543/AB
vom 25.04.2025 zu 564/J (XXVIII. GP)

Bundesministerium
Bildung

bmb.gv.at

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.156.143

Die schriftliche parlamentarische Anfrage Nr. 564/J-NR/2025 betreffend Cyberangriffe auf österreichische Ministerien, die die Abgeordneten zum Nationalrat Michael Schnedlitz, Kolleginnen und Kollegen am 26. Februar 2025 an meinen Amtsvorgänger richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Eingangs wird darauf hingewiesen, dass es aufgrund der Bundesministeriengesetz-Novelle 2025 zum Teil zu erheblichen Veränderungen in der Zusammensetzung der Bundesministerien kam. Nach den Bestimmungen des Bundesministeriengesetzes in der nunmehr geltenden Fassung, BGBl. I Nr. 10/2025, bin ich zur Beantwortung dieser parlamentarischen Anfrage für den Bereich Bildung zuständig. Darüber hinaus verweise ich für die Bereiche Wissenschaft und Forschung auf die Beantwortung durch die Frau Bundesministerin für Frauen, Wissenschaft und Forschung.

Zu 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".

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese werden durch die IKT-Sicherheitssysteme ebenso weitestgehend automatisiert abgewehrt.

In Einzelfällen kommt es zu Angriffsversuchen, welche über diesem „Grundrauschen“ liegen. Dazu wird für den angefragten Zeitraum bis zum 12. Juni 2024 auf die Beantwortung der Parlamentarischen Anfrage Nr. 18816/J-NR/2024 vom 12. Juni 2024 verwiesen und für den Zeitraum vom 13. Juni 2024 bis zum Einlangen der Anfrage

angemerkt, dass es zu keinerlei gezielten Aktionen bzw. Angriffsversuchen der genannten Art gekommen ist.

Zu den Fragen 2, 4 und 5:

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

Zur Gewährleistung der Cybersicherheit werden Maßnahmen auf strategischer, operativer und technischer Ebene entsprechend dem Stand der aktuellen Technik ergriffen. Das Ministerium bedient sich zur Überprüfung der getroffenen Maßnahmen auch externer (Security-)Unternehmen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit der Technik im Ministerium zeitnahe umgesetzt. IKT-Sicherheit (und damit auch Datensicherheit) wird dabei als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und den dahinterliegenden Prozessen vorgenommen. Dies betrifft sowohl die Beschaffung von State-of-the-Art IKT-Sicherheitsinfrastruktur als auch die permanente Evaluierung und Anpassung der Prozesse. Darüber hinaus werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des Ministeriums zeitnahe umgesetzt.

Von einer detaillierten Auflistung aller Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT-Sicherheitsniveaus gemäß Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018, sowie der Auflistung einzelner im Einsatz befindlicher Cybersicherheitsprodukt muss im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu Frage 3:

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

Die Aufgabenwahrnehmung zur Bekämpfung von Cyberkriminalität obliegt dem Bundesministerium für Inneres, dem Bundesministerium für Justiz sowie dem Bundesministerium für Landesverteidigung.

Die Sicherung der IKT-Systeme fällt grundsätzlich in die Verantwortung der zuständigen obersten Organe. Mein Ministerium arbeitet u.a. über das Computer-Notfallteam der

öffentlichen Verwaltung (govCERT) eng mit anderen Ressorts zusammen, wobei es einen fortlaufenden Austausch über das aktuelle Lagebild gibt. Für die wichtigen Querschnittsapplikationen des Bundes, wie ELAK oder IT-Personalmanagement und Haushaltsverrechnung, betreibt die BRZ GmbH zentral ein eigenes Sicherheitssystem. Die IKT-Sicherheitsbeauftragten und/oder Informationssicherheitsbeauftragten der Bundesministerien treffen einander regelmäßig unter Schirmherrschaft des Bundeskanzleramtes und teilen Informationen und Best-Practices.

Zu den Fragen 6 und 7:

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

Die individuellen Risiken vor allem aus den Bereichen Datenschutz und IT-Sicherheit werden einem laufenden Monitoring unterzogen. Identifizierten Risiken wird mittels geeigneter technischer und organisatorischer Maßnahmen gegengesteuert.

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 wurden die kritischen Dienste identifiziert und mit entsprechenden Prozessen zur Aufrechterhaltung bzw. zur Weiterführung der Kernaufgaben nach Systemausfällen hinterlegt.

Im Übrigen darf auf die Beantwortung zu den Fragen 2, 4 und 5 hingewiesen werden.

Zu 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?

Die genannten bzw. vergleichbaren Aufgaben werden vom zuständigen Referat wahrgenommen.

Dazu gehören die Stärkung des Bewusstseins für IT-Sicherheit im Managementbereich, die Einbringung von IT-Sicherheits-Projektanträgen, die Gewährleistung der IT-Sicherheit im laufenden Betrieb sowie die Durchführung der notwendigen Risikoanalysen und Bewertungen und daraus folgende Maßnahmenableitung.

Darüber hinaus kann auf einzelne Personen im Hinblick auf den Schutz vor Ausspähung und der Sicherung der Effektivität der Maßnahmen nicht eingegangen werden.

Zu den Fragen 9 und 10:

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

Im Rahmen der Grundausbildung erfolgt eine grundlegende Schulung im Rahmen des Fachs Datenschutz und IT-Sicherheit. Darüber hinaus informiert die zuständige IKT-Abteilung routinemäßig und proaktiv zu Cybersicherheitsthemen inklusive konkreter Handlungsanleitungen. Weiters werden Angebote für Schulungen des Bundesministeriums für Inneres für oberste Organe in Anspruch genommen.

Wien, 25. April 2025

Christoph Wiederkehr, MA

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR BILDUNG
@ AMTSSIGNATUR

Unterzeichner	Bundesministerium für Bildung
Datum/Zeit	2025-04-25T11:01:03+02:00
Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Serien-Nr.	2097799830
Hinweis	Dieses Dokument wurde amtssigniert.
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at. Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmb.gv.at/verifizierung.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-04-25T14:51:17+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	