

Dr.ⁱⁿ Anna Sporrer
Bundesministerin

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2026-0.279.799

Ihr Zeichen: BKA - PDion (PDion)5489/J-NR/2026

Wien, am 27. Mai 2026

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Süleyman Zorba, Kolleginnen und Kollegen haben am 27. März 2026 unter der Nr. **5489/J-NR/2026** an mich eine schriftliche parlamentarische Anfrage betreffend „Cybersicherheitsvorfälle und -maßnahmen in den Bundesministerien“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 1:

- *Gab es in Ihrem Ressort im Jahr 2025 Cyberangriffe oder Cybersicherheits-Vorfälle?*
 - *a. Falls ja, um wie viele Angriffe/Vorfälle hat es sich gehandelt?*
 - *b. Bei wie vielen Angriffen konnten die Täter ermittelt werden? Um welche Täter handelte es sich?*

Das Bundesministerium für Justiz sieht sich, wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im Jahr 2025 erfolgten mehrere Überlastungsangriffe (sogenannte Distributed Denial of Service (DDoS)-Angriffe) auf IT-Verfahren in der Dauer von wenigen Minuten bis mehrere Stunden.

Im Zusammenwirken mit der Bundesrechenzentrum GmbH (dem zentralen IKT-Dienstleister der Justiz) konnten die Angriffsversuche erfolgreich abgewehrt sowie Schäden und Ausfälle hintangehalten werden. Meldungen zu Cyberangriffen werden an die zuständigen Strafverfolgungsbehörden im Bundesministerium für Inneres übermittelt. Nachdem hierbei in der Regel die Bundesrechenzentrum GmbH als anzeigende Stelle auftritt, liegen dem Bundesministerium für Justiz keine näheren Informationen vor.

Zu den Fragen 2 und 3:

- *2. Welche Präventionsmaßnahmen wurden von Ihrem Ministerium im vergangenen Jahr ergriffen, um sich vor Cyberangriffen und -kriminalität zu schützen?*
 - *a. Arbeiten Sie mit externen Expertinnen und Experten im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen?*
 - *b. Wenn ja, um welche Experten handelte es sich im Jahr 2025?*
 - *c. Wie erfolgte die Auswahl?*
 - *d. Arbeiten Sie mit externen Unternehmen im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen? Wenn ja, mit welchen?*
- *3. Gab es in Ihrem Ressort Risikoanalysen im Hinblick auf Cyberbedrohungen im Jahr 2025 und welche Ergebnisse brachten diese Analysen?*

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 zeitnah umgesetzt. Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT-Sicherheitsniveaus gemäß dem Netz- und Informationssystemsystemsicherheitsgesetz, BGBl. I Nr. 111/2018 (NISG), oder aber auch der Auflistung einzelner im Einsatz befindlicher Cybersicherheitsprodukte im Hinblick auf die Sicherung der Effektivität dieser Schutzmaßnahmen Abstand genommen werden.

Zur Frage 4:

- *Gibt es in Ihrem Ministerium Cybersicherheitsbeauftragte?*
 - *a. Welche Abteilungen oder Teams waren im Jahr 2025 innerhalb Ihres Ministeriums dafür zuständig?*
 - *b. Wie viele Personen waren in Ihrem Ministerium im Jahr 2025 im Bereich Cyber- und IT-Sicherheit tätig?*
 - *c. Welche konkreten Aufgaben nahmen diese Personen wahr?*

Im Bundesministerium für Justiz wird diese Rolle durch den Chief Information Security Officer (CISO) sowie das ISMS-Team wahrgenommen. Die jeweiligen Aufgaben und Verantwortlichkeiten sind in den Arbeitsplatzbeschreibungen geregelt und dienen der Erhöhung sowie Wahrung der Cybersicherheit im Bundesministerium für Justiz, sowohl auf strategischer als auch auf operativer beziehungsweise technischer Ebene. Da die Mitarbeiter:innen im Bereich der Infosicherheit in einem besonders sensiblen Bereich tätig sind, muss von der Bekanntgabe weiterer Details Abstand genommen werden.

Zur Frage 5:

- *Wie hoch war das Budget Ihres Hauses für IT- und Cybersicherheit im Jahr 2025?*

Da IT- und Cybersicherheit eine Querschnittsmaterie darstellen, sind die damit verbundenen Aufwände und Kosten nicht eindeutig zuordenbar.

Zur Frage 6:

- *Gab es im Jahr 2025 konkrete verpflichtende Schulungsangebote in Fragen der IT- und Cybersicherheit für Mitarbeiter:innen Ihres Hauses sowie nachgeordneter Dienststellen?*
 - *a. Wenn ja, um welche Schulungsangebote handelte es sich?*
 - *b. Wie hoch waren die Kosten für diese Schulungen?*

Im Bundesministerium für Justiz erfolgt die Schulung hinsichtlich der geltenden Regelungen im Zusammenhang mit der Informationssicherheit und dem Datenschutz sowie die Sensibilisierung zu Fragen von relevanten Cyberrisiken mit elektronischen Lernprogrammen, die zielgruppenspezifisch gestaltet und verpflichtend zu absolvieren sind. Im Rahmen der funktionsspezifischen Aus- und Fortbildung erfolgen darüber hinaus entsprechende Fachvorträge durch Informationssicherheitsexpert:innen. Da eine Aktualisierung der elektronischen Lernprogramme nur bei Änderungen der geltenden Regelungen erfolgt und im Jahr 2025 keine solchen Änderungen erforderlich waren, fielen im Jahr 2025 diesbezüglich keine gesonderten Kosten an.

Dr.ⁱⁿ Anna Sporrer

