875/AB
vom 27.05.2025 zu 863/J (XXVIII. GP)

Bundesministerium
Europäische und internationale Angelegenheiten

bmeia.gv.at

Mag.ª Beate Meinl-Reisinger, MES
Bundesministerin

Minoritenplatz 8, 1010 Wien,
Österreich

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Wien, am 27.05.2025

GZ. BMEIA-2025-0.258.492

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 27. März 2025 unter der Zl. 863/J-NR/2025 an mich eine schriftliche parlamentarische Anfrage betreffend „Mögliche Hackerangriffe auf Ihr Ministerium“ gerichtet.

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

Zu Frage 1:

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

Angriffsversuche und Angriffe selbst können nie ausgeschlossen werden. Das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) 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.

Zu Frage 2:

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

Auch 2024 gab es eine Vielzahl von Überlastungsangriffe (DDoS), 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, als alltäglich angesehen werden müssen und Teil jeder Standardrisikobewertung sind.

Zu Frage 3:

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

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

Zu Frage 4:

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

Seitens des BMEIA konnten zuletzt keine Datenlecks festgestellt werden.

Zu Frage 5:

- *Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
  Welche Kosten entstehen für diese Systeme jährlich? (Einkauf, Installation, Wartung, Betreuung, Ausbau etc)
  Welche Kosten sind 2023 und 2024 entstanden?

Im BMEIA 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 6:

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

Neben technischen Maßnahmen zum Update und Upgrade bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung auf zum Einsatz zu bringende Sicherheitssysteme hin. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Auflistung Abstand genommen werden.

Zu Frage 7:

- *Wie ist die vorgeschriebene Vorgehensweise, wenn so ein Hackingangriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*
  Ist diese Vorgehensweise in allen Ministerien einheitlich?
  Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?

Das NISG (Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018) regelt Grundsätzliches, die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Im BMEIA 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.

Mag.ª Beate Meinl-Reisinger, MES

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR EUROPÄISCHE UND INTERNATIONALE ANGELEGENHEITEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für europäische und internationale Angelegenheiten
	Datum/Zeit	2025-05-27T16:42:10+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.	2062159656
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmeia.gv.at/verifizierung	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-05-27T16:43:45+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	