5632/AB
vom 31.07.2026 zu 6209/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 31. Juli 2026

GZ. BMEIA-2026-0.505.340

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 1. Juni 2026 unter der Zl. 6209/J-NR/2026 an mich eine schriftliche parlamentarische Anfrage betreffend „Hacking-Angriffe auf Ministerien – Daten 2025“ gerichtet.

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

Zu Frage 1:

- *Wie beurteilen Sie die aktuelle Gefahr, dass Hackerangriffe gegen Ihr Ressort vorgenommen werden und gelingen könnten?*

Angriffsversuche und erfolgreiche Angriffe auf IT-Systeme können grundsätzlich nicht vollständig ausgeschlossen werden. Das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) setzt technische und organisatorische Sicherheitsmaßnahmen nach dem Stand der Technik ein, um Risiken in den Bereichen Prävention, Absicherung, Erkennung und „Incident Response“ möglichst wirksam zu reduzieren.

Zu den Fragen 2, 4, 5 und 7:

- *Inwieweit ist Ihr Ressort auf mögliche Hackerangriffe vorbereitet?*
- *Wie wird seitens Ihres Ressorts aktuell für die Datensicherheit gesorgt?*

- *Wer kann wie auf die von Ihnen verarbeiteten Daten aktuell zugreifen?*
- *Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
  Wie hoch sind die aktuellen jährlichen Kosten hierfür (Einkauf, Installation, Wartung, Betreuung, Ausbau etc.)?
  Welche Kosten sind 2025 entstanden?

lm BMEIA wird seit dem Jahr 2025 ein lnformationssicherheits-Managementsystem (ISMS) aufgebaut, welches sich am internationalen Sicherheitsstandard ISO/IEC 27001:2022 sowie der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2- Richtlinie) orientiert. Das Managementsystem sorgt unter anderem dafür, dass die diesbezüglich geltenden Rechtsvorschriften eingehalten und bestehende Risiken systematisch identifiziert, beurteilt und mittels geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik in den Bereichen Prävention, Erkennung und Reaktion reduziert werden. Es sieht darüber hinaus vor, dass die Wirksamkeit der Maßnahmen sowohl regelmäßig als auch im Anlassfall überprüft, bewertet und evaluiert wird. Dabei wird auch die Expertise externer Stellen genutzt, wie z.B. von Computer-Notfallteams im Sinne des vierten Abschnitts des NISG 2026 und von qualifizierten Stellen im Sinne des § 3 Z 11 NISG bzw. des dritten Absatzes des NISG.

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

Zu Frage 3:

- *Gab es im Jahr 2025 sogenannte „Überlastungsangriffe" oder andere abgewehrte Angriffe?*
  Wenn ja, wann?
  Wenn ja, in welchem Umfang?
  Wenn ja, kennen Sie den Ursprung dieser Hacking-Angriffe?

Auch 2025 gab es eine Vielzahl von Überlastungsangriffen (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 6:

- *Konnten im Jahr 2025 durch Ihr Ressort Datenlecks festgestellt werden?*
  Wenn ja, wie konnte es dazu kommen?
  Wenn ja, welche Daten waren betroffen?

Nach dem am 13. August 2025 aufgetretenen Verdacht eines möglichen Datenlecks hat das BMEIA umgehend umfassende technische Analysen in Zusammenarbeit mit externen Expertinnen und Experten eingeleitet. Die Untersuchungen zeigten, dass die IT-Systeme des BMEIA durchgehend sicher und zuverlässig geschützt waren. Es gab keine Hinweise auf ein Eindringen in die internen Systeme. Die vorliegenden Erkenntnisse deuten darauf hin, dass einzelne Nutzerinnen und Nutzer von BMEIA-Webseiten auf ihren persönlichen Geräten Ziel von Schadsoftware-Angriffen wurden. Die Ursache eines möglichen Datenabflusses lag daher außerhalb des IT-Systems des BMEIA.

Darüber hinaus verweise ich auf meine Beantwortung der parlamentarischen Anfrage Zl. 5483/J-NR/2026 vom 26. März 2026.

Zu Frage 8:

- *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. lm Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Auflistung Abstand genommen werden.

Zu Frage 9:

- *Wer ist mit der Instandhaltung der ministeriellen Sicherheitssysteme beauftragt?*

Ich verweise auf meine Beantwortung der parlamentarischen Anfrage Zl. 3134/J-NR/2025 vom 12. August 2025.

Zu Frage 10:

- *Wie ist die derzeitige Vorgabe im Umgang mit Hacking-Angriffen?*
  Ist diese Vorgehensweise in allen Resorts einheitlich?
  Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?

Das NISG (Netz- und lnformationssystemsicherheitsgesetz, BGBI. I Nr. 111/2018 idgF) regelt Grundsätzliches, die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. lm BMEIA regeln Notfallpläne das Vorgehen im Falle von Cyberangriffen. lm 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	2026-07-31T17:00:35+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	2026-08-03T07:43:37+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	