18231/AB
vom 12.08.2024 zu 18817/J (XXVII. GP)

Bundesministerium
Kunst, Kultur,
öffentlicher Dienst und Sport

bmkoes.gv.at

Mag. Werner Kogler
Vizekanzler
Bundesminister für Kunst, Kultur,
öffentlichen Dienst und Sport

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2024-0.450.081

Wien, am 12. August 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 12. Juni 2024 unter der **Nr. 18817/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Mögliche Hackerangriffe auf Ihr Ministerium“ gerichtet.

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

Zu Frage 1:

- *Besteht die Möglichkeit, dass Hackerangriffe gegen Ihr Ministerium vorgenommen werden und gelingen könnten?*
    a. *Wenn ja, wie sind Sie auf so einen Fall vorbereitet?*

Angriffsversuche und Angriffe selbst auf die IT-Systeme eines Bundesministeriums können nie ausgeschlossen werden. Das Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS) ist zur Abwehr solcher Versuche durch technische und organisatorische Sicherheitsmaßnahmen auf dem Stand der Technik. Mit der BRZ GmbH (BRZ) als zentralem IT-Dienstleister des BMKÖS ist das Höchstmaß an technischer Sicherheit garantiert.

Zu Frage 2:

- *Gab es in den letzten fünf Jahren sogenannte „Überlastungsangriffe" oder andere, abgewehrte Angriffe?*
    a. *Wenn ja, wann?*
    b. *Wenn ja, in welchem Umfang?*

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese werden durch die IKT-Sicherheitssysteme ebenso weitestgehend automatisiert abgewehrt. Aktuell sind keine Überlastungsangriffe auf die IT-Infrastruktur des BMKÖS bekannt.

Zu den Fragen 3, 5 und 6:

- *Wie wird seitens Ihres Ministeriums für die Datensicherheit gesorgt?*
- *Gibt es zusätzlich ein eigenes Sicherheitssystem für Ihr Ministerium?*
- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

IKT-Sicherheit (und damit auch Datensicherheit) wird im BMKÖS als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden, gemeinsam mit dem BRZ, kontinuierlich Anpassungen und Weiterentwicklungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen. 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. Darüber hinaus werden bei Bedarf, gemeinsam mit der BRZ GmbH, basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt.

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

Zu Frage 4:

- *Gibt es ein übergeordnetes Sicherheitssystem, das über alle Bundesministerien und die vorhandenen Daten wacht?*
    a. *Wenn nein, ist zukünftig ein derartiges Sicherheitssystem geplant?*
    b. *Wenn ja, wann soll dieses in Betrieb gehen?*

Prinzipiell fällt die Sicherung der IKT-Systeme in die Verantwortung der zuständigen obersten Organe. Das BMKÖS arbeitet im Bereich der IKT-Sicherheit eng mit anderen Ressorts zusammen. Für die wichtigen Querschnittsapplikationen des Bundes, wie ELAK oder IT-Personalmanagement und Haushaltsverrechnung, betreibt das BRZ zentral ein eigenes Sicherheitssystem. Die IKT-Sicherheitsbeauftragten und/oder Informationssicherheitsbeauftragten der Bundesministerien treffen einander auf regelmäßiger Basis und teilen Informationen und Best-Practices.

Zu Frage 7:

- *Welches Gremium ist vorgesehen, wenn so ein Angriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*

Sollte ein Cyberangriff krisenhafte Auswirkungen verursachen, tritt das Cyberkrisenmanagement in Kraft. Die Strukturen und Zuständigkeiten sind im NISG geregelt. Treten darüber hinaus die Cyberdimension überschreitende Effekte auf, erfolgt die Koordination der Krise gemäß Bundes-Krisensicherheitsgesetz (B-KSG), BGBl. I Nr. 89/2023.

Zu Frage 8:

- *Werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?*
    a. *Wenn ja, wie oft?*
    b. *Wenn ja, in welchem Umfang?*
    c. *Wenn nein, warum nicht?*

Die einzuleitenden Maßnahmen und Zuständigkeiten bei Vorfällen im Zusammenhang mit wesentlichen Cyberbedrohungen werden im BMKÖS gemeinsam mit dem BRZ laufend evaluiert.

Zu Frage 9:

- *Wie lange würde es voraussichtlich dauern, um ein Parallelsystem herstellen zu können, um auch weiterhin einsatzfähig zu sein?*

Die technischen Maßnahmen zur Trennung kritischer Systeme sowie die fortlaufenden Anpassungen an sich ändernde Bedrohungen sollen weitreichende Auswirkungen nach Cyberangriffen verhindern.

Mag. Werner Kogler

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR KUNST, KULTUR, ÖFFENTLICHEN DIENST UND SPORT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport
	Datum/Zeit	2024-08-12T14:42:28+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2099471880
	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	2024-08-12T14:49:04+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	