RN/144

14. Punkt

Bericht des Ausschusses für innere Angelegenheiten über den Antrag 655/A(E) der Abgeordneten Süleyman Zorba, Kolleginnen und Kollegen betreffend Ethical Hacking straffrei stellen – Proaktives Aufdecken von Sicherheitslücken mit dem Ziel der Erhöhung der Cybersicherheit (377 d.B.)

Präsident Peter Haubner: Wir gelangen nun zum 14. Punkt der Tagesordnung.

Auf eine mündliche Berichterstattung wurde verzichtet.

Als Erster zu Wort gemeldet ist Herr Abgeordneter Michael Schilchegger. Ich stelle seine Redezeit auf 3 Minuten ein. – Bitte, Herr Abgeordneter.

RN/145

18.27

Abgeordneter MMag. Dr. Michael Schilchegger (FPÖ): Sehr geehrter Herr Präsident! Sehr geehrte Damen und Herren! Wir sprechen hier über diesen Antrag der Grünen zum proaktiven Aufdecken von Sicherheitslücken mit dem Ziel der Erhöhung der Cybersicherheit. Inhaltlich geht es offenbar um die Vorstellung, dass Hacker natürlich auch einmal einen positiven Zweck erfüllen können, also es müssen nicht nur Kriminelle sein, sondern es gibt auch sozusagen die Situation, dass Hacker Probeangriffe oder was auch immer durchführen, um die Sicherheitslücken in Unternehmen aufzudecken und diese so für die Unternehmen, für die Behörden kenntlich zu machen, damit diese dann geschlossen werden können.

Aus unserer Sicht wird auch da der Fall beschrieben, dass das natürlich in Abstimmung und mit Zustimmung der betroffenen Unternehmen passiert, die

das sozusagen beauftragen oder zumindest damit einverstanden sind. Das ist aus unserer Sicht auch der einzige zulässige Fall. Dieser Antrag möchte aber darüber hinaus auch weitere Hackerangriffe – ich sage es einmal salopp – legalisieren und ein Konzept dafür entwickeln, wie solche Angriffe möglich werden sollen.

Wir stehen einer Diskussion darüber grundsätzlich aufgeschlossen gegenüber. Wir können diesem Antrag heute hier aber nicht zustimmen, weil wir der Meinung sind, dass dieser Antrag, so wie er jetzt formuliert ist, einfach zu Missbrauch einlädt, auch zu einer vollkommen unkontrollierten Verbreitung von personenbezogenen Daten – alles womöglich auch an den Behörden vorbei.

Das heißt, aus unserer Sicht wäre es schön gewesen, dieses Konzept, so wie es unser Vorschlag war, auch noch einmal im Ausschuss mit Experten zu diskutieren. Es ist schade, dass das nicht gelungen ist. Das alles ist die Erklärung dafür, warum wir Freiheitliche hier nicht zustimmen. *(Beifall bei der FPÖ.)*

18.28

Präsident Peter Haubner: Als Nächster zu Wort ist Herr Abgeordneter Thomas Elian. Freiwillige Redezeitbeschränkung: 3 Minuten. – Bitte Herr Abgeordneter.

RN/146

18.29

Abgeordneter Ing. Thomas Elian (ÖVP): Sehr geehrter Herr Präsident! Herr Staatssekretär! Geschätzte Kolleginnen und Kollegen! Werte Zuseher! Wir beraten heute einen Entschließungsantrag, der ein hochaktuelles Thema, die digitale Transformation, und zugleich eine zentrale Standortfrage für Österreich berührt: den rechtlichen Umgang mit Ethical Hacking.

