825/AB
vom 27.05.2025 zu 870/J (XXVIII. GP)

Bundesministerium
Innovation, Mobilität
und Infrastruktur

bmimi.gv.at

Peter Hanke
Bundesminister

ministerbuero@bmimi.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsident des Nationalrates
Dr. Walter Rosenkranz

Parlament
1017 W i e n

Geschäftszahl: 2025-0.239.264

. Mai 2025

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Rosa Ecker und weitere Abgeordnete haben am 27. März 2025 unter der **Nr. 870/J** eine schriftliche parlamentarische Anfrage betreffend Mögliche Hackerangriffe auf Ihr Ministerium an mich gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu 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 BMIMI ist zur Abwehr solcher Versuche durch technische und organisatorische Sicherheitsmaßnehmen auf dem Stand der Technik in den Bereichen Prävention, Absicherung, Erkennung und Incident Response vorbereitet und setzt mehrere spezifische Sicherheitsvorkehrungen zum Schutz der IKT-Systeme des Ressorts ein, um die IKT-Sicherheitsrisiken zu minimieren. Ich ersuche aber um Verständnis, dass es im Hinblick auf die Effektivität dieser Maßnahmen nicht möglich ist, die Sicherheitsvorkehrungen im Detail öffentlich mitzuteilen.

Zu Frage 2:

- *Gab es im Jahr 2024 sogenannte „Überlastungsangriffe“ oder andere abgewehrte Angriffe?*
  - *a. Wenn ja, wann?*
  - *b. Wenn ja, in welchem Umfang?*

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Darunter auch Überlastungsangriffe (DDoS), welche durch die IKT-Sicherheitssysteme ebenso weitgehend automatisiert abgewehrt

werden. Allgemein wird festgehalten, dass DDoS Angriffe, die eine Dauer von einigen Minuten bis Stunden aufweisen, als alltäglich angesehen werden müssen und Teil jeder Standardrisikobewertung sind.
Ein spezieller Überlastungsangriff auf die im Ressort betriebenen Computersysteme, der Schaden verursacht hätte, wurde nicht beobachtet.

Zu den Fragen 3 und 6:

- *Wie wird seitens Ihres Ministeriums aktuell für die Datensicherheit gesorgt?*
    a. *Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?*
- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Im BMIMI 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. Zugriffsberechtigungen erfolgen nach dem Bedarfsprinzip unter Berücksichtigung der Sensibilität der Daten.

Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des Ressorts zeitnahe umgesetzt. Dies betrifft sowohl die Beschaffung von State-of-the-Art IKT-Sicherheitsinfrastruktur, als auch die permanente Evaluierung und Anpassung der Prozesse. Darüber hinaus muss von der detaillierten Auflistung der IKT-Sicherheitsmaßnahmen und auch von der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu 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 BMIMI konnten zuletzt keine Datenlecks festgestellt werden.

Zu Frage 5:

- *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?*

Im BMIMI werden basierend auf erfolgten Risikobewertungen und Bedrohungsanalysen unterschiedliche Sicherheitssysteme zum Einsatz gebracht. Im Hinblick auf die Sicherung der Effektivität dieser Schutzmaßnahmen muss von einer detaillierten Bekanntgabe Abstand genommen werden.

Zu 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 BMIMI werden verschiedene Aspekte der IKT-Sicherheitsmaßnahmen regelmäßig geübt und geprüft. Es wird aber um Verständnis ersucht, dass die Details zu den Übungen und Überprüfungen nicht öffentlich bekannt gegeben werden können.

Mit freundlichen Grüßen

Peter Hanke

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNOVATION, MOBILITÄT UND INFRASTRUKTUR @ AMTSSIGNATUR	Hinweis	Dieses Dokument wurde amtssigniert.
	Datum	2025-05-27T13:55:18+02:00
	Seriennummer	2069212815
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-05-27T14:13:30+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	