1617/AB
vom 22.06.2020 zu 1683/J (XXVII. GP)

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

Rudolf Anschober
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2020-0.260.153

Wien, 17.6.2020

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 1683 /J des Abgeordneten Hoyos-Trauttmansdorff betreffend Cyberangriffe auf Gesundheitseinrichtungen** wie folgt:

Frage 1: *Gab es seit Bekanntwerden der ersten Covid-19-Fälle in Österreich Cyberangriffe auf das BMSGPK?*

a. Wenn ja, wann genau?

b. Wenn ja, wurden diese Cyberangriffe frühzeitig erkannt, d.h. bevor der Angriff erfolgreich war?

i. Wenn ja, von wem und wie war dies möglich?

ii. Wenn nein, welcher Schaden ist dem BMSGPK durch diesen Angriff/diese Angriffe entstanden?

1. Wurden Gesundheitsdaten gestohlen? Welche? Wurden die betroffenen Personen kontaktiert?

iii. Warum wurde dies nicht öffentlich bekanntgegeben?

c. War es möglich, die Angreifer zu identifizieren?

i. Wenn ja, um wen handelt es sich?

Es gibt permanent Versuche, Handlungen gemäß § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) zu setzen. Eine öffentliche Bekanntgabe von Details würde aus sicherheitstechnischer Sicht dem evidenten Interesse an der Wahrung der wesentlichen äußeren und inneren Sicherheitsinteressen der Republik Österreich zuwiderlaufen, weswegen von einer näheren Beantwortung der Fragen Abstand genommen werden muss.

Frage 2: *Gab es seit Bekanntwerden der ersten Covid-19-Fälle in Österreich Cyberangriffe auf Gesundheitseinrichtungen?*

- *a. Wenn ja, wann genau?*
- *b. Wenn ja, um welche Gesundheitseinrichtungen handelt es sich?*
- *c. Wenn ja, wurden diese Cyberangriffe frühzeitig erkannt, d.h. bevor der Angriff erfolgreich war?*
  - *i. Wenn ja, von wem und wie war dies möglich?*
  - *ii. Wenn nein, welcher Schaden ist den jeweiligen Gesundheitseinrichtungen durch diesen Angriff/diese Angriffe entstanden?*
- *1. Wurden Gesundheitsdaten gestohlen? Welche? Wurden die betroffenen Personen kontaktiert?*
  - *iii. Warum wurde dies nicht öffentlich bekanntgegeben?*
- *d. War es möglich, die Angreifer zu identifizieren?*
  - *i. Wenn ja, um wen handelt es sich?*

Nein, bei den Sozialversicherungsträgern und dem Dachverband sind keine vermehrten Cyberangriffe auf Infrastruktur und Mitarbeiter (Bürotätigkeit, eigene Gesundheits-einrichtungen sowie IT-Infrastruktur) als vor dem Bekanntwerden der ersten Covid-19-Fälle zu verzeichnen.

Angemerkt wird, dass die Sicherheitssysteme täglich zahlreiche Angriffe abwehren. So werden beispielsweise von monatlich einlangenden ca. 20 Mio. E-Mails nur in etwa 2 Mio. durch die Sicherheitssysteme durchgelassen; 18 Mio. E-Mails werden als Spam, Pishing, Malware und Ähnliches identifiziert und abgewehrt.

Frage 3: *Wie hoch schätzt das BMSGPK das Risiko ein, dass das Ministerium während der Covid-19-Epidemie selbst Opfer von Cyberangriffen werden könnte?*

Eine Risikobewertung findet laufend im Rahmen der Cyberabwehrmechanismen der Bundesregierung statt und ist unabhängig von der derzeitigen Covid-19-Lage.

