859/AB
vom 27.05.2025 zu 861/J (XXVIII. GP)

bmi.gv.at

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.337.802

Wien, am 26. Mai 2025

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 27. März 2025 unter der Nr. **861/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Mögliche Hackerangriffe auf Ihr Ministerium“ gerichtet.

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

Zur Frage 1:

- *Besteht aktuell die Gefahr, dass Hackerangriffe gegen Ihr Ministerium vorgenommen werden und gelingen könnten?*
  a. Wenn ja, wie sind Sie aktuell auf so einen Fall vorbereitet?

Angriffsversuche und Angriffe selbst können nie ausgeschlossen werden. Das Bundesministerium für Inneres ist zur Abwehr solcher Versuche durch technische und organisatorische Sicherheitsmaßnahmen auf dem Stand der Technik in den Bereichen Prävention, Absicherung, Erkennung und Incident Response vorbereitet.

Zur Frage 2:

- *Gab es im Jahr 2024 sogenannte „Überlastungsangriffe" oder andere abgewehrte Angriffe?*
  a. Wenn ja, wann?

b. Wenn ja, in welchem Umfang?

2024 gab es eine Vielzahl von Überlastungsangriffen (DDoS-Attacken), deren Auswirkungen durch eine Kombination von automatischer Mitigierung und manuellem Eingriff minimiert werden konnten. Allgemein wird festgehalten, dass DDoS-Angriffe, die eine Dauer von einigen Minuten bis Stunden aufweisen, Teil jeder Standardrisikobewertung sind.

Zur Frage 3:

- *Wie wird seitens Ihres Ministeriums aktuell für die Datensicherheit gesorgt?*
  a. Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?

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

Zur Frage 4:

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

Seitens des Bundesministeriums für Inneres konnten zuletzt keine Datenlecks festgestellt werden.

Zu den Fragen 5 und 6:

- *Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
  a. Welche Kosten entstehen für diese Systeme jährlich? (Einkauf, Installation, Wartung, Betreuung, Ausbau etc)
  b. Welche Kosten sind 2023 und 2024 entstanden?
- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Im Bundesministerium für Inneres werden basierend auf erfolgten Risikobewertungen und Bedrohungsanalysen unterschiedliche Sicherheitssysteme zum Einsatz gebracht. Neben technischen Maßnahmen zum Update und Upgrade bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung auf zum Einsatz zu bringende Sicherheitssysteme hin.

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 im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zur Frage 7:

- *Wie ist die vorgeschriebene Vorgehensweise, wenn so ein Hackingangriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*
  a. *Ist diese Vorgehensweise in allen Ministerien 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

	Datum/Zeit	2025-05-27T15:08:49+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.	148769640
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	2025-05-27T15:13:00+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	