Bundesministerium
Justiz

bmj.gv.at

Dr.in Anna Sporrer
Bundesministerin

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2026-0.472.619

Ihr Zeichen: BKA - PDion (PDion)6218/J-NR/2026

Wien, am 29. Juli 2026

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 1. Juni 2026 unter der Nr. **6218/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 den Fragen 1 bis 4:

- *1. Wie beurteilen Sie die aktuelle Gefahr, dass Hackerangriffe gegen Ihr Ressort vorgenommen werden und gelingen könnten?*
- *2. Inwieweit ist Ihr Ressort auf mögliche Hackerangriffe vorbereitet?*
- *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?*
- *4. Wie wird seitens Ihres Ressorts aktuell für die Datensicherheit gesorgt?*

Die Bundesrechenzentrum GmbH (BRZG) ist der zentrale IKT-Dienstleister des Bundesministeriums für Justiz. Die BRZG betreibt ihre Sicherheitssysteme am Stand der Technik und passt diese auch laufend an neue Entwicklungen und Bedrohungen an.

Informationssicherheit ist ein wesentlicher Grundpfeiler in der BRZG. Das eigene interne Computer Emergency Response Team (BRZ-CERT) hat die Aufgabe, Sicherheitsvorfälle durch präventive Maßnahmen zu vermeiden. Im Anlassfall werden vom BRZ-CERT die geeigneten Abwehrmaßnahmen eingeleitet und koordiniert und damit die höchste Sicherheit für die Informationen und die IT-Systeme gewährleistet.

Angriffsversuche und Angriffe können trotz aller Vorkehrungen nie ausgeschlossen werden. 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, Teil jeder Standardrisikobewertung sind und im Rahmen eines professionellen IT-Betrieb zu bewältigen sind. Darüber hinaus verfügen sowohl BRZ als auch das Bundesministerium für Justiz (BMJ) über ein Information Security Management System (ISMS), welches Verfahren und Regeln nach den Vorgaben internationaler Normen betreffend Informationssicherheit definiert und laufend evaluiert bzw. weiterentwickelt wird.

Zur Frage 5:

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

Der Zugriff auf verarbeitete Daten erfolgt ausschließlich über die dafür vorgesehenen IT-Systeme. Die Berechtigungen werden dabei strikt nach der organisatorischen Einordnung sowie den jeweiligen Zuständigkeiten der Benutzer:innen vergeben.

Zur 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?*

Seitens des Bundesministeriums für Justiz konnten keine Datenlecks festgestellt werden.

Zu den Fragen 7 bis 9:

- *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?*

- *8. In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*
- *9. Wer ist mit der Instandhaltung der ministeriellen Sicherheitssysteme beauftragt?*

Im Bundesministerium für Justiz werden zur Erhöhung der Cybersicherheit Maßnahmen auf strategischer, operativer und technischer Ebene in den Bereichen Prävention, Absicherung, Erkennung und Incident Response nach dem Stand der Technik ergriffen. Das Bundesministerium für Justiz arbeitet hier auch mit externen Expert:innen zusammen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit der Bundesrechenzentrum GmbH zeitnahe umgesetzt. 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 (NISG), oder aber auch der Auflistung einzelner im Einsatz befindlicher Cybersicherheitsprodukte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zur 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 NISG bzw. NIS2G regeln Grundsätzliches, die Ministerien regeln das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Notfallpläne regeln das Vorgehen im Falle von Cyberangriffen und werden laufend evaluiert. Im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen muss von einer detaillierten Bekanntgabe Abstand genommen werden.

Dr.in Anna Sporrer

	Datum/Zeit	2026-07-29T12:34:21+02:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.justiz.gv.at/amtssignatur

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-07-29T12:41:46+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	