11485/AB
vom 08.09.2022 zu 11857/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: 2022-0.525.769

Wien, am 7. September 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA und weitere Abgeordnete haben am 8. Juli 2022 unter der Nr. **11857/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 auch nur im Geringsten die Möglichkeit, dass derartige Hackerangriffe mit Datenklau gegen Ihr Ministerium vorgenommen werden und gelingen könnten?*
    a. *Wenn ja, wie sind Sie konkret auf so einen Zwischenfall vorbereitet?*

Angriffsversuche und Angriffe selbst 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 in den Bereichen Prävention, Absicherung, Erkennung und Incident Response vorbereitet.

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?

In meinem Ressort gibt es keine Hinweise auf derartige Angriffe.

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?*

Das Thema Datensicherheit wird im BMKÖS sowohl auf technischer, organisatorischer als auch technischer Ebene adressiert. Die gesetzliche Verpflichtung hierzu erwächst aus § 22 Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018.

IKT-Sicherheit (und damit auch Datensicherheit) wird im BMKÖS 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-Sicherheits-Infrastruktur als auch die permanente Evaluierung und Anpassung der Prozesse.

Basierend auf den aktuellen Bedrohungslagen werden auch Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Techniker:innen des Ressorts zeitnahe umgesetzt.

Ich bitte um Verständnis, dass von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß NISG oder der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden muss.

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. Wann soll dieses in Betrieb gehen?*

Prinzipiell fällt die Sicherung der IKT-Systeme in die Verantwortung der zuständigen obersten Organe. Das NISG ermöglicht dem Bundesministerium für Inneres den Betrieb eines IOC-basierten Frühwarnsystems. Für Details zur Umsetzung darf ich auf die Beantwortung der parlamentarischen Anfrage Nr. 11856/J vom 8. Juli 2022 durch den Herrn Bundesminister für Inneres verweisen.

Zu Frage 7:

- *Welches Gremium ist vorgesehen, wenn so wie im Fall des Bundeslands Kärnten 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.

Zu Frage 8:

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

Das BMKÖS nimmt an unterschiedlichen sowohl international als auch national ausgerichteten Übungen statt, wie z.B.:

- Übung „Cyber Europe 2022“ (https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2022)
- Cybersicherheitsübungen mit weiteren EU-Mitgliedsstaaten

Zu Frage 9:

- *Wie lange würde es voraussichtlich dauern um, wie im vorliegenden Fall des Bundeslands Kärnten, ein Parallelsystem wiederherstellen 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 wie im Fall Kärnten verhindern.

Das kontinuierliche Risikomanagement definiert die im BMKÖS kritischen Prozesse und Dienste. Darüber hinaus wurden Vorkehrungen getroffen, um sowohl technische als auch von Dritten verursachte Ausfälle möglichst zeitnah zu kompensieren.

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	2022-09-08T08:33:56+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

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-08T08:37:55+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	