

**18227/AB**  
Bundesministerium vom 12.08.2024 zu 18818/J (XXVII. GP)  
[bmj.gv.at](http://bmj.gv.at)  
Justiz

Dr. <sup>in</sup> Alma Zadić, LL.M.  
Bundesministerin für Justiz

Herrn  
Mag. Wolfgang Sobotka  
Präsident des Nationalrats  
Parlament  
1017 Wien

Geschäftszahl: 2024-0.440.440

Ihr Zeichen: BKA - PDion (PDion)18818/J-NR/2024

Wien, am 12. August 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 12. Juni 2024 unter der Nr. **18818/J-NR/2024** 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 und 6:**

- *1. Besteht die Möglichkeit, dass Hackerangriffe gegen Ihr Ministerium vorgenommen werden und gelingen könnten?*
  - a. *Wenn ja, wie sind Sie auf so einen Fall vorbereitet?*
- *2. Gab es in den letzten fünf Jahren sogenannte „Überlastungsangriffe“ oder andere, abgewehrte Angriffe?*
  - a. *Wenn ja, wann?*
  - b. *Wenn ja, in welchem Umfang?*
- *3. Wie wird seitens Ihres Ministeriums für die Datensicherheit gesorgt?*
- *6. In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

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

nie ausgeschlossen werden. Die BRZG betreibt ihre Sicherheitssysteme jedoch 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.

Informationen über konkrete Angriffe liegen dem Bundesministerium für Justiz nicht vor, jedoch gebietet ein professioneller IT-Betrieb auch Vorkehrungen für diesbezügliche Szenarien vorzusehen.

**Zu den Fragen 4, 5 und 7 bis 9:**

- *4. Gibt es ein übergeordnetes Sicherheitssystem, das über alle Bundesministerien und die vorhandenen Daten wacht?*
  - a. *Wenn nein, ist zukünftig ein derartiges Sicherheitssystem geplant?*
  - b. *Wenn ja, wann soll dieses in Betrieb gehen?*
- *5. Gibt es zusätzlich ein eigenes Sicherheitssystem für Ihr Ministerium?*
- *7. Welches Gremium ist vorgesehen, wenn so ein Angriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*
- *8. Werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?*
  - a. *Wenn ja, wie oft?*
  - b. *Wenn ja, in welchem Umfang?*
  - c. *Wenn nein, warum nicht?*
- *9. Wie lange würde es voraussichtlich dauern, um ein Parallelsystem herstellen zu können, um auch weiterhin einsatzfähig zu sein?*

IKT-Sicherheit wird im Bundesministerium für Justiz als fortlaufender und umfassender Prozess im engen Zusammenwirken mit der Bundesrechenzentrum GmbH verstanden. Bezuglich der im österreichischen eGovernment eingerichteten Gremien und Maßnahmen im Zusammenhang mit Cybersicherheit wird auf die Österreichische Cybersicherheitsstrategie (ÖCSC) 2021 verwiesen, die online unter

<https://www.onlinesicherheit.gv.at/Services/Publikationen/Sicherheitsstrategien-und-Initiativen/2021-Oesterreichische-Strategie-Cybersicherheit.html> abrufbar ist.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystem-sicherheitsgesetz, BGBl. I Nr. 111/2018, oder aber auch der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Dr.<sup>in</sup> Alma Zadić, LL.M.

