517/AB
vom 25.04.2025 zu 528/J (XXVIII. GP)

bmi.gv.at

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.251.420

Wien, am 11. April 2025

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Michael Schnedlitz hat am 26. Februar 2025 unter der Nr. **528/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberangriffe auf österreichische Ministerien gerichtet.

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

Zur Frage 1:

- *Gab es in Ihrem Ressort Cyberangriffe seit dem Jahr 2022?*
  a. *Falls ja, bitte um detaillierte Schilderung des Angriffs bzw. der Angriffe und der daraus resultierenden „Schäden".*

Im betreffenden Zeitraum ereigneten sich 41 Distributed Denial of Service (DDoS)-Attacken. Aufgrund der präventiven und reaktiven Sicherheitsmaßnahmen konnten in keinem Fall Gefährdungen festgestellt werden. Wahrnehmbare Beeinträchtigungen ergaben sich hinsichtlich der Erreichbarkeit von Services über das Internet. Die Größenordnung bewegte sich von 119.000 Anfragen pro zwei Minuten bis hin zu 3.030.000 Anfragen pro zwei Minuten. Betroffen waren in diesen Fällen die Adressen „bmi.gv.at“, „polizei.gv.at“ sowie „migration.gv.at“.

Zur Frage 2:

- *Gibt es konkrete Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?*

Von der Auflistung von konkreten Plänen muss in Hinblick auf die Sicherung der Maßnahmen Abstand genommen werden. Die konkrete Vorbereitung ist stark von der zu schützenden Infrastruktur und den zu schützenden Services, als auch dem ausgesetzten Risiko abhängig.

Zur Frage 3:

- *Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?*

Auf die Beantwortung der Frage 2 der Anfrage 12157/J XXVII. GP der Abgeordneten Katharina Kucharowits, Genossinnen und Genossen vom 14. September 2024 (11874/AB XXVII. GP) darf verwiesen werden.

Zur Frage 4:

- *Welche konkreten Maßnahmen werden aktiv von Ihrem Ministerium ergriffen, um sich präventiv gegen Cyberattacken und gegen Cyberkriminalität zu schützen?*

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

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 Abstand genommen werden.

Zur Frage 5:

- *Welche Rolle spielen externe Experten in der Vorbereitung und im Schutz gegen potenzielle Cyberangriffe?*
  a. *Welche Art von Experten wird hier beigezogen und warum?*

Das Bundesministerium für Inneres steht in enger Abstimmung mit Personen aus der Wissenschaft und der Zivilgesellschaft und bedient sich deren Expertise. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den IT-Spezialisten des Ressorts zeitnahe umgesetzt.

Zu den Fragen 6 und 7:

- *Gab es in Ihrem Ressort eigene Risikoanalysen?*
  a. *Falls ja, welche?*
  b. *Falls nein, warum nicht?*
- *Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ministeriums gerecht zu werden?*

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.

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 8:

- *Gibt es so etwas wie „Cybersicherheitsbeauftragte" in Ihrem Ministerium?*
  a. *Wenn ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dafür vorgesehen?*
  b. *Wenn ja, über welche Expertise verfügt diese Person/ verfügen diese Personen?*
  c. *Wenn ja, was sind die konkreten Aufgaben dieser Person/Personen?*
  d. *Wenn nein, warum nicht?*

Im Bundesministerium für Inneres wurde die Funktion des Chief Information Security Officer (CISO) eingerichtet. Der Chief Information Security Officer trägt 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.

Der CISO und seine Mitarbeiter verfügen jeweils über ein abgeschlossenes Hochschulmasterstudium mit Fokus IT-Security und eine langjährige Berufserfahrung im Bereich IKT-Sicherheit.

Darüber hinaus sorgt eine kontinuierliche berufsbegleitende Weiterbildung für das notwendige Expertenwissen, um gegen die ständig steigende Bedrohung durch Cyberangriffe entsprechend vorbereitet zu sein.

Zur Frage 9:

- *Welche Maßnahmen wurden ergriffen, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?*

Das BMI bietet eine Vielzahl an E-Learning Inhalte über den eigenen e-Campus an, die speziell auf die Bedrohungen durch Cyberangriffe und die entsprechenden Sicherheitsmaßnahmen eingehen. Diese Kurse sind für alle Bediensteten zugänglich. Die Schulungen umfassen sowohl verpflichtende Module, als auch freiwillige Vertiefungen in Schwerpunktthemen.

Zur Frage 10:

- *Welche Maßnahmen werden in Zukunft ergriffen bzw. sind geplant, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?*

Die Inhalte der persönlichen Schulungen sowie der E-Learning Angebote werden kontinuierlich aktualisiert, um den neuesten Entwicklungen und Best Practices gerecht zu werden.

Gerhard Karner

	Datum/Zeit	2025-04-25T13:39:58+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	2025-04-25T13:43:26+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	