11423/AB
vom 07.09.2022 zu 11861/J (XXVII. GP)

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

Johannes Rauch
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2022-0.503.965

Wien, 26.8.2022

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 11861/J der Abgeordneten Rosa Ecker betreffend mögliche Hackerangriffe auf Ihr Ministerium** wie folgt:

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 selbst können trotz aller Maßnahmen nie ausgeschlossen werden. Das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK) 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.

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 Jahren konnten folgende gezielte Aktionen identifiziert werden:

- 2017 – Schadsoftware (Wurm): Zum Zwecke der Bereinigung des Systems ist es zu einem vorübergehenden Stillstand des Mailsystems gekommen.
- 2020 – Angriff auf Citrix-Netscaler: Es ist dabei zu keiner für Anwender:innen wahrnehmbaren Einschränkung der Verfügbarkeit und zu keinem unberechtigten Zugriff auf Daten gekommen.

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?*

Das Thema Datensicherheit wird im BMSGPK sowohl auf technischer, organisatorischer als auch technischer Ebene verfolgt und permanent an neue Gegebenheiten angepasst. Die gesetzliche Verpflichtung hierzu erwächst aus § 22 Netz- und Informationssystem-sicherheitsgesetz, BGBl. I Nr. 111/2018.

IKT-Sicherheit (und damit auch Datensicherheit) wird im BMSGPK 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. Dadurch entsteht ein umfangreiches Sicherheitssystem mit entsprechenden Maßnahmen.

Außerdem 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 Informations-systemsicherheitsgesetz, BGBl. I Nr. 111/2018, oder aber auch der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutz-maßnahmen Abstand genommen werden.

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 8. Juli 2022 durch den Bundesminister für Inneres verweisen. Es gibt darüber hinaus eine enge Zusammenarbeit und einen permanenten Informationsaustausch in Gremien und mit den zuständigen CERTs.

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 Cyberkrisen-management in Kraft. Die Strukturen und Zuständigkeiten sind im NIS Gesetz geregelt. Darüber hinaus ist es möglich das GovCERT als Partner bei einem Cyberangriff hinzuzuziehen.

Frage 8: *Werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?*

a. Wenn ja, wie oft?

b. Wenn ja, in welchem Umfang?

Es werden verschiedene Szenarien für Cyberbedrohungen mehrfach jährlich wieder-kehrend geprüft und durchgespielt. Das BMSGPK nimmt auch an unterschiedlichen, sowohl international als auch national ausgerichteten Übungen teil. Als Beispiel für derartige Kooperationen/Übungen wären folgende anzuführen:

- Das BMSGPK und weitere Partner im Gesundheitsbereich nahmen unter anderem an der ENISA Übung „Cyber Europe 2022“ (https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2022)teil.
- Cybersicherheitsübungen mit weiteren EU-Mitgliedsstaaten, welche aus Cybersicherheitsgruppen des Gesundheitssektors bestehen.
- Nationale Gesundheitsarbeitsgruppen wie der Cybersicherheitsausschuss für eHealth; in diesem sind Bund und Länder vertreten

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 BMSGPK 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 zeitnah zu kompensieren.

Mit freundlichen Grüßen

Johannes Rauch

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2022-09-07T09:15:37+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.	2098721075
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: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-07T09:19:25+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.	