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

Bundesministerium
Frauen, Wissenschaft
und Forschung

bmfwf.gv.at

Herrn Präsident des Nationalrates
Dr. Walter Rosenkranz
Parlamentsdirektion
Dr. Karl Renner Ring 3
1017 Wien

Geschäftszahl: 2025-0.258.931

Ich darf darauf hinweisen, dass nach den Bestimmungen des Bundesministeriengesetzes in der nunmehr geltenden Fassung, BGBl. I Nr. 10/2025, die Zuständigkeit zur Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 564/J-NR/2025 betreffend Cyberangriffe auf österreichische Ministerien der Abg. Michael Schnedlitz, Kolleginnen und Kollegen vom 26. Februar 2025 für die Bereiche Wissenschaft und Forschung an mich übergegangen ist.

Die Anfrage wird nach den mir vorliegenden Informationen wie folgt beantwortet:

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. In den letzten Jahren waren dies insbesondere folgende gezielten Aktionen:

- Angriffe bis 12. Juni 2024: Dazu wird auf die Beantwortung der parlamentarischen Anfrage Nr. 18816/J-NR/2024 vom 12. August 2024 verwiesen.
- Angriffe seit dem 13. Juni 2024 bis zum Einlagen der Anfrage: Keine

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 Bereich Wissenschaft und Forschung werden zur Gewährleistung der Cybersicherheit Maßnahmen auf strategischer, operativer und technischer Ebene auf dem Stand der aktuellen Technik ergriffen. Dabei bedient sich das Ministerium zur Überprüfung der getroffenen Maßnahmen auch externer (Security-)Unternehmen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des Bereiches Wissenschaft und Forschung zeitnahe umgesetzt. IKT-Sicherheit (und damit auch Datensicherheit) wird im Bereich Wissenschaft und Forschung 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 Bereiches Wissenschaft und Forschung zeitnahe umgesetzt.

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

Zu Frage 3:

- *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. Der Bereich Wissenschaft und Forschung 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 unter Schirmherrschaft des Bundeskanzleramtes auf regelmäßiger Basis und teilen Informationen und Best-Practices.

Zu den Fragen 6 bis 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 Bereich Wissenschaft und Forschung werden die individuellen Risiken vor allem aus den Bereichen Datenschutz und IT-Sicherheit 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.

Zu Frage 8:

- *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 bis 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 Bereich Wissenschaft und Forschung erfolgt im Rahmen der Grundausbildung 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

Eva-Maria Holzleitner, BSc eh.

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR FRAUEN, WISSENSCHAFT UND FORSCHUNG @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Frauen, Wissenschaft und Forschung
	Datum/Zeit	2025-04-25T07:51:18+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.	641649373
	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.bmfwf.gv.at/verifizierung.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-04-25T09:32:19+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	