gerade in Zeiten zunehmender geopolitischer Spannungen ist es umso relevanter, resilient zu sein.

Dieses Gesetz schafft Klarheit, stärkt effektiv die Sicherheit und bleibt dabei verhältnismäßig, deshalb stimmen wir NEOS – oder in dem Fall hier ich – diesem Gesetz heute auch zu. – Vielen Dank. *(Beifall bei ÖVP und SPÖ.)*

13.45

Präsident Peter Samt: Zu Wort gemeldet hat sich Herr Staatssekretär Mag. – schon wieder Magister – Jörg Leichtfried. *(Staatssekretär **Leichtfried:** Magister passt schon! – Bundesrat **Reisinger** [SPÖ/OÖ]: Stimmt eh! In dem Fall stimmt's eh! – Staatssekretär **Leichtfried:** Passt ja! Nicht Doktor!)*

RN/64

13.45

Staatssekretär im Bundesministerium für Inneres Mag. Jörg Leichtfried: Vielen Dank, Herr Präsident! Geschätzte Damen und Herren Bundesrätinnen und Bundesräte! Geschätzte Besuchergruppe aus dem Burgenland! Schöne Grüße an den Landeshauptmann, wenn ihr ihn wieder einmal seht. *(Allgemeine Heiterkeit.)* Sehr geehrte Damen und Herren, die Sie sonst zusehen! Die Bedrohung für Europa und auch für Österreich ist in vielerlei Hinsicht größer, komplexer und anspruchsvoller geworden. Hybride Bedrohungen, Spionage, Desinformation haben oft ihre Ursprünge im Ausland, aber gefährden unmittelbar unseren Staat, unsere Gesellschaft und die Wirtschaft hier in Österreich. Darum geht es in diesem Gesetz, sehr geehrte Damen und Herren Bundesrätinnen und Bundesräte.

Herr Bundesrat Gradwohl und Frau Bundesrätin Kittl haben die Frage Sicherheitslücken angesprochen. Genau diese Sicherheitslücken sollen durch dieses Gesetz geschlossen werden, nämlich bei den Menschen, die es brauchen, bei den Unternehmen, die es brauchen, und auch bei den öffentlichen Behörden, die es brauchen. *(Beifall bei SPÖ und ÖVP.)*

Aber, geschätzte Damen und Herren, ich sage das auch ganz klar und sehe da keinen Widerspruch: Das Gegenteil gilt für Menschen, die bei uns Terroranschläge verüben wollen, das Gegenteil gilt für Menschen, die bei uns Menschen umbringen möchten. Die sollen sich in Zukunft nicht einmal in ihren verschlüsselten Whatsapp-Kanälen sicher in unserem Land fühlen, sehr geehrte

Damen und Herren! *(Beifall bei SPÖ und ÖVP sowie der Bundesrätin **Deutsch** [NEOS/W].)*

Frau Kollegin Jäckel, Sie haben den Konflikt – es ist schon ein bisschen ein Konflikt – zwischen der Personalsituation in zentralen Stellen und in den Posten, die direkt am Land und in der Stadt angesiedelt sind, angesprochen. Diesen Konflikt gibt es natürlich. Mir wäre auch lieber, es würden alle so besetzt werden, dass alle zufrieden sind. Das werden wir wahrscheinlich nie erreichen, deshalb würde ich meinen, es ist beides wichtig.

Ich möchte, weil Sie eben die Posten angesprochen haben, im Gegenzug auch erwähnen: Eine Zentralstelle, für die ich zuständig bin, nämlich die Direktion Staatsschutz und Nachrichtendienst, hat in den letzten zwei Jahren ganz konkret neun Terroranschläge in Österreich verhindert. Dafür möchte ich mich herzlich bedanken, und es ist natürlich auch notwendig, das zu tun. *(Beifall bei SPÖ und ÖVP sowie der Bundesrätin **Jäckel** [FPÖ/Vbg.].)*

Es wurde auch angesprochen, dass es zu dem Thema früher andere Meinungen gegeben hat. Ich selbst war früher auch der Auffassung, dass der Vorschlag, der damals vorgelegt wurde, nicht so gut war, und ich war auch nicht dafür. Aber man muss schon sagen, es hat sich jetzt einiges geändert, die Dinge haben sich massiv verbessert: Also es ist insgesamt die Stärkung des Datenschutzes besser geworden; die Entlastung von kleinen und mittleren Unternehmen; die Einrichtung als unabhängige – soweit es in der Dienststruktur möglich ist – und entpolitisierte Einrichtung; die Berichtspflichten an den National- und den Bundesrat, die Auskunftserteilung an den National- und den Bundesrat und auch die Änderung von jährlichen Berichten auf halbjährliche, all das ist schon erreicht worden. Das war meines Erachtens eine durchaus positive Entwicklung, wenn man jetzt den Erststand der Vorschläge mit dem, was jetzt herauskommt, vergleicht.

