533/AB
vom 25.04.2025 zu 647/J (XXVIII. GP)

Bundesministerium
Wohnen, Kunst, Kultur,
Medien und Sport

bmwkms.gv.at

Andreas Babler, MSc
Vizekanzler
Bundesminister für Wohnen, Kunst, Kultur,
Medien und Sport

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.169.176

Wien, am 24. April 2025

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Schnedlitz und weitere Abgeordnete haben am 27. Februar 2025 unter der **Nr. 647/J** an meinen Amtsvorgänger Mag. Werner Kogler eine schriftliche parlamentarische Anfrage betreffend „Cyberangriffe auf österreichische Ministerien“ gerichtet.

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

Zum Stichtag der Anfrage war das nunmehrige Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport noch in der Zusammensetzung des Bundesministeriums für Kunst, Kultur, Öffentlichen Dienst und Sport (BMKÖS), weshalb in der Folge die Bezeichnung „BMKÖS“ verwendet wird.

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".*

Das BMKÖS sieht sich – wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen – kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im BMKÖS konnten bisher derartige Angriffsversuche abgewehrt sowie Schäden und Ausfälle weitgehend hintangehalten werden.

Zu Frage 2:

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

Die IKT-Sicherheit wird im Bund als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das Governmental Computer Emergency Response Team (GovCERT) und den Inneren Kreis der operativen Koordinierungsstruktur (IKDOK), kontinuierlich Anpassungen der IKT-Sicherheitsstruktur vorgenommen um auch auf sich ändernde Bedrohungen reagieren zu können. Gemeinsam mit dem BRZ werden kontinuierlich Anpassungen und Weiterentwicklungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen um das BMKÖS vor Cyberangriffen zu schützen. Dies betrifft sowohl die Beschaffung von State-of-the-Art IKT-Sicherheitsinfrastruktur, als auch die permanente Evaluierung und Anpassung der Prozesse und den Aufbau von Organisationseinheiten.

Sollte ein Cyberangriff krisenhafte Auswirkungen verursachen, tritt das Cyberkrisenmanagement in Kraft. Die Strukturen und Zuständigkeiten sind im NIS-Gesetz geregelt. Treten darüber hinaus die Cyberdimension überschreitende Effekte auf, erfolgt die Koordination der Krise gemäß B-KSG.

Im Zug der IT-Umstellung und der Neuorganisation des BMKÖS zum BMWKMS wird auch an der Ausgestaltung einer neuen allgemeinen IT-Sicherheitsrichtlinie, an Cybersecurity-Notfallplänen und der Etablierung eines Informationssicherheits-management-Systems gearbeitet.

Zu Frage 3:

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

Die Aufgabenwahrnehmung zur gesamtstaatlichen Bekämpfung der Cyberkriminalität obliegt dem Bundesministerium für Inneres. Ich darf daher auf die diesbezügliche Beantwortung der parlamentarischen Anfrage durch den Herrn Bundesminister für Inneres (Nr. 528/J) verweisen.

Zu Frage 4:

- *Welche konkreten Maßnahmen werden aktiv von Ihrem Ministerium ergriffen, um sich präventiv gegen Cyberattacken und gegen Cyberkriminalität zu schützen?*

Folgende Maßnahmen werden ergriffen:

- Securityspezifische Schulungen für einen Teil der IT-Mitarbeiter:innen (BKA Schulung)
- Verwendung eines CERT Postfachs für Security Anliegen
- Allgemeine Schulungen in Sicherheitsthemen und ähnlichen Belangen durch ein Online-Schulungsportal (momentan in Arbeit)
- Beiwohnen unseres CISOs in IKT Bund Meetings und CISO Board Meetings
- Empfehlung der Verwendung von KeyPass, Passwortverwaltungstool für Mitarbeiter:innen vor allem für neueintretende Mitarbeiter:innen
- Aktuelle IT Sicherheitshinweise im Intranet
- Laufende Abstimmung mit dem BRZ in Hinblick auf die Weiterentwicklung der IT Sicherheit