Gemeint ist damit das verantwortungsvolle Testen von IT-Systemen, um Sicherheitslücken frühzeitig zu erkennen, bevor sie von kriminellen Akteuren

ausgenutzt werden können. In einer zunehmend digitalisierten Wirtschaft ist das kein Randthema mehr, sondern ein wesentlicher Faktor für Vertrauen, Stabilität und Wettbewerbsfähigkeit. Derzeit ist die Rechtslage nicht in allen Bereichen eindeutig geregelt: Während beauftragte Sicherheitstests klar geregelt sind, besteht beim proaktiven Aufdecken von Sicherheitslücken und Schwachstellen ohne ausdrücklichen Auftrag rechtliche Unsicherheit. Das führt oft dazu, dass vorhandenes Know-how nicht ausgeschöpft und potenzielle Sicherheitslücken dadurch unentdeckt bleiben. Gerade aus Sicht der Standortpolitik ist dies problematisch. Österreich braucht Rahmenbedingungen, die Innovationen ermöglichen und Fachkräfte ermutigen, ihr Wissen verantwortungsvoll einzubringen.

Der Entschließungsantrag setzt genau da an. Er fordert klare, praxisorientierte Leitlinien, die auf eine sorgfältige Überprüfung der bestehenden straf- und datenschutzrechtlichen Bestimmungen abzielen. Ein moderner Rechtsstaat braucht klare Regeln, gerade im digitalen Raum. Unternehmen, Forschungseinrichtungen und öffentliche Stellen müssen sich darauf verlassen können, dass verantwortungsvolles Handeln nicht zum rechtlichen Risiko wird. Gleichzeitig muss klar sein, wo die Grenzen liegen.

Für uns stehen dabei drei Aspekte im Vordergrund. Erstens: Sicherheit durch Klarheit. Wer in guter Absicht unsere IT-Systeme testen möchte und zur Sicherheit etwas beitragen will, braucht klare, verlässliche rechtliche Leitlinien.

Zweitens, rechtsstaatliche Verlässlichkeit: Rechtssicherheit darf keine pauschale Straffreiheit bedeuten, sondern muss an klare und überprüfbare Voraussetzungen geknüpft sein.

Drittens, Stärkung des Standorts Österreich: Klare Regeln für Ethical Hacking erhöhen das Vertrauen in unsere digitalen Systeme und machen Österreich als Standort für IT-Sicherheit und digitale Forschung attraktiver.

Missbrauchsgefahren und datenschutzrechtliche Risiken sind dabei selbstverständlich ernst zu nehmen. Gerade deshalb geht es nicht darum, bestehende Grenzen aufzuweichen, sondern sie so weiterzuentwickeln, dass legitimes, verantwortungsvolles Handeln geschützt bleibt und rechtswidriges Verhalten weiterhin konsequent sanktioniert wird.

Meine geschätzten Damen und Herren! Rechtssicherheit ist kein Selbstzweck, sondern ein Grundpfeiler unseres Rechtsstaats, auch im Cyberraum. Wenn wir da vorausschauend handeln, stärken wir Sicherheit, Innovation und Vertrauen gleichermaßen. Lassen Sie uns daher gemeinsam klare Spielregeln schaffen und einen sachlichen Beitrag zur Stärkung der Cybersicherheit in Österreich leisten. – Vielen Dank. *(Beifall bei der ÖVP sowie des Abg.* ***Zorba*** *[Grüne].)*

18.32

Präsident Peter Haubner: Als Nächste zu Wort gemeldet ist Frau Abgeordnete Sabine Schatz. – Ich stelle Ihre Redezeit auf 3 Minuten ein, Frau Abgeordnete.

RN/147

18.32

Abgeordnete Sabine Schatz (SPÖ): Danke, Herr Präsident! Herr Staatssekretär! Sehr geehrte Damen und Herren! Ja, ich glaube, wir sind uns einig: Cybersicherheit ist mittlerweile ein wesentlicher Bestandteil im gesamten Aufgabenkomplex der inneren Sicherheit. Der Schutz der Bürger und Bürgerinnen, der kritischen Infrastruktur, genauso wie öffentlicher Einrichtungen, der Wirtschaft, der Forschung, der Kultur – all das muss auch im digitalen Raum gewährleistet sein.