Sehr geehrte Damen und Herren! Weil dieses Gesetz auch in die Kompetenzen der Länder eingreift, ist es notwendig, dafür auch Verfassungsmehrheiten zu finden, und ich möchte mich bei jenen bedanken, die außerhalb der Koalition diese Verfassungsmehrheit auch ermöglicht haben; das ist auch nicht selbstverständlich. Herzlichen Dank dafür, das ist schon ein konstruktiver Oppositionszugang, würde ich sagen. *(Beifall bei SPÖ und ÖVP sowie der Bundesrätin **Hauschildt-Buschberger** [Grüne/OÖ].)*

Sehr geehrte Damen und Herren, mit diesem Entwurf ist ein wichtiger Schritt in Richtung eines robusten Sicherheitsnetzes gelungen. Wir haben ein gesamtstaatliches Konzept geschaffen.

Mein letzter Appell geht noch an die FPÖ, vielleicht im Sinne einer Gesamtverantwortung noch einmal darüber nachzudenken – eine Rede kommt ja noch –, zuzustimmen. Das würde mich sehr freuen. Ansonsten herzlichen Dank für Ihre Aufmerksamkeit. *(Beifall bei SPÖ und ÖVP sowie der Bundesrätin **Deutsch** [NEOS/W].)*

13.50

Präsident Peter Samt: Als Nächster zu Wort gemeldet ist Bundesrat Christoph Stillebacher. Ich erteile es ihm.

RN/65

13.50

Bundesrat Christoph Stillebacher (ÖVP, Tirol): Sehr geehrter Herr Präsident! Sehr geehrter Herr Staatssekretär! Hohes Haus! Werte Kolleginnen und Kollegen! Liebe Zuseherinnen und Zuseher zu Hause! Der Herr Staatssekretär und meine Kollegen im Bundesrat, die Vorredner, haben bereits dargelegt, wie dieses Gesetz technisch ausgestaltet ist, und haben es auch schon ausführlich erklärt.

Ich möchte meine Rede daher nutzen, um über das Warum und über die Verantwortung, die wir heute hier für die Bundesländer und für unseren Wirtschaftsstandort übernehmen, zu sprechen. Wir haben im Nationalrat eine bemerkenswerte Einigkeit mit einer Ausnahme, die wir heute schon zweimal gehört haben. Die Ausnahme ist, wie wir es mittlerweile schon gewohnt sind, die Freiheitliche Partei. Was haben wir gesehen? – Die ÖVP, die SPÖ, die NEOS und die Grünen haben für diesen Gesetzentwurf gestimmt. *(Zwischenruf des Bundesrates **Bernard** [FPÖ/NÖ].)* Warum? – Weil Sicherheit in einer digitalen Welt keine Frage der Parteifarbe, sondern eine Überlebensfrage für unsere kritische Infrastruktur ist. *(Beifall bei ÖVP und SPÖ sowie der Bundesrätin **Deutsch** [NEOS/W]. – Zwischenruf der Bundesrätin **Steiner-Wieser** [FPÖ/Sbg.].)*

Wir haben es heute schon gehört, es kam auch in den Debatten im Nationalrat schon öfter: Es wurde immer wieder das Bild eines Bürokratiemonsters an die Wand gemalt. Es wird behauptet, wir würden die österreichische Wirtschaft quälen. – Lassen Sie mich dem hier ganz entschieden widersprechen: Die Bedrohungslage hat sich massiv geändert. Wir sprechen nicht mehr von Hobbyhackern im Keller, wir sprechen von hybriden Angriffen, von staatlich gesteuerten Akteuren und von organisierter Kriminalität. *(Beifall bei ÖVP und SPÖ sowie der Bundesrätin **Deutsch** [NEOS/W].)*

Diese Angriffe sind, wie wir wissen, leise, sie hinterlassen keine aufgebrochenen Türen, aber sie können unsere Energieversorgung, unsere Krankenhäuser und unser gesamtes gesellschaftliches Leben lahmlegen. Wer heute behauptet, Sicherheitsstandards seien eine reine Belastung für die Wirtschaft, der verkennt die Realität. Ein erfolgreicher Cyberangriff kostet ein Unternehmen ein Vielfaches dessen, was Prävention kostet. Datendiebstahl, Produktionsausfälle, Vertrauensverlust sind die wahren Gefahren für unsere 4 000 betroffenen Unternehmen und ihre Lieferketten.

Dieses Gesetz ist daher kein Zwangskorsett, sondern eine Schutzweste für den Wirtschaftsstandort Österreich. Ja, wir nehmen die Sorgen der Wirtschaft ernst, und deshalb gilt bei der Umsetzung ganz klar der Grundsatz: beraten statt strafen. Die neue Cybersicherheitsbehörde ist nicht dazu da, um sofort Bußgelder zu verteilen, sie ist da, um Unternehmen bei der Risikoanalyse zu unterstützen und Bewusstsein zu schaffen.