Frage 4: *Wie hoch schätzt das BMSGPK das Risiko ein, dass österreichische Gesundheitseinrichtungen während der Covid-19-Epidemie Opfer von Cyberangriffen werden könnten?*

Insbesondere durch Warnungen anderer Organisationen (z. B. Computer Emergency Response Team Austria [CERT.at], Cyber Security Center des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung [CSC] und andere) wurde das Risiko für den Bereich der Sozialversicherung zu Beginn der COVID-19-Epidemie als hoch eingestuft. Nach laufender Beobachtung der Situation konnte die Einstufung auf ein erhöhtes Risiko herabgestuft werden.

Frage 5: *Erging eine Warnung vor einer erhöhten Gefahr von Cyberangriffen während der Covid-19-Epidemie auf das Ministerium und Gesundheitseinrichtungen an das BMSGPK?*

a. Wenn ja, von welchen Stellen/Behörden/Einrichtungen/Organisationen?

b. Wenn ja, wie wurde vonseiten des BMSGPK auf diese Warnung reagiert?

Mein Ministerium erhält laufend von verschiedensten Quellen (CERTs, …) einschlägige Informationen und beobachtet die Lage laufend. Aus sicherheitstechnischer Sicht ist es nicht angezeigt, Details bekannt zu machen, da eine öffentliche Bekanntgabe dem evidenten Interesse an der Wahrung der wesentlichen äußeren und inneren Sicherheitsinteressen der Republik Österreich zuwiderlaufen würde.

Frage 6: *Welche Maßnahmen setzt das BMSGPK, um Cyberangriffe auf das Ministerium und Gesundheitseinrichtungen insbesondere während der Covid-19-Epidemie zu verhindern bzw. abzuwehren?*

Der Schutz der IKT-Systeme, als auch personenbezogener Daten hat für das BMSGPK eine hohe Priorität. IKT-Sicherheit wird als fortlaufender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur vorgenommen. Bestehende und neue IKT-Lösungen werden in Zusammenarbeit durch das GovCERT, als auch das Cyber Security Center des BMI fortlaufend evaluiert und Sicherheitslücken zeitnah adressiert. Systeme, die klassifizierte Informationen verarbeiten, werden im Rahmen eines Zulassungsprozesses auf deren Sicherheit überprüft.

Die Auswahl von IKT-Lösungen basiert auf konkreten Bedarfsanalysen, Sicherheitsanalysen und holistischen Betrachtungen des Application Lifecycles (Updates, Wartung, Ort der Datenverarbeitung und -speicherung, etc.).

Frage 7: *Wurden Krankenhäuser und Gesundheitseinrichtungen - wie in Tschechien – vom BMSGPK angewiesen, wie sie sich im Falle eines Cyberangriffes zu verhalten haben?*

a. Wenn ja, welche Anweisungen haben diese Einrichtungen erhalten?

b. Wenn nein, warum nicht? Ist es geplant, diesen Einrichtungen in Zukunft Anweisungen zu kommunizieren?

Bekanntermaßen bestehen zwischen dem Gesundheitssystem in Tschechien und jenem in Österreich Unterschiede. Ein Vergleich auf Basis einer APA-Meldung ist daher weder zweckmäßig noch zielführend.

Dem föderalen Gesundheitswesen Österreichs entsprechend wurde seit längerem im Rahmen der Bundeszielsteuerung als oberstes strategisches Gremium punkto Cybersicherheit im Gesundheitswesen der Cybersicherheitsausschuss für eHealth eingesetzt. Dieser ist mit den Akteuren der staatlichen Cyberabwehr bestens vernetzt. Diesem untergeordnet ist das operative Gremium der CISO AG, in der die Sicherheits-experten der Krankenanstalten und deren Verbünden, der Sozialversicherung und weiterer Akteure im Gesundheitswesen zusammenarbeiten und über aktuelle Bedrohungslagen informiert sind.

Im Falle aktueller Bedrohungen oder Angriffsvektoren sind sowohl Warnungen als auch das Erlassen situationsadäquater Handlungsanweisungen gewährleistet.

Mit freundlichen Grüßen

Rudolf Anschober

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2020-06-22T09:20:04+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	2020-06-22T09:25:02+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.	