5623/AB
vom 31.07.2026 zu 6210/J (XXVIII. GP)

Bundesministerium
Wohnen, Kunst, Kultur,
Medien und Sport

bmwkms.gv.at

Andreas Babler, MSc
Vizekanzler
Bundesminister für Wohnen, Kunst, Kultur,
Medien und Sport

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2026-0.472.545

Wien, 27. Juli 2026

Sehr geehrter Herr Präsident,

die Abgeordnete zum Nationalrat Rosa Ecker, MBA und weitere Abgeordnete haben am 1. Juni 2026 unter der **Nr. 6210/J** 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 den Fragen 1 und 2:

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

Angriffsversuche und Angriffe selbst können nie ausgeschlossen werden. Das Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport (BMWKMS) 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 3:

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

Im Jahr 2025 erfolgten mehrere Überlastungsangriffe auf IT-Verfahren, sogenannte Distributed Denial of Service (DDoS)-Angriffe. Die Dauer dieser Angriffe betrug wenige Minuten bis mehrere Stunden.

Die Angriffe konnten aufgrund der getroffenen technischen und organisatorischen Maßnahmen erfolgreich abgewehrt werden. Der Ursprung konnte ermittelt werden und die daraus gewonnenen Erkenntnisse wurden zur weiteren Stärkung der Sicherheits- und Qualitätsprozesse genutzt.

Zu Frage 4:

- *Wie wird seitens Ihres Ressorts aktuell für die Datensicherheit gesorgt?*

Im BMWKMS wird sowohl für die technische und auch organisatorische Datensicherheit gesorgt. Hier werden insbesondere die geltenden gesetzlichen Vorgaben und Sicherheitsstandards beachtet.

Die bestehenden Sicherheitsprozesse und die IKT-Sicherheitsstruktur werden laufend überprüft. Sollte sich bei diesen Überprüfungen ein Verbesserungspotenzial herausstellen, wird dieses in Zusammenarbeit mit den Mitarbeiter:innen im Ressort und dem Bundesrechenzentrum zeitnahe umgesetzt.

Zu Frage 5:

- *Wer kann wie auf die von Ihnen verarbeiteten Daten aktuell zugreifen?*

Berechtigungen werden nach einem Bedarfsprinzip (Need-to-Do/Need to Know) unter der Berücksichtigung der Sensibilität der Daten vergeben. Die vergebenen Zugriffsberechtigung werden in regelmäßigen Abständen überprüft.

Zu Frage 6:

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

Im BMWKMS konnte zuletzt kein Datenleck festgestellt werden.

Zu Frage 7:

- *Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
    a. *Wie hoch sind die aktuellen jährlichen Kosten hierfür (Einkauf, Installation, Wartung, Betreuung, Ausbau etc.)?*
    b. *Welche Kosten sind 2025 entstanden?*

Im BMWKMS werden basierend auf erfolgten Risikobewertungen und Bedrohungsanalysen unterschiedliche interne oder auch externe Sicherheitssysteme zum Einsatz gebracht. Im Hinblick auf die Sicherung der Effektivität dieser Schutzmaßnahmen muss von einer detaillierten Auflistung Abstand genommen werden.

Zu Frage 8:

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

Ergänzend zu technischen Updates und Upgrades der bestehenden Systeme erfolgt regelmäßig eine risikobasierte Überprüfung des Bedarfs an zusätzlichen Sicherheitssystemen. Im Interesse der Aufrechterhaltung der Wirksamkeit der Schutzmaßnahmen wird von einer detaillierten Auflistung der eingesetzten Sicherheitsmaßnahmen abgesehen.

Zu Frage 9:

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

Im BMWKMS ist mit der Instandhaltung der ministeriellen Sicherheitssysteme vorwiegend der Chief Information Security Officer (CISO) betraut. Für das Management der Informationssicherheit waren im Jahr 2025 die Abteilung I/A/8 sowie das Referat I/A/8/b-IT zuständig.

Zudem wurde im Jahr 2025 eine Expert:innengruppe gegründet, die sich aus den Fachkräften im Bereich Informationssicherheit, Cybersicherheit, Datenschutz und Risikomanagement zusammensetzt.

Zu Frage 10:

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

Das Netz- und Informationssystemsicherheitsgesetz regelt Grundsätzliches; die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Bekanntgabe Abstand genommen werden.

Andreas Babler, MSc

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR WOHNEN, KUNST, KULTUR, MEDIEN UND SPORT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport
	Datum/Zeit	2026-07-31T10:19:16+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.	479679199
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-07-31T10:28:05+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	