Bundesministerium
Innovation, Mobilität
und Infrastruktur

bmimi.gv.at

Peter Hanke
Bundesminister

ministerbuero@bmimi.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.155.611

. April 2025

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Schnedlitz und weitere Abgeordnete haben am 26. Februar 2025 unter der **Nr. 566/J** eine schriftliche parlamentarische Anfrage betreffend Cyberangriffe auf österreichische Ministerien an meine Amtsvorgängerin gerichtet.

Diese Anfrage beantworte ich wie folgt:

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“.*

Es gab in den letzten Jahren laufend Angriffe und Angriffsversuche auf die im Ressort eingesetzten Computersysteme. Es ist uns auf Basis der umgesetzten Sicherheitsvorkehrungen bisher jedoch immer gelungen, nennenswerte Schäden durch solche Angriffe abzuwehren.

Zu den Frage 2, 4, 5 und 7:

- *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?*
- *Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ministeriums gerecht zu werden?*

Das Ressort arbeitet kontinuierlich daran die IKT-Systeme durch spezifische Sicherheitsvorkehrungen präventiv und im Ernstfall gegen Cyberattacken und Cyberkriminalität zu schützen. Diese Sicherheitsvorkehrungen sollen die IKT-Sicherheitsrisiken minimieren und so die IKT-Systeme des Ressorts schützen. Für den Ernstfall werden Szenarien regelmäßig geübt, Wiederherstellungsprozesse evaluiert und redundante Infrastruktur aufgebaut.

Mein Ressort zieht dabei in allen Phasen der präventiven und aktiven Cyberangriffbewältigung – von der Planung, Umsetzung und Prüfung von Sicherheitsvorkehrungen, der Identifizierung von Schwachstellen, beim Betrieb von kritischen Services sowie im Incident Handling – externe Expertise hinzu. Ich ersuche allerdings um Verständnis, dass es gerade im Hinblick auf die Effektivität dieser Maßnahmen nicht möglich ist, die Sicherheitsvorkehrungen im Detail öffentlich mitzuteilen.

Zu Frage 3:

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

Die Wahrnehmung gesamtstaatlicher Aufgaben im Bereich der Cyberkriminalität ist kein Gegenstand der Vollziehung des Bundesministeriums für Innovation, Mobilität und Infrastruktur.

Zu Frage 6:

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

IKT-Sicherheit und damit auch die Cybersicherheit werden als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen. Für kritische Services sind Risikoanalysen ein Teil des Entwicklungsprozesses.

Das Österreichische Patentamt (ÖPA) führt eine spezifische Risikoanalyse durch, im Rahmen derer umfassende Risiken, die das ÖPA treffen können, laufend erhoben, beschrieben und bewertet und mit entsprechenden Maßnahmen hinterlegt 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?*

Wie oben ausgeführt, werden die IKT-Sicherheit und damit auch die Cybersicherheit als fortlaufender und umfassender Prozess verstanden, der mehrere Bereiche des Ressorts betrifft. An der Planung und Umsetzung von Cybersicherheitsmaßnahmen sind daher, abhängig von der aktuellen Lage und den aktuellen Herausforderungen mehrere Personen, mit jeweils unterschiedlicher Expertise, beteiligt. Jedenfalls werden die Agenden bezüglich Cybersicherheit vom CISO des Ressorts wahrgenommen.

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?*

Bedienstete meines Ministeriums haben E-Learnings zum Umgang mit klassifizierten Informationen und eine Schulung zur DSGVO 2024 verpflichtend jährlich zu absolvieren. Weiters können an der Verwaltungsakademie des Bundes (VAB) entsprechende Seminare, wie beispielsweise „OT-BS 150 - Cybersicherheit-Awareness-Training“ oder „BS-L 160/6 - Die Qualität der Arbeit im öffentlichen Dienst“, absolviert werden. Es wird außerdem auf die Möglichkeit verwiesen, die VAB E-Learning Plattform der Verwaltungsakademie des Bundes zu nutzen, in der beispielsweise das E-Learning „Persönliche Daten schützen“ absolviert werden kann. Seitens der IKT-Abteilung werden anlassbezogene Sensibilisierungsaktionen durchgeführt und Mitarbeiter:innen über neue Gefahrenquellen informiert. Eine auf das Führungspersonal zugeschnittene Informationssicherheitsschulung und themenspezifische Awareness Kampagnen sind geplant.

Im ÖPA finden Awareness-Trainings in Präsenz und als wiederkehrende Online-Kurse statt. Zudem werden entsprechende Anleitungen und Hinweise zur Verfügung gestellt und in Abteilungsmeetings wird Informationssicherheit immer wieder thematisiert. Die Wirkung der Maßnahmen werden durch Security-Tests geprüft (z.B. Phishing-Kampagne) und daraus die weiteren Maßnahmen abgeleitet.

Mein Ressort evaluiert laufend das interne Weiterbildungsangebot und steht auch bezüglich des Themas „Digitale Sicherheit“ im laufenden Austausch mit Bediensteten und den betreffenden Fachabteilungen. Die Bediensteten des Ministeriums werden regelmäßig auf die Möglichkeit des Besuchs von Seminaren an der Verwaltungsakademie des Bundes hingewiesen. Im Bedarfsfall sind darüberhinausgehende anlassbezogene Weiterbildungen möglich.

Mit freundlichen Grüßen

Peter Hanke

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNOVATION, MOBILITÄT UND INFRASTRUKTUR @ AMTSSIGNATUR	Hinweis	Dieses Dokument wurde amtssigniert.
	Datum	2025-04-25T15:56:07+02:00
	Seriennummer	2069212815
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2025-04-25T16:16:25+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	