11285/AB
vom 01.09.2022 zu 11860/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: 2022-0.499.196

. September 2022

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Ecker, MBA und weitere Abgeordnete haben am 08. Juli 2022 unter der **Nr. 11860/J** an mich eine schriftliche parlamentarische Anfrage betreffend mögliche Hackerangriffe auf Ihr Ministerium gerichtet.

Diese Anfrage beantworte ich 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?*

Hackerangriffe und Angriffsversuche können nie ausgeschlossen werden. Mein Ministerium setzt mehrere spezifische Sicherheitsvorkehrungen zum Schutze der IKT-Systeme des Ressorts ein, um die IKT-Sicherheitsrisiken zu minimieren. Ich ersuche aber um Verständnis, dass gerade im Hinblick auf die Effektivität dieser Maßnahmen es nicht möglich ist, die Sicherheitsvorkehrungen im Detail öffentlich mitzuteilen.

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?*

Es gab in den letzten Jahren verschiedene Angriffe auf die im Ressort betriebenen Computersysteme, ein erfolgreicher Angriff ist uns aber nicht bekannt. Ein spezieller Überlastungsangriff auf die im Ressort betriebenen Computersysteme, der nennenswerten Schaden verursacht hätte, wurde nicht beobachtet.

Das Österreichische Patentamt musste 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 die Datensicherheit werden 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. Insbesondere im Rahmen von Systemerneuerungen und Systemerweiterungen werden auch die Sicherheitssysteme angepasst.

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 IKT-Sicherheitsmaßnahmen und auch von 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. *Wann soll dieses in Betrieb gehen?*

Prinzipiell fällt die Sicherung der IKT-Systeme in die Verantwortung der zuständigen obersten Organe. Das NIS-Gesetz 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 08. Juli 2022 durch den 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 NIS-Gesetz geregelt.

Zu Frage 8:

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

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, wie im vorliegenden Fall des Bundeslands Kärnten, ein Parallelsystem wieder herstellen zu können um auch weiterhin einsatzfähig zu sein?*

Die Dauer für die Bewältigung einer IKT-Krise hängt wesentlich von den betroffenen Systemen und vom Ausmaß des Schadens ab. Eine pauschale Beantwortung für die Dauer einer 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	2022-09-01T12:45:20+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/

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-01T12:50:59+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.	