Wenn es zu Sicherheitslücken kommt, kann das fatale Folgen haben: etwa das Absaugen von relevanten personenbezogenen Daten, genauso wie wirtschaftlicher und sicherheitspolitischer Daten und Informationen oder eben

auch das Lahmlegen ganzer Betriebssysteme mit enormen datenschutzrechtlichen, mit enormen wirtschaftlichen und mit enormen systemrelevanten Folgen.

Die Studie zu Cybersecurity in Österreich 2025 zeigt klar auf: Österreich ist nicht nur betroffen, sondern auch extrem verwundbar. Jeder siebte Cyberangriff in Österreich ist erfolgreich. Das zeigt in Wahrheit den Handlungsbedarf hinsichtlich Prävention in diesem Kontext noch einmal klar auf.

Unter Ethical Hacking versteht man das gezielte Testen von IT-Systemen auf ihre Verwundbarkeit. Sicherheitslücken sollen aufgedeckt werden, bevor sie durch Kriminelle missbraucht und ausgenutzt werden. Deswegen beauftragen auch viele Institutionen und Unternehmen Experten und Expertinnen, um Sicherheitslücken im IT-System zu testen. Wenn wir von Ethical Hacking sprechen, dann meinen wir ausdrücklich nicht Cyberkriminalität, sondern die Absicht, Schäden in der digitalen Infrastruktur zu vermeiden, bevor diese überhaupt entstehen.

Mit dem vorliegenden Antrag sollen nun jene rechtlichen Grauzonen evaluiert werden, wenn es um Ethical Hacking hinsichtlich Sicherheitslücken ohne einen konkreten Auftrag geht; da gibt es keine entsprechenden Absicherungen. Das heißt konkret: Wenn IT-Experten und Expertinnen Systeme von sich aus überprüfen, ausschließlich mit der Absicht, auf Sicherheitslücken aufmerksam zu machen, ist das aktuell ein rechtlicher Graubereich, und obwohl positive Absicht besteht, ist das auch strafrechtlich relevant und mit Folgen verbunden.

Sehr geehrte Damen und Herren! Ich glaube, wir sind uns einig: Digitale Sicherheit ist kein Luxus, sondern eine Voraussetzung für unseren funktionierenden Staat, für unsere Wirtschaft, für sichere Arbeitsplätze. Deswegen ist es auch wichtig, dass wir eine Evaluierung und einen Leitfaden für

Ethical Hacking auf den Weg bringen. Um nicht mehr und nicht weniger geht es bei dem vorliegenden Antrag. – Vielen Dank. *(Beifall bei der SPÖ.)*

18.35

Präsident Peter Haubner: Als Nächster zu Wort gemeldet ist Abgeordneter Süleyman Zorba. – Ich stelle Ihre Redezeit auf 4 Minuten ein, Herr Abgeordneter.

RN/148

18.36

Abgeordneter Süleyman Zorba (Grüne): Danke, Herr Präsident! Geschätzte Kolleginnen und Kollegen! Werte Zuseherinnen und Zuseher! Herr Staatssekretär! Wir haben uns ja heute schon länger mit Sicherheitslücken beschäftigt. Jetzt schauen wir uns das Ganze von der anderen Seite an: nämlich Menschen, die Sicherheitslücken finden und sie melden, damit sie geschlossen werden – ein bisschen anders als Jörg Leichtfried. *(Heiterkeit und Beifall bei den Grünen.)*

Solche Menschen gibt es. Man stelle sich vor – ich versuche das jetzt ein bisschen von der digitalen Welt in die analoge rüberzubringen –, Sie gehen an einem Haus vorbei, sehen, dass eine Hintertür offen ist, läuten an und sagen: Hey bitte, deine Tür ist offen, das Fenster ist offen, mach es bitte zu! – Was in der analogen Welt jetzt nichts Absurdes und auch kein rechtlicher Graubereich wäre, ist im digitalen Raum nicht ganz unumstritten.

