Bundesministerium
Justiz

bmj.gv.at

Dr.in Anna Sporrer
Bundesministerin für Justiz

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2025-0.157.150

Ihr Zeichen: BKA - PDion (PDion)562/J-NR/2025

Wien, am 25. April 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Michael Schnedlitz, Kolleginnen und Kollegen haben am 26. Februar 2025 unter der Nr. **562/J-NR/2025** an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberangriffe auf österreichische Ministerien“ gerichtet.

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

Zur Frage 1:

- *Gab es in Ihrem Ressort Cyberangriffe seit dem Jahr 2022?*
  a. Falls ja, bitte um detaillierte Schilderung des Angriffs bzw. der Angriffe und der daraus resultierenden „Schäden".

Das Bundesministerium für Justiz sieht sich, wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im Bundesministerium für Justiz konnten bisher derartige Angriffsversuche abgewehrt sowie Schäden und Ausfälle hintangehalten werden. Die IKT-Sicherheit wird im Bund als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch die Bundesrechenzentrum GmbH (dem zentralen IKT-Dienstleister der Justiz), das Governmental Computer Emergency Response Team (GovCERT) und den „Innerer Kreis der operativen Koordinierungsstruktur (IK-DOK)“, kontinuierlich Anpassungen der IKT-

Sicherheitsstruktur vorgenommen, um auch auf sich ändernde Bedrohungen reagieren zu können.

Zu den Fragen 2, 4 und 5:

- *2. Gibt es konkrete Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?*
- *4. Welche konkreten Maßnahmen werden aktiv von Ihrem Ministerium ergriffen, um sich präventiv gegen Cyberattacken und gegen Cyberkriminalität zu schützen?*
- *5. Welche Rolle spielen externe Experten in der Vorbereitung und im Schutz gegen potenzielle Cyberangriffe?*
  - *a. Welche Art von Experten wird hier beigezogen und warum?*

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 dem Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018 (NISG), sowie auch die Auflistung einzelner im Einsatz befindlicher Cybersicherheitsprodukte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zur Frage 3:

- *Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?*

Den Staatsanwaltschaften und Gerichten obliegt gemeinsam mit dem Bundesministerium für Inneres die Strafverfolgung bei Cyberkriminalitätsdelikten.

Das Strafgesetzbuch (StGB) enthält eine Reihe von Straftatbeständen mit direktem Bezug des strafbaren Handelns zu Computersystemen (sogenannte Cybercrime-Delikte ieS), insbesondere:

- § 118a StGB „Widerrechtlicher Zugriff auf ein Computersystem“;
- § 119 StGB „Verletzung des Telekommunikationsgeheimnisses“;

- § 119a StGB „Missbräuchliches Abfangen von Daten“;
- § 126a StGB „Datenbeschädigung“;
- § 126b StGB „Störung der Funktionsfähigkeit eines Computersystems“;
- § 126c StGB „Missbrauch von Computerprogrammen oder Zugangsdaten“.

Daneben wird Informations- und Kommunikationstechnik aber auch als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt (zB Betrugsdelikte nach den §§ 146ff StGB, Erpressung nach den §§ 144f StGB oder Verhetzung nach § 283 StGB). Die technologieneutrale Formulierung der Straftatbestände und die generell abstrakte Umschreibung der Strafbarkeitsvoraussetzungen macht dabei die Straftatbestände offen für Entwicklungen, die zum Zeitpunkt ihrer Erlassung noch nicht voraussehbar waren – gerade auch im technologischen Bereich.

Zu den Fragen 6 und 7:

- *6. Gab es in Ihrem Ressort eigene Risikoanalysen?*
  a. Falls ja, welche?
  b. Falls nein, warum nicht?
- *7. Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ministeriums gerecht zu werden?*

Im Zuge der Umsetzung der NIS RL (Richtlinie (EU) 2016/1148, über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystem) durch das NISG (Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018) wurden die kritischen Dienste identifiziert, einer Risikoanalyse unterzogen und mit entsprechenden Prozessen zur Aufrechterhaltung bzw. zur Weiterführung der Kernaufgaben nach Systemausfällen hinterlegt.

Darüber hinaus wird auf die Beantwortung der Fragen 2, 4 und 5 verwiesen.

Zur Frage 8:

- *Gibt es so etwas wie „Cybersicherheitsbeauftragte" in Ihrem Ministerium?*
  a. Wenn ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dafür vorgesehen?
  b. Wenn ja, über welche Expertise verfügt diese Person/ verfügen diese Personen?
  c. Wenn ja, was sind die konkreten Aufgaben dieser Person/Personen?
  d. Wenn nein, warum nicht?

in meinem Ressort ist die Rolle des Chief Information Security Officers (CISO) vorgesehen. Der CISO trägt als Durchführungsverantwortlicher des Informationssicherheits-management-Prozesses die Gesamtverantwortung für die IT-Sicherheit im Ressort. Zu seinen Aufgaben gehören die Stärkung des Bewusstseins für IT-Sicherheit im Managementbereich, die Einbringung von IT-Sicherheits-Projektanträgen sowie die Gewährleistung der IT-Sicherheit im laufenden Betrieb.

Zu den Fragen 9 und 10:

- *9. Welche Maßnahmen wurden ergriffen, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?*
- *10. Welche Maßnahmen werden in Zukunft ergriffen bzw. sind geplant, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?*

Im Bundesministerium für Justiz werden allen Mitarbeiter:innen im Wege des Serviceportals Schulungen zum Thema der „IKT-Benutzungsrichtlinie“ zur Verfügung gestellt, im Rahmen derer insbesondere auch IKT-Sicherheitsthemen adressiert werden und somit auch eine Sensibilisierung der Mitarbeiter:innen für diese Thematik erfolgt. Für sämtliche Führungskräfte ist diese verpflichtend.

Dr.in Anna Sporrer

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2025-04-25T09:33:53+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	2025-04-25T09:37:26+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	