377 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVIII. GP

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

Die Abgeordneten Süleyman **Zorba**, Kolleginnen und Kollegen haben den gegenständlichen Entschließungsantrag am 12. Dezember 2025 im Nationalrat eingebracht und wie folgt begründet:

„Ethical Hacking ist das gezielte und verantwortungsvolle Testen von IT-Systemen, um Sicherheitslücken aufzudecken, bevor Kriminelle sie ausnutzen können. So hat etwa der Chaos Computer Club ein riesiges Datenleck im Volkswagen-Konzern ebenso aufgedeckt wie bei der Hotelkette Numa oder auf der Reha-Plattform MediTec.

Derartiges ‚Ethical Hacking' hat in den vergangenen Jahren stetig an Bedeutung gewonnen. Immer mehr Unternehmen, Organisationen und Institutionen beauftragen ausgewiesene Expert:innen für Cybersecurity, ihre Sicherheitskonzepte möglichst praxisnah und ähnlich wie bei Hacker-Angriffen auf die Probe zu stellen. Wird die Aufdeckung von Sicherheitslücken von Betreiber:innen von Computersystemen direkt beauftragt oder wird durch eine Auslobung zur Aufdeckung von Sicherheitslücken aufgefordert, so ist bei einem damit in unmittelbarem Zusammenhang stehenden Überwinden von Sicherheitsvorkehrungen des betreffenden Computersystems von keiner Strafbarkeit auszugehen.

Problematisch ist hingegen ein anderer Bereich: Wenn Expert:innen Sicherheitslücken ohne ausdrücklichen vorangegangenen Auftrag aufdecken, befinden sie sich in einer rechtlichen Grauzone. Selbst wenn ihre Absichten nicht böswillig sind, sondern auf eine Verstärkung der Cybersicherheit abzielen, drohen strafrechtliche Ermittlungsverfahren. Diese Rechtsunsicherheit hält Expert:innen davon ab, Schwachstellen offen zu legen bzw. der betroffenen Institution Schwachstellen aufzuzeigen – zum Schaden der allgemeinen IT-Sicherheit.

Es braucht daher klare Rahmenbedingungen: Die geltenden straf- und datenschutzrechtlichen Bestimmungen müssen eine verantwortungsvolle Offen-legung von Schwachstellen (Coordinated Vulnerability Disclosure) ermöglichen und schützen. Expert:innen, die mit guter Absicht handeln und Sicherheitslücken den Verantwortlichen zur Beseitigung melden, brauchen Rechtssicherheit und Schutz vor zivil- und strafrechtlicher Verfolgung. Ein klarer gesetzlicher Leitfaden sowie eine Evaluierung und gegebenenfalls gesetzliche Klarstellungen sind notwendig, um sowohl die IT-Sicherheit zu stärken als auch um ethisch handelnde Sicherheitsforscher:innen zu schützen."

Der Ausschuss für innere Angelegenheiten hat den gegenständlichen Entschließungsantrag in seiner Sitzung am 15. Jänner 2026 in Verhandlung genommen. An der Debatte beteiligte sich außer dem Berichterstatter Abgeordneten Süleyman **Zorba** der Abgeordnete MMag. Dr. Michael **Schilchegger**.

Ein im Zuge der Debatte vom Abgeordneten MMag. Dr. Michael **Schilchegger** eingebrachter Antrag, die Verhandlungen zu vertagen, fand nicht die Zustimmung der Ausschussmehrheit (**für den Antrag:** F, **dagegen:** V, S, N, G).

Bei der Abstimmung wurde der gegenständliche Entschließungsantrag der Abgeordneten Süleyman **Zorba**, Kolleginnen und Kollegen mit Stimmenmehrheit (**für den Antrag:** V, S, N, G, **dagegen:** F) beschlossen.

Als Ergebnis seiner Beratungen stellt der Ausschuss für innere Angelegenheiten somit den **Antrag**, der Nationalrat wolle die **angeschlossene Entschließung** annehmen.

Wien, 2026 01 15

Süleyman Zorba	**Mag. Ernst Gödl**
Berichterstattung	Obman

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-01-16T09:29:40+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	