18240/AB
vom 12.08.2024 zu 18815/J (XXVII. GP)

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2024-0.532.894

Wien, am 12. August 2024

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Rosa Ecker, MBA, hat am 12. Juni 2024 unter der Nr. **18815/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 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 auf IT-Systeme können generell nie 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 Umgang?*

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese werden durch die IKT-Sicherheitssysteme ebenso weitestgehend automatisiert abgewehrt. Angriffe von größerer Intensität bzw. Komplexität waren nur in Einzelfällen feststellbar.

Im Durchschnitt werden pro Jahr ca. 40 bis 50 nennenswerte DDoS Attacken – die in der Regel zwischen wenigen Minuten bis hin zu einigen Stunden andauern – detektiert. Durch die vorhandenen präventiven und reaktiven Sicherheitsmaßnahmen war jedoch innerhalb der letzten fünf Jahre keine Gefährdung feststellbar.

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 Bundesministerium für Inneres als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz unter Abstützung auf entsprechende Systeme 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 Technikerinnen und 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 Informationssystemsicherheitsgesetz, 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. *Wenn ja, wann soll dieses in Betrieb gehen?*

Das Bundesministerium für Inneres arbeitet u.a. über das Computer-Notfallteam der öffentlichen Verwaltung (govCERT) eng mit anderen Ressorts zusammen, wobei es einen fortlaufenden Austausch über das aktuelle Lagebild gibt. Für die wichtigen Querschnittsapplikationen des Bundes, wie ELAK oder IT-Personalmanagement und Haushaltsverrechnung, betreibt die BRZ GmbH zentral ein eigenes Sicherheitssystem. Die IKT-Sicherheitsbeauftragten und/oder Informationssicherheitsbeauftragten der Bundesministerien treffen einander unter Schirmherrschaft des Bundeskanzleramtes auf regelmäßiger Basis und teilen Informationen und Best-Practices.

Darüber hinaus darf ich auf die Beantwortung der parlamentarischen Anfragen Nr. 11856/J vom 8. Juli 2022 durch den Bundesminister für Inneres sowie 11854/J vom 8. September 2022 durch den Bundeskanzler verwiesen werden.

Zur 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 NIS-Gesetz geregelt. Treten darüber hinaus die Cyberdimension überschreitende Effekte auf, erfolgt die Koordination der Krise gemäß Bundes-Krisensicherheitsgesetz.

Zur 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?*

Das Bundesministerium für Inneres verfügt über einen Notfallplan, der die einzuleitenden Maßnahmen und Zuständigkeiten bei auftretenden Vorfällen im Zusammenhang mit wesentlichen Cyberbedrohungen regelt, und führt regelmäßige Notfallübungen in Form von Simulationen, Planspielen, Workshops und dergleichen durch.

Das Bundesministerium für Inneres und die im Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) vertretenen Ministerien nehmen an unterschiedlichen, sowohl international als auch national ausgerichteten Übungen teil. Darunter sind:

Alle zwei Jahre nimmt das Bundesministerium für Inneres an der von der Agentur der Europäischen Union für Cybersicherheit (ENISA) organisierten Übung „Cyber Europe“ teil. Die diesjährige „Cyber Europe“ fand am 18. und 19. Juni statt und hatte den Sektor Energie im Fokus.

Das Bundesministerium für Inneres nimmt an den vom Kompetenzzentrum Sicheres Österreich (KSÖ) organisierten Planspielen zu Cybersicherheit teil.

Zur 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 eines Sicherheitsvorfalles verhindern.

Gerhard Karner

	Datum/Zeit	2024-08-12T17:03:33+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.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-12T17:08:19+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	