Wir haben auch aus der Diskussion der Vergangenheit gelernt und das Gesetz entscheidend verbessert, was ja auch zur Zustimmung der anderen Fraktionen geführt hat. Wir haben die bestehenden Zertifizierungen anerkannt, um Doppelgleisigkeiten zu vermeiden, wir haben Berichtspflichten praxistauglicher gestaltet und wir haben die Unabhängigkeit der Behörde gesichert; sie ist zwar im Innenministerium angesiedelt, dort aber ganz klar von der Generaldirektion für die öffentliche Sicherheit getrennt. Der Vorwurf, es würde eine Überwachungsbehörde geschaffen oder Vermischung mit polizeilichen Aufgaben stattfinden, ist schlichtweg falsch und dient nur zur Verunsicherung. *(Bundesrätin **Jäckel** [FPÖ/Vbg.]: Hat keiner gesagt! Das stimmt ja nicht!)* Es geht um Resilienz und nicht um Repression.

Meine Damen und Herren, wir sind hier im Bundesrat, der Länderkammer. Denken Sie an die Landeskrankenhäuser, an die regionalen Energieversorger in Ihren Bundesländern! Das ist das Nervensystem unserer Republik, und wenn dort das Licht ausgeht oder Patientendaten verschlüsselt werden, hilft uns keine Polemik weiter, dann helfen nur robuste, geübte Sicherheitsstrukturen – und genau diese schaffen wir heute. *(Beifall bei ÖVP und SPÖ sowie der Bundesrätin **Deutsch** [NEOS/W].)*

Wir setzen europäisches Recht um, aber wir tun es mit Augenmaß, und wir sorgen dafür, dass Österreich kein weiches Ziel für Cyberkriminelle ist. Ich bitte Sie daher: Lassen Sie uns den nationalen Schulterschluss für Cybersicherheit,

den wir im Nationalrat gesehen haben, auch hier im Bundesrat vollziehen! Stimmen Sie im Sinne der Sicherheit unserer Wirtschaft und zum Schutz der Menschen in unseren Bundesländern diesem Gesetzentwurf zu. *(Beifall bei ÖVP und SPÖ sowie der Bundesrätin **Deutsch** [NEOS/W].)*

Da das heute normalerweise meine letzte Rede im heurigen Jahr sein wird, möchte ich noch die Gelegenheit nutzen und Ihnen allen, euch allen eine frohe und besinnliche Weihnachtszeit, einen guten Rutsch und gute Erholung wünschen. Ich freue mich auf ein Wiedersehen im nächsten Jahr! – Vielen Dank. *(Beifall bei ÖVP und SPÖ sowie der Bundesrätin **Deutsch** [NEOS/W], der Bundesrätin **Kittl** [Grüne/W] und des Bundesrates **Kober** [FPÖ/Stmk.].)*

13.55

Präsident Peter Samt: Eine weitere Wortmeldung liegt mir dazu nicht vor.

Wünscht noch jemand das Wort? – Das ist nicht der Fall. Die Debatte ist geschlossen.

RN/66

Abstimmung

Präsident Peter Samt: Wir gelangen zur Abstimmung. – Bitte nehmen Sie Ihre Plätze ein.

Dieser Beschluss ist ein Fall des Art. 44 Abs. 2 Bundes-Verfassungsgesetz und bedarf daher der in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von mindestens zwei Dritteln der abgegebenen Stimmen zu erteilenden Zustimmung des Bundesrates.

Ich stelle zunächst die für die Abstimmung erforderliche Anwesenheit der Mitglieder des Bundesrates fest. – Diese ist gegeben.

Wir gelangen zunächst zur Abstimmung, gegen den vorliegenden Beschluss des Nationalrates keinen Einspruch zu erheben.

Ich ersuche jene Bundesrätinnen und Bundesräte, die dem Antrag zustimmen, gegen den vorliegenden Beschluss des Nationalrates keinen Einspruch zu erheben, um ein Handzeichen. – Das ist die **Stimmenmehrheit.** Der Antrag, keinen Einspruch zu erheben, ist somit **angenommen.**

Nunmehr lasse ich über den Antrag abstimmen, dem vorliegenden Beschluss des Nationalrates gemäß Art. 44 Abs. 2 Bundes-Verfassungsgesetz die verfassungsmäßige Zustimmung zu erteilen.

Ich bitte jene Bundesräte und Bundesrätinnen, die diesem Antrag zustimmen, um ein Handzeichen. – Das ist die **Stimmenmehrheit.** Der gegenständliche Antrag ist somit unter Berücksichtigung der besonderen Beschlusserfordernisse **angenommen.**

Ausdrücklich stelle ich die verfassungsmäßig erforderliche Zweidrittelmehrheit fest.