Zu Frage 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?*

Das BRZ nimmt als externer Betreiber der BMKÖS IT-Infrastruktur eine wichtige Rolle in der Vorbereitung und im Schutz gegen potenzielle Cyberangriffe ein. Daher werden bei Bedarf ausschließlich Mitarbeiter:innen des BRZ beigezogen, da diese mit den IT-Systemen des BMKÖS vertraut sind. Darüber hinaus erfolgt ein regelmäßiger Austausch mit anderen Ressorts in den einschlägigen IT-Gremien des Bundes (bspw. IKT Bund und CDO Task Force).

Zu den Fragen 6 und 7:

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

Die IKT-Sicherheit wird als fortlaufender Prozess verstanden. Dabei werden gemeinsam mit dem BRZ die ressortspezifischen Risiken im Bereich IT Sicherheit laufend evaluiert und bei Bedarf entsprechende Maßnahmen gesetzt. Ein wesentlicher Baustein der aktiven

Ausgestaltung der IT Sicherheit in der Praxis ist ein einheitlicher IT Standardarbeitsplatz. Der „Managed Desktop“ des BRZ ist der Standardarbeitsplatz des Bundes und unterliegt den höchsten Sicherheitsbestimmungen. Das ermöglicht einen sicheren Betrieb in Zusammenarbeit mit dem externen IT-Dienstleister BRZ. Die zur Verfügung gestellte Standardsoftware wird laufend erweitert und angepasst um IT Sicherheitsrisiken zu minimieren. Die erst kürzlich durchgeführte Umstellung auf Windows 11 als Basisbetriebssystem erfolgte insbesondere auf Grund von IT Sicherheitsüberlegungen.

Bei der Einführung von neuer Software werden gegebenenfalls begleitend auch organisatorische Maßnahmen gesetzt um einen sicheren IT Betrieb gewährleisten zu können.

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?*

IT-Sicherheit ist eine Querschnittsmaterie und wird daher von mehreren Personen übernommen. In der Geschäftseinteilung des BMKÖS ist ein CISO (Chief Information Security Officer) vorgesehen. Die mit IT-Sicherheit befassten Personen verfügen über Ausbildungen im IT-Bereich, mehrjährige einschlägige Berufserfahrung und bilden sich laufend auf dem Gebiet der Cybersicherheit weiter, wie z.B. bei CISO-Schulungen des BKA. Die Aufgaben der mit IT-Sicherheit befassten Personen ergeben sich aus der Geschäftseinteilung des BMKÖS. Im Wesentlichen beziehen sich diese Aufgaben auf den sicheren IT Betrieb im BMKÖS.

Zu Frage 9:

- *Welche Maßnahmen wurden ergriffen, um alle Mitarbeitenden in Ihrem Ministerium gegen die drohende Gefahr von Cyberangriffen zu sensibilisieren?*

Die Mitarbeiter:innen des BMKÖS werden diesbezüglich sowohl in Präsenz als auch online über verschiedenste Kanäle wie E-Mail und das Intranet geschult und sensibilisiert.

Zu Frage 10:

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

Geplant beziehungsweise in Auftrag gegeben sind Online Schulungen mit einem verpflichtenden Abschluss/Test zu Ende des Lernmoduls. Die Schulungen sind künftig verpflichtend für alle Mitarbeiter:innen einmal jährlich durchzuführen und sollen abgesehen vom Umgang mit drohenden Cybersecuritygefahren bzw. -angriffen auch grundsätzlich auf einen bewussten und sicheren Umgang mit der IT bzw. mit IT-Equipment schulen.

Zu Frage 11:

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

Es gibt keine abweichenden Regeln oder Maßnahmen für das Kabinett der Staatssekretärin.

Andreas Babler, MSc

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR WOHNEN, KUNST, KULTUR, MEDIEN UND SPORT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport
	Datum/Zeit	2025-04-25T10:08:14+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.	479679199
	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	2025-04-25T14:23:38+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	