Es kommt aber vor, dass ethisch korrekt handelnde Sicherheitsexperten solche Sicherheitslücken melden. Als Beispiel: Der Chaos Computer Club hat so ein massives Datenleck bei Volkswagen entdeckt, da waren Standortdaten von über 800 000 Autos frei zugänglich. Sie haben das gemeldet, der Fehler konnte behoben werden. Selbiges bei der Hotelkette Numa, da waren es Gästedaten,

oder bei Meditec sensible Gesundheitsinformationen. Es gibt also Sicherheitsexpertinnen und -experten, die, wenn sie Lücken oder Fehler in Systemen finden, diese melden. Diese Menschen leisten einen Dienst an der Allgemeinheit und verhindern Schaden.

Jetzt kommt das Absurde: Oft bewegen sie sich dabei in einem rechtlichen Graubereich, und es ist nicht ganz ausgeschlossen, dass sie dafür auch strafrechtlich belangt werden. Die gute Absicht so konkret darzustellen, ist auch immer schwer, und da braucht es Leitlinien, deshalb habe ich auch den Antrag gestellt, dem im Ausschuss von einer breiten Mehrheit zugestimmt wurde – bis auf die Kollegen von der FPÖ; aber vielleicht schaffen wir es ja jetzt, Herr Kollege.

Ich habe ja nichts dagegen, wenn wir das nochmals mit Expertinnen und Experten durcharbeiten, aber wie auch im Ausschuss schon gesagt: Der Antrag selber fordert keine konkreten Gesetzesänderungen, sondern zum einen, dass das Innenministerium eine Leitlinie ausarbeiten soll – denn dort gibt es viele Menschen, die sich damit beschäftigen –, und auf der anderen Seite, dass das Justizministerium die gesetzlichen Bestimmungen, die datenschutzrechtlichen Regelungen überprüfen soll und, wenn es dort Änderungen benötigt, man diese auch nachzieht. Wir wissen ja, was die ehemalige Justizministerin Zadić in diesem Bereich aus dem Justizministerium heraus schon Positives geleistet hat, aber vielleicht können wir das ja in eine gesetzliche Situation bringen, wo dann der Graubereich wirklich komplett aufgehoben ist. *(Beifall bei den Grünen.)*

Cybersicherheit ist kein Nischenthema und Sicherheitslücken verschwinden nicht von selber. Am besten werden sie geschlossen, bevor der Staatstrojaner sie missbraucht. Ich hoffe auf breite Zustimmung. Vielleicht geht es ja doch in

letzter Sekunde, dass man sich einen Ruck gibt. – Danke schön. *(Beifall bei den Grünen.)*

18.39

Präsident Peter Haubner: Als Nächste zu Wort gemeldet ist Frau Abgeordnete Margreth Falkner. – Ich stelle Ihre Redezeit auf 3 Minuten ein, Frau Abgeordnete.

RN/149

18.39

Abgeordnete Margreth Falkner (ÖVP): Vielen Dank, Herr Präsident! Geschätzter Herr Staatssekretär! Kolleginnen und Kollegen! Wir leben in einer digitalen Welt, in der Sicherheit längst nicht mehr nur eine Frage von Schlössern und Mauern ist.

Unsere kritischste Infrastruktur liegt heute in Serverräumen, in Datenleitungen, auf Clouds oder auch in unseren Hosentaschen. Wir sind heute stärker denn je von funktionierender Cybersicherheit abhängig. Der Antrag zum Thema Ethical Hacking greift daher ein sehr zentrales Zukunftsthema auf. Es ist richtig und wichtig, Sicherheitslücken frühzeitig zu erkennen – und das eben, bevor Schaden entsteht – und sie auch rechtzeitig zu schließen.

Prävention ist in jedem Fall besser als Schadensbehebung. Wenn im digitalen Raum Sicherheitslücken erst nach einem Angriff bekannt werden, dann kann man nur den Schaden begrenzen und die Krise managen. Das ist aber dann leider oft zu wenig.

