11519/AB
vom 08.09.2022 zu 11856/J (XXVII. GP)

bmi.gv.at

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2022-0.518.246

Wien, am 31. August 2022

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Rosa Ecker, MBA, und weitere Abgeordnete haben am 8. Juli 2022 unter der Nr. **11856/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:

Zur 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 können nie generell ausgeschlossen werden. Das Bundesministerium für Inneres 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.

Zur 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 den letzten 12 Monaten wurden insgesamt 41 DDoS Attacken, in der Dauer von wenigen Minuten bis einigen Stunden, detektiert. Durch die vorhandenen präventiven und reaktiven Sicherheitsmaßnahmen konnte jedoch innerhalb der letzten fünf Jahre keine Gefährdung festgestellt werden. Es kam lediglich zeitweise zu temporärer Nichterreichbarkeit von über das Internet angebotene IT-Services.

Zur Frage 3:

- *Wie wird seitens Ihres Ministeriums für die Datensicherheit gesorgt?*

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

IKT-Sicherheit (und damit auch Datensicherheit) wird im Bundesministerium für Inneres als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen 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.

Darüber hinaus werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikern des Ressorts zeitnahe umgesetzt.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetzes, 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.

Zur 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. Darüberhinausgehende Auskünfte können aus sicherheitstechnischen Gründen nicht erteilt werden.

Zur Frage 5:

- *Gibt es zusätzlich ein eigenes Sicherheitssystem für Ihr Ministerium?*

Ja.

Zur Frage 6:

- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Die IT-Systeme und Netzwerke des Ressorts werden jährlich einer umfassenden technischen Evaluierung unterzogen und gegebenenfalls angepasst.

Zur 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 NIS Gesetz geregelt.

Zur Frage 8:

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

Ja. Alle zwei Jahre nimmt das Bundesministerium für Inneres an der von der ENISA organisierten „Cyber Europe“ Übung teil. Jährlich findet auf EU-Ebene, in Bezug auf die im Schengenraum gemeinsamen betriebenen nationalen und internationalen Systeme, eine

gemeinsame überregionale Cyber Security Übung unter der Aufsicht der Europäischen Kommission statt.

Zur 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 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 Bundesministerium für Inneres kritischen Prozesse und Dienste. Für diese ist ein Betriebskontinuitätsmanagement eingerichtet. Darüber hinaus wurden Vorkehrungen getroffen, um sowohl technische als auch von Dritten verursachte Ausfälle möglichst zu verhindern oder zeitnah zu kompensieren.

Gerhard Karner

	Datum/Zeit	2022-09-08T13:07:43+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.	148769640
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-08T13:13:52+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.	