655/A(E)
vom 12.12.2025 (XXVIII. GP)

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

betreffend Ethical Hacking straffrei stellen - Proaktives Aufdecken von Sicherheitslücken mit dem Ziel der Erhöhung der Cybersicherheit

BEGRÜNDUNG

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 Offenlegung 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.

Die unterfertigenden Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

„Die Bundesregierung, insbesondere die Bundesministerin für Justiz und der Bundesminister für Inneres, wird aufgefordert,

1. einen praxisorientierten Leitfaden für das verantwortungsvolle Offenlegen von Sicherheitslücken (Coordinated Vulnerability Disclosure) zu erarbeiten, der klare Kriterien und Verfahrensweisen für ethisches Hacking definiert und sowohl Sicherheitsforscher:innen als auch betroffenen Organisationen Orientierung bietet;
2. die bestehenden straf- und datenschutzrechtlichen Bestimmungen dahingehend zu evaluieren und gegebenenfalls anzupassen, dass für ethisch handelnde Sicherheitsforscher:innen, die Schwachstellen verantwortungsvoll melden, Rechtssicherheit besteht."

In formeller Hinsicht wird die Zuweisung an den Ausschuss für innere Angelegenheiten vorgeschlagen.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-12-12T11:23:26+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	