6209/J XXVIII. GP

Eingelangt am 01.06.2026

ANFRAGE

der Abgeordneten Rosa Ecker, MBA
an die Bundesministerin für europäische und internationale Angelegenheiten
betreffend **Hacking-Angriffe auf Ministerien – Daten 2025**

Im Jahr 2025 wurden in Österreich 63.459 Fälle von Internetkriminalität angezeigt.[1] Unter den Begriff Cybercrime im engeren Sinne fallen Delikte, bei denen mit dem Tatmittel Internet direkte Angriffe auf Daten- und Computersysteme erfolgen. Darunter fallen zum Beispiel Hacking oder Virenangriffe, die besonders große Einrichtungen häufig erfahren müssen.[2]

Immer wieder heißt es medial, dass Cybercrime-Gruppen auch in Österreich tätig sind, wie z.B. „Die Presse“ im Februar 2024 berichtete.[3] Ein Angriff auf Ministerien, um sensible Daten zu erhalten, ist damit denkbarer denn je.

In diesem Zusammenhang richtet die unterfertigte Abgeordnete an die Bundesministerin für europäische und internationale Angelegenheiten nachstehende

Anfrage

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?
5. Wer kann wie auf die von Ihnen verarbeiteten Daten aktuell zugreifen?
6. Konnten im Jahr 2025 durch Ihr Ressort Datenlecks festgestellt werden?

---

1 https://www.bundeskriminalamt.at/501/files/kriminalpolizeiliche_anzeigenstatistik_2025_bf.pdf (aufgerufen am 05.05.2026)
2 https://de.statista.com/themen/4253/internetkriminalitaet-in-oesterreich/#topicOverview (aufgerufen am 05.05.2026)
3 https://www.diepresse.com/18193378/lockbit-die-russischen-hacker-waren-in-oesterreich-aktiv (aufgerufen am 05.05.2026)

   a. Wenn ja, wie konnte es dazu kommen?
   b. Wenn ja, welche Daten waren betroffen?
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?
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?