11497/AB
vom 08.09.2022 zu 11848/J (XXVII. GP)

Bundesministerium
Europäische und internationale
Angelegenheiten

bmeia.gv.at

Mag. Alexander Schallenberg
Bundesminister

Minoritenplatz 8, 1010 Wien, Österreich

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Wien, am 8. September 2022

GZ. BMEIA-2022-0.508.470

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 8. Juli 2022 unter der Zl. 11848/J-NR/2022 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 den Fragen 1, 3, 5 und 6:

- *Besteht auch nur im Geringsten die Möglichkeit, dass derartige Hackerangriffe mit Datenklau gegen Ihr Ministerium vorgenommen werden und gelingen könnten?*
  Wenn ja, wie sind Sie konkret auf so einen Zwischenfall vorbereitet?
- *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?*

Die Sicherheit von Informations- und Kommunikationstechnik (IKT-Sicherheit) ist ein fortlaufender, nie abgeschlossener Prozess, wobei Maßnahmen und Konzepte einer dauerhaften, dem aktuellen Stand der Technik entsprechenden Evaluierung und Anpassung unterliegen. Angriffe auf IT-Systeme können auch prinzipiell nie ausgeschlossen werden. Das gilt selbstverständlich auch für das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA). Ein besonderer Fokus liegt auf dem Bereich der Sensibilisierung für Sicherheitsfragen für die Mitarbeiterinnen und Mitarbeiter meines Ressorts, die laufend in

2 von 3

IKT-sicherheitsrelevante Verhaltensregelungen geschult werden. Anlassbezogen erfolgt dies auch mit Unterstützung externer Expertinnen und Experten. Von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gem. dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (NISG), BGBI. I Nr. 111/2018, wird in Hinblick auf die Sicherung der Effektivität dieser Maßnahmen Abstand genommen.

Zu Frage 2:

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

In den vergangenen fünf Jahren kam es zu vier Überlastungsangriffen („Distributed Denial-of-Service“-Angriffe) auf Systeme des BMEIA, die aufgrund des Netzdesigns und der eingesetzten Schutzmechanismen jedoch kaum Einfluss auf die Verfügbarkeit der Services hatten.

Zu Frage 4:

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

Entsprechend den Bestimmungen des NISG wird ein Frühwarnsystem betrieben.

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?*
  Wenn ja, wie oft?
  Wenn ja, in welchem Umfang?

Das BMEIA nimmt an unterschiedlichen, sowohl international als auch national ausgerichteten Übungen teil, bei denen u.a. Hackerangriffe und Abwehrstrategien simuliert werden. Die eingesetzten Systeme und Applikationen werden laufend auf Schwachstellen überprüft.

Zu Frage 9:

- *Wie lange würde es voraussichtlich dauern um, wie im vorliegenden Fall des Bundeslands Kärnten, ein Parallelsystem wieder herstellen zu können um auch weiterhin einsatzfähig zu sein?*

Die technischen Sicherheitsmaßnahmen sowie die fortlaufenden Anpassungen an sich ändernde Bedrohungen haben zum Ziel, weitreichende Auswirkungen auf die Verfügbarkeit der Systeme zu verhindern.

Mag. Alexander Schallenberg

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR EUROPÄISCHE UND INTERNATIONALE ANGELEGENHEITEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für europäische und internationale Angelegenheiten
	Datum/Zeit	2022-09-08T10:33:59+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.	789818819
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmeia.gv.at/verifizierung	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-08T10:37:32+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.	