388/AB
vom 31.03.2025 zu 561/J (XXVIII. GP)

Bundesministerium
Arbeit und Wirtschaft

bmaw.gv.at

Dr. Wolfgang Hattmannsdorfer
Bundesminister

Stubenring 1, 1010 Wien

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.155.688

Ihr Zeichen: BKA - PDion (PDion)561/J-NR/2025

Wien, am 31. März 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Michael Schnedlitz und weitere haben am 26.02.2025 unter der **Nr. 561/J** an meinen Amtsvorgänger 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?*
    - *Falls ja, bitte um detaillierte Schilderung des Angriffs bzw. der Angriffe und der daraus resultierenden "Schäden".*

Ja. Alle Angriffe konnten automatisch abgewehrt werden; Schäden sind nicht entstanden.

Zur Frage 2

- *Gibt es konkrete Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?*

Ja.

Zur Frage 3

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

Dem Ressort fallen in der gesamtstaatlichen Bekämpfung von Cyberkriminalität keine speziellen Aufgaben zu.

Zu den Fragen 4 und 7

- *Welche konkreten Maßnahmen werden aktiv von Ihrem Ministerium ergriffen, um sich präventiv gegen Cyberattacken und gegen Cyberkriminalität zu schützen?*
- *Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ministeriums gerecht zu werden?*

Für den Verwaltungsbereich Wirtschaft betreibt das Ressort ein Informationssicherheitsmanagement-System, welches auf Basis von Risikokategorien alle Informationssicherheitsrisiken beinhaltet. Daraus leiten sich technische und organisatorische Sicherheitsmaßnahmen ab. Das Krisenhandbuch des Ressorts sowie auch das Incident Response Management stellen einige dieser konkreten Pläne für die Bewältigung von Cyberangriffen dar.

Im Verwaltungsbereich Arbeit wird entsprechende Hard- und Software, bereitgestellt durch den Dienstleister BRZ GmbH, eingesetzt, die den nicht autorisierten Zugriff auf das Netzwerk und die IKT-Systeme grundsätzlich verhindert. Weitere Belange zu Cyber-Awareness und dem Umgang mit der Arbeitsplatzausstattung hinsichtlich Cyber-Kriminalität sind durch einschlägige Richtlinien sowie der Implementierung von eLearning Plattformen dazu geregelt.

Zur Frage 5

- *Welche Rolle spielen externe Experten in der Vorbereitung und im Schutz gegen potenzielle Cyberangriffe?*
    - *Welche Art von Experten wird hier beigezogen und warum?*

Für den Verwaltungsbereich Wirtschaft betreibt das Ressort gemeinsam mit einem externen IKT-Dienstleister ein sogenanntes Security Operation Center zur raschen Erkennung und Analyse von Anomalien. Einmal im Jahr wird die IKT-Infrastruktur einer technischen Sicherheitsüberprüfung durch externe Spezialisten unterzogen.

Im Verwaltungsbereich Arbeit findet ein laufender Austausch mit dem Dienstleister BRZ GmbH sowie ressortübergreifend hinsichtlich IKT- und Cybersicherheit statt.

Zur Frage 6

- *Gab es in Ihrem Ressort eigene Risikoanalysen?*
    - *Falls ja, welche?*
    - *Falls nein, warum nicht?*

Für den Verwaltungsbereich Wirtschaft existiert pro IKT-Verfahren eine grundlegende Informationssicherheitsrisikoanalyse. Ergibt diese einen erhöhten Schutzbedarf, wird eine erweiterte Informationssicherheits- und Datenschutzrisikoanalyse durchgeführt.

Im Verwaltungsbereich Arbeit erfolgen laufende Beurteilungen durch den CISO und Risikoanalysen gemäß Risikodatenblatt sowie Implementierung und Betrieb der Anwendung CRISAM.

Zur Frage 8

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

Im Verwaltungsbereich Wirtschaft befassen sich derzeit drei Personen hauptsächlich mit dem Themenkomplex IKT-Sicherheit in einem eigenen Referat in der IKT-Abteilung. Diese Personen verfügen jeweils über jahrzehntelange Erfahrung im Bereich IKT(-Sicherheit). Weiterbildungen (teilweise samt Zertifizierungen) werden ebenfalls laufend durchgeführt. Das Team verantwortet gesamthaft die IKT-Sicherheit.

Im Verwaltungsbereich Arbeit befindet sich ein CISO & CISM als Cybersicherheitshauptverantwortlicher. Die jahrelange Expertise begründet sich aus der fundierten militärischen Ausbildung für IKT- und Cyber-Sicherheit als aktiver Stabs-, Fach-, und Lehroffizier im Fachbereich sowie durch weitere zivile Ausbildungen.

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?*

Zu nennen sind etwa Verankerung in der Grundausbildung, Schulungen verschiedener Zielgruppen, e-Learning, ein umfassendes Informationsangebot, Richtlinien, Checklisten, Merkblätter sowie eine Blackoutübung. Alle Maßnahmen werden fortgeführt.

Zur Frage 11

- *Wie sind die Fragen 1 bis 10 für das Kabinett der Staatssekretärin zu beantworten? (Bitte um gegliederte Beantwortung)*

Es ist nicht erkennbar, inwieweit für das Büro der Frau Staatssekretärin andere Feststellungen gelten könnten oder sollten als jene für das Ressort insgesamt, die vorstehend dargestellt wurden.

Dr. Wolfgang Hattmannsdorfer

Elektronisch gefertigt

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR ARBEIT UND WIRTSCHAFT
@ AMTSSIGNATUR

Unterzeichner	Bundesministerium für Arbeit und Wirtschaft
Datum/Zeit	2025-03-31T15:18:39+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.	1056650987
Hinweis	Dieses Dokument wurde amtssigniert.
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-03-31T15:25:08+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	