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.