

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 irgendwem 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 unserer aller digitalen 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.*)

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