Bundesministerium
Justiz
bmj.gv.at

Dr.in Anna Sporrer
Bundesministerin für Justiz

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2025-0.241.911

Ihr Zeichen: BKA - PDion (PDion)862/J-NR/2025

Wien, am 27. Mai 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 27. März 2025 unter der Nr. **862/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 den Fragen 1 bis 3:

- *1. Besteht aktuell die Gefahr, dass Hackerangriffe gegen Ihr Ministerium vorgenommen werden und gelingen könnten?*
  - *a. Wenn ja, wie sind Sie aktuell auf so einen Fall vorbereitet?*
- *2. Gab es im Jahr 2024 sogenannte „Überlastungsangriffe" oder andere abgewehrte Angriffe?*
  - *a. Wenn ja, wann?*
  - *b. Wenn ja, in welchem Umfang?*
- *3. Wie wird seitens Ihres Ministeriums aktuell für die Datensicherheit gesorgt?*
  - *a. Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?*

Die Bundesrechenzentrum GmbH (BRZG) ist der zentrale IKT-Dienstleister des Bundesministeriums für Justiz. Angriffsversuche und Angriffe auf die IT-Systeme der Justiz im BRZ können nie gänzlich ausgeschlossen werden. 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.

Das Information Security Management System (ISMS) und das Business Continuity Management System (BCMS) der BRZG (eine Aufstellung von Verfahren und Regeln nach den Vorgaben internationaler Normen betreffend die Informationssicherheit und die Verfügbarkeit von BRZ-Services) werden laufend erfolgreich auditiert.

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, Teil jeder Standardrisikobewertung sind und im Rahmen eines professionellen IT-Betrieb zu bewältigen sind.

Zur Frage 4:

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

Seitens des Bundesministeriums für Justiz konnten wurden keine Datenlecks festgestellt.

Zu den Fragen 5 und 6:

- *5. Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
  - *a. Welche Kosten entstehen für diese Systeme jährlich? (Einkauf, Installation, Wartung, Betreuung, Ausbau etc)*
  - *b. Welche Kosten sind 2023 und 2024 entstanden?*
- *6. In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Im Bundesrechenzentrum werden – basierend auf Risikobewertungen und Bedrohungsanalysen – auch für das Bundesministerium für Justiz unterschiedliche Sicherheitssysteme zum Einsatz gebracht und laufend aktualisiert.

Zur Frage 7:

- *Wie ist die vorgeschriebene Vorgehensweise, wenn so ein Hackingangriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*
  - *a. Ist diese Vorgehensweise in allen Ministerien 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 Bundeskanzleramt 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.

Dr.[in] Anna Sporrer

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2025-05-27T11:12:31+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	2025-05-27T11:19:07+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	