Gleichzeitig sagen wir aber ganz klar: Es kann in einem Rechtsstaat keine pauschale Straffreiheit für Hacking geben. Gute Absichten allein, das darf kein Freibrief sein. Eigentumsrechte, Datenschutz und Rechtssicherheit sind keine Nebensächlichkeiten, sie sind Grundpfeiler unseres Systems. Deshalb lautet

unsere Position: Ethical Hacking ja, aber nur innerhalb eines klaren rechtsstaatlichen Rahmens. Das bedeutet: klar definierte Voraussetzungen, transparente Verfahren, keine Datenweitergabe und auch keine Veröffentlichung. Selbstverständlich müssen gefundene Sicherheitslücken an die Betroffenen gemeldet werden, sofort und verpflichtend. Nur so verhindern wir Missbrauch und stellen sicher, dass sich kriminelle Akteure nicht im Nachhinein auf angeblich ethische Motive berufen.

Der vorliegende Antrag ist für uns eine sehr gute Grundlage für eine weiterführende parlamentarische Ausarbeitung. Bei der Cybersicherheit geht es nicht um Ideologie – darf es nicht um Ideologie gehen! –, vielmehr geht es um Fragen des Standorts, der Sicherheit und auch der Wirtschaft. Oder, um es auf den Punkt zu bringen, wie es der IT-Sicherheitsexperte Bruce Schneier formuliert hat: Sicherheit ist kein Zustand, sondern Sicherheit ist ein Prozess. – Genau diesen Prozess gilt es jetzt verantwortungsvoll, klar geregelt und rechtsstaatlich sauber weiterzuentwickeln. *(Beifall bei der ÖVP sowie des Abg.* ***Zorba*** *[Grüne].)*

18.42

Präsident Peter Haubner: Als Nächster zu Wort gemeldet ist Abgeordneter Christian Oxonitsch. Ebenfalls 3 Minuten gemeldete Redezeit. – Bitte, Herr Abgeordneter.

RN/150

18.42

Abgeordneter Christian Oxonitsch (SPÖ): Danke schön, Herr Präsident! Sehr geehrter Herr Staatssekretär! Liebe Kolleginnen und Kollegen! Zum Thema Cybersicherheit und deren Bedeutung ist jetzt, glaube ich, mehr als genug gesprochen worden, es ist aber trotzdem immer wieder verwunderlich, dass selbst bei einem solchen Antrag – und es ist ja schon mehrmals gesagt worden,

worum es geht: um Evaluierung und um die Erarbeitung eines Leitfadens – die Vertreter der sogenannten Sicherheitspartei FPÖ wieder hier herauskommen und sagen, sie stimmen dem nicht zu. Ich finde das ja verwunderlich, dass es der FPÖ immer dann, wenn irgendetwas ein bisschen konkreter wird – und noch einmal: wir reden nicht über ein Gesetz, wir reden noch nicht über einen ganz konkreten Rahmen oder über Straffreiheit, sondern eigentlich nur über die Evaluierung –, einfällt, da dagegenzustimmen.

Das reiht sich ja bei dieser Sicherheitspartei neben anderen Fällen ein: Das Waffengesetz nach dem schrecklichen Attentat in Graz verschärfen? – Die FPÖ ist dagegen. Gesetzesinitiativen im Bereich internationaler Kooperationsabkommen, bei denen es um mehr Sicherheit geht, Zusammenarbeit bei Datenbanken, zum Beispiel beim Reiseinformationssystem, wodurch europäische Staaten letztendlich Daten austauschen? – Die FPÖ ist dagegen. Dass das jetzt auch bei diesem Antrag erfolgt, finde ich einfach bemerkenswert. Das festzuhalten, ist mir wichtig, und ich glaube, man sollte einmal hinterfragen, ob man tatsächlich die Sicherheitspartei ist, die zu sein man immer behauptet. – Danke schön. *(Beifall bei der SPÖ und bei Abgeordneten der ÖVP.)*

18.43

Präsident Peter Haubner: Als Nächste zu Wort gemeldet ist Frau Abgeordnete Ines Holzegger. – Ich stelle auch Ihre Zeit auf 3 Minuten ein, Frau Abgeordnete.

