5626/AB
vom 31.07.2026 zu 6217/J (XXVIII. GP)

bmi.gv.at

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2026-0.514.906

Wien, am 30. Juli 2026

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Rosa Ecker, MBA hat am 1. Juni 2026 unter der Nr. **6217/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Hacking-Angriffe auf Ministerien – Daten 2025“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 1:

- *Wie beurteilen Sie die aktuelle Gefahr, dass Hackerangriffe gegen ihr Ressort vorgenommen werden und gelingen könnten?*

Meinungen und Einschätzungen unterliegen nicht dem Interpellationsrecht.

Zur Frage 2:

- *Inwieweit ist Ihr Ressort auf mögliche Hackerangriffe vorbereitet?*

Das Bundesministerium für Inneres ist zur Abwehr von Hackerangriffen durch technische und organisatorische Sicherheitsmaßnahmen auf dem Stand der Technik in den Bereichen Prävention, Absicherung, Erkennung und Incident Response vorbereitet.

Zur Frage 3:

- *Gab es im Jahr 2025 sogenannte „Überlastungsangriffe“ oder andere abgewehrte Angriffe?*
  a. *Wenn ja, wann?*
  b. *Wenn ja, in welchem Umfang?*
  c. *Wenn ja, kennen Sie den Ursprung dieser Hacking-Angriffe?*

Im Jahr 2025 ereigneten sich 22 Distributed Denial-of-Service (DDoS) Attacken verteilt im Zeitraum Jänner bis Juni. Die Größenordnung bewegte sich von 220.000 Anfragen pro zwei Minuten bis hin zu 10.600.000 Anfragen pro zwei Minuten. Da diese Angriffe automatisiert über weltweit verteilte Systeme durchgeführt wurden, kann der konkrete Ursprung nicht bestimmt werden.

Zur Frage 4:

- *Wie wird seitens Ihres Ressorts aktuell für die Datensicherheit gesorgt?*

Im Bundesministerium für Inneres wird sowohl technisch als auch organisatorisch für Datensicherheit gesorgt. IKT-Sicherheit (und damit auch Datensicherheit) wird als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des Ressorts zeitnah umgesetzt.

Zur Frage 5:

- *Wer kann wie auf die von Ihnen verarbeiteten Daten aktuell zugreifen?*

Der Zugriff von durch das BMI verarbeiteten Daten erfolgt strikt nach Vorgabe der gesetzlichen Grundlagen und dort geregelten Befugnisse.

Zur Frage 6:

- *Konnten im Jahr 2025 durch Ihr Ressort Datenlecks festgestellt werden?*
  a. *Wenn ja, wie konnte es dazu kommen?*
  b. *Wenn ja, welche Daten waren betroffen?*

Es gab einen Cyberangriff gegen das E-Mail-System des Bundesministeriums für Inneres. Die für den IT-Betrieb des Bundesministeriums für Inneres zuständige Organisationseinheit erkannte Ende Juni 2025 Anzeichen von Unregelmäßigkeiten in

einem der Büro-IT-Systeme des Innenministeriums. Die eingehende Analyse ergab, dass es sich um einen gezielten und professionellen Angriff handelt. Es wurden daraufhin umgehend Maßnahmen ergriffen, um den Sicherheitsvorfall zu bereinigen.

Eine Auskunft hinsichtlich der damit zusammenhängenden Ermittlungsverfahren ist nicht möglich, da eine Offenlegung aus kriminaltaktischen Gründen unterbleiben muss.

Zur Frage 7:

- *Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
  a. *Wie hoch sind die aktuellen jährlichen Kosten hierfür (Einkauf, Installation, Wartung, Betreuung, Ausbau etc.)?*
  b. *Welche Kosten sind 2025 entstanden?*

Im Bereich des Bundesministeriums für Inneres wurden 2025 die Ausgaben für IT- und Cybersicherheit im Rahmen des IKT-Budgets abgedeckt. Eine konkrete Auskunft über die detaillierten Ausgaben für IT- und Cybersicherheit ist auf Grund schutzwürdiger Interessen der Sicherheitsbehörden nicht möglich.

Zur Frage 8:

- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

IKT-Sicherheit (und damit auch Datensicherheit) wird im Bundesministerium für Inneres als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz unter Abstützung auf entsprechende Systeme kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen. Dies betrifft sowohl die Beschaffung von dem Stand der Technik entsprechenden IKT-Sicherheitsinfrastruktur, als auch die permanente Evaluierung und Anpassung der Prozesse.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT-Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018, oder aber auch der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zur Frage 9:

- *Wer ist mit der Instandhaltung der ministeriellen Sicherheitssysteme beauftragt?*

Die Sektion IV mit der Gruppe Direktion Digitale Services (DDS).

Zur Frage 10:

- *Wie ist die derzeitige Vorgabe im Umgang mit Hacking-Angriffen?*
  - *a. Ist diese Vorgehensweise in allen Resorts einheitlich?*
  - *b. Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?*

Das NISG regelt Grundsätzliches, die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Im Bundesministerium für Inneres regeln Notfallpläne das Vorgehen im Falle von Cyberangriffen. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Bekanntgabe Abstand genommen werden.

Gerhard Karner

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2026-07-31T14:12:42+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2052038352
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-07-31T14:33:16+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	