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.