RN/151

18.43

Abgeordnete Ines Holzegger (NEOS): Sehr geehrter Herr Präsident! Werter Herr Staatssekretär! Hohes Haus! Sehr geehrte Zuseherinnen und Zuseher! Schwarzer Hoodie, tief ins Gesicht gezogene Kapuze, in einem Keller sitzend:

Das ist das Bild, das sicher viele im Kopf haben, wenn sie an Hacker denken. Das wird natürlich auch durch Hollywoodfilme und -serien befeuert.

Die Realität kann aber auch anders aussehen. Es gibt nicht nur die Hacker, also die Einbrecher, es gibt auch einen Schlüsseldienst, es gibt auch die, die Sicherheitslücken suchen, aber nicht, um einzubrechen, sondern um davor zu warnen und sie dann zu schließen, bevor die Einbrecher kommen. Das ist Ethical Hacking – kurz gesagt. Viele Unternehmen haben das längst als Chance verstanden. Sie zahlen Bug-Bountys – also Prämien für gefundene Fehler –, weil sie wissen, ein gestopftes Sicherheitsloch ist immer noch günstiger als ein Datenleck.

Grundsätzlich handelt es sich bei Ethical Hacking aus unserer Sicht bereits heute schon um kein strafbares Verhalten, weil eben genau dieser Vorsatz, Schaden zu verursachen, fehlt. Die Einschätzung deckt sich übrigens mit der des Justizministeriums. Das ändert aber nichts daran, dass es trotzdem im Zweifel zu Beweisschwierigkeiten oder sogar Ermittlungsverfahren kommen kann. Ich möchte nur in Erinnerung rufen: Vor einigen Jahren war ja auch das grün geführte Gesundheitsministerium dabei, zum Beispiel Epicenter Works anzuzeigen. Das geht natürlich nicht. Sicherheitslücken aufzeigen darf nicht strafbar sein und darf nicht dazu führen, dass man Angst haben muss, verfolgt zu werden. *(Beifall bei den NEOS. – Abg.* ***Gewessler*** *[Grüne] – auf Abgeordnete Zadič weisend –: Deswegen hat es die Justizministerin Zadič geändert!)*

Wer Sicherheit schafft, darf nicht wie ein Krimineller behandelt werden. Die Angst vor Anzeigen darf eben nicht größer sein als der Wille, zu helfen. Deshalb stimmen wir heute für diesen Antrag: Ein Leitfaden für Responsible Disclosure ist nämlich ein echt wichtiger Schritt für noch mehr Rechtssicherheit.

Abschließend würde ich mir persönlich auch noch gern mehr Aufmerksamkeit für genau diese Art von Positive Hacking wünschen, denn wenn es eines ist,

was wir in Österreich brauchen, dann sind es genau diese Leute. Die sind unsere digitale Feuerwehr, und wir brauchen mehr davon, besonders natürlich auch IT-Sicherheitsspezialist**innen**.

Noch ein Satz zur FPÖ, die dem Antrag ja vermutlich nicht zustimmen will: Wer die Feuerwehr nicht stärkt, hilft nur den Brandstiftern. Vielleicht überlegen Sie es sich ja noch einmal. – Vielen Dank. *(Beifall bei den NEOS sowie bei Abgeordneten von ÖVP und SPÖ.)*

18.47

Präsident Peter Haubner: Zu Wort ist dazu niemand mehr gemeldet. Die Debatte ist geschlossen.

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

RN/152

Abstimmung

Präsident Peter Haubner: Wir kommen jetzt zur Abstimmung über die dem Ausschussbericht 377 der Beilagen angeschlossene Entschließung betreffend Ethical Hacking straffrei stellen – Proaktives Aufdecken von Sicherheitslücken mit dem Ziel der Erhöhung der Cybersicherheit.

Ich bitte jene Damen und Herren, die hiefür eintreten, um ein Zeichen der Zustimmung. – Das ist die **Mehrheit, angenommen.** *(xx/E)*