4932/AB
vom 27.05.2026 zu 5487/J (XXVIII. GP)

bmi.gv.at

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2026-0.357.236

Wien, am 27. Mai 2026

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Süleyman Zorba, Kolleginnen und Kollegen haben am 27. März 2026 unter der Nr. **5487/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Cybersicherheitsvorfälle und -maßnahmen in den Bundesministerien“ gerichtet.

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

Zur Frage 1:

- *Gab es in Ihrem Ressort im Jahr 2025 Cyberangriffe oder Cybersicherheitsvorfälle?*
  a. *Falls ja, um wie viele Angriffe/Vorfälle hat es sich gehandelt?*
  b. *Bei wie vielen Angriffen konnten die Täter ermittelt werden? Um welche Täter handelte es sich?*

Im betreffenden Zeitraum ereigneten sich 22 Distributed Denial of Service (DDoS)-Attacken. Aufgrund der präventiven und reaktiven Sicherheitsmaßnahmen konnten die Gefährdungen abgewehrt bzw. bereinigt werden. Die Größenordnung bewegte sich von 220.000 Anfragen pro zwei Minuten bis hin zu 10.600.000 Anfragen pro zwei Minuten. Betroffen waren in diesen Fällen die Adressen „bmi.gv.at“, „polizei.gv.at“ sowie „migration.gv.at“. Wahrnehmbare Beeinträchtigungen ergaben sich hinsichtlich der eingeschränkten Erreichbarkeit von Services über das Internet.

Weiters gab es 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 2:

- *Welche Präventionsmaßnahmen wurden von Ihrem Ministerium im vergangenen Jahr ergriffen, um sich vor Cyberangriffen und -kriminalität zu schützen?*
  a. *Arbeiten Sie mit externen Expertinnen und Experten im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen?*
  b. *Wenn ja, um welche Experten handelte es sich im Jahr 2025?*
  c. *Wie erfolgte die Auswahl?*
  d. *Arbeiten Sie mit externen Unternehmen im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen? Wenn ja, mit welchen?*

Das Bundesministerium für Inneres ist zur Abwehr von Cyberattacken durch technische und organisatorische Sicherheitsmaßnahmen vorbereitet, insbesondere durch Vorkehrungen in den Bereichen Prävention, Absicherung, Erkennung und „Incident Response“.

Das Bundesministerium für Inneres steht in enger Abstimmung mit Personen aus der Wissenschaft und der Zivilgesellschaft und bedient sich deren Expertise. Im Zuge einer BBG-Ausschreibung wurde darüber hinaus eine vertiefende Zusammenarbeit mit der Firma Ikarus und deren IT-Sicherheitsexperten vereinbart. Zusätzlich werden Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess in Zusammenarbeit mit den IT-Spezialisten des Ressorts zeitnahe umgesetzt.

Zur Frage 3:

- *Gab es in Ihrem Ressort Risikoanalysen im Hinblick auf Cyberbedrohungen im Jahr 2025 und welche Ergebnisse brachten diese Analysen?*

Das kontinuierliche Risikomanagement definiert die im Bundesministerium für Inneres kritischen Prozesse und Dienste. Für diese ist ein Betriebskontinuitätsmanagement

eingerichtet. Dementsprechend werden im risikobasierten Ansatz laufend Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen.

Zusätzlich werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt.

Von der detaillierten Auflistung der Analysen und deren Ergebnissen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018 muss im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zur Frage 4:

- *Gibt es in Ihrem Ministerium Cybersicherheitsbeauftragte?*
  a. *Welche Abteilungen oder Teams waren im Jahr 2025 innerhalb Ihres Ministeriums dafür zuständig?*
  b. *Wie viele Personen waren in Ihrem Ministerium im Jahr 2025 im Bereich Cyber- und IT-Sicherheit tätig?*
  c. *Welche konkreten Aufgaben nahmen diese Personen wahr?*

Die IT- und Cybersicherheit im Bundesministerium für Inneres wird als übergreifende Querschnittsaufgabe verstanden. Die Abteilung IV/DDS/13 IT-Security arbeitet in enger Abstimmung mit der Direktion Staatsschutz- und Nachrichtendienst sowie den operativen IT-Betriebsabteilungen zusammen.

Im Bundesministerium für Inneres wurde die Funktion des Chief Information Security Officer (CISO) im Sinne eines „Cybersicherheitsbeauftragten“ eingerichtet. Der Chief Information Security Officer trägt dabei als Durchführungsverantwortlicher des Information Security Management (ISM)-Prozesses die Gesamtverantwortung für das Qualitätsmanagement der IT-Sicherheit im Ressort.

Zu seinen Aufgaben gehören die Stärkung des Bewusstseins für IT-Sicherheit im Managementbereich, die Einbringung von IT-Sicherheits-Projektanträgen, die Gewährleistung der IT-Sicherheit im laufenden Betrieb sowie die Verwaltung der für den ISM-Prozess zur Verfügung stehenden Ressourcen. Konkrete Auskünfte über die Personalsituation können hingegen auf Grund schutzwürdiger Interessen der Sicherheitsbehörden nicht mitgeteilt werden.

Zur Frage 5:

- *Wie hoch war das Budget Ihres Hauses für IT- und Cybersicherheit im Jahr 2025?*

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 6:

- *Gab es im Jahr 2025 konkrete verpflichtende Schulungsangebote in Fragen der IT- und Cybersicherheit für Mitarbeiter:innen Ihres Hauses sowie nachgeordneter Dienststellen?*
  a. *Wenn ja, um welche Schulungsangebote handelte es sich?*
  b. *Wie hoch waren die Kosten für diese Schulungen?*

Ja, es gab verpflichtende Schulungsangebote in Fragen der IT- und Cybersicherheit für Mitarbeiterinnen und Mitarbeiter.

Das Angebot umfasst sowohl verpflichtende Basismodule als auch freiwillige Vertiefungen in Schwerpunktthemen und wurde in Zusammenarbeit mit der Sicherheitsakademie von der Abteilung IV/DDS/13 IT-Security im Rahmen des Sicherheitsmanagements erarbeitet.

- Cybersicherheit
- Deepfakes
- Handlungssicherheit im Umgang mit IT
- Handlungssicher im digitalen Raum
- IT-Sicherheit (im Rahmen der ICDL Online Schulungen)
- Cybersecurity im Umgang mit IKT-Infrastruktur
- Kontrolle zur Abwehr von Schäden an der IKT-Infrastruktur
- Einhaltung von IT-Sicherheitsrichtlinien

Da die Schulungen intern über den e-Campus bereitgestellt wurden, fielen keine externen Kosten an. Es entstanden lediglich interne Personalkosten für die Entwicklung und Durchführung.

Gerhard Karner

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2026-05-27T16:12:45+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	2026-05-28T08:18:11+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	