18234/AB
vom 12.08.2024 zu 18813/J (XXVII. GP)

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

bmk.gv.at

Leonore Gewessler, BA
Bundesministerin

leonore.gewessler@bmk.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 W i e n

Geschäftszahl: 2024-0.441.228

. August 2024

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Ecker, MBA und weitere Abgeordnete haben am 12. Juni 2024 unter der **Nr. 18813/J** an mich eine schriftliche parlamentarische Anfrage betreffend Mögliche Hackerangriffe auf Ihr Ministerium gerichtet.

Diese Anfrage beantworte ich 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 Informationstechnik (IT) Systeme eines Ministeriums können nie ausgeschlossen werden. Mein Ressort 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?*

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese werden durch die Informations- und Kommunikationstechnologie (IKT)-Sicherheitssysteme ebenso weitestgehend automatisiert abgewehrt.

Darüber hinaus ist kein erfolgreicher Angriff auf die im Ressort betriebenen Computersysteme bekannt.

Weiters musste auch das Österreichische Patentamt in den letzten fünf Jahren keine „Überlastungsangriffe“ oder andere Angriffe abwehren.

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 werden als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz unter Abstützung auf entsprechende Systeme kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und den dahinterliegenden Prozessen vorgenommen. Dies betrifft sowohl die Beschaffung von State-of-the-Art IKT-Sicherheitsinfrastruktur, als auch die permanente Evaluierung und Anpassung der Prozesse.

Weiters werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Techniker:innen 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.

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. Mein Ministerium arbeitet darüber hinaus 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 wird 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.

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 NIS-Gesetz geregelt. Treten darüber hinaus die Cyberdimension überschreitende Effekte auf, erfolgt die Koordination der Krise gemäß B-KSG.

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?*

Verschiedene Aspekte der IKT-Sicherheitsmaßnahmen werden regelmäßig geübt und geprüft. Es wird aber um Verständnis ersucht, dass die Details zu den Übungen und Überprüfungen nicht öffentlich bekannt gegeben werden können.

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. Die Dauer für die Bewältigung einer IKT-Krise hängt wesentlich von den betroffenen Systemen und vom Ausmaß des Schadens ab. Eine pauschale Beantwortung in Bezug auf die Dauer für die Krisenbewältigung kann daher nicht gegeben werden.

Leonore Gewessler, BA

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR KLIMASCHUTZ, UMWELT, ENERGIE, MOBILITÄT, INNOVATION UND TECHNOLOGIE @ AMTSSIGNATUR	Hinweis	Dieses Dokument wurde amtssigniert.
	Datum	2024-08-12T16:33:13+02:00
	Seriennummer	1871969199
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-12T16:37:49+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	