1297/AB
vom 22.05.2020 zu 1305/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: 2020-0.203.262

Wien, 20.5.2020

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 1305/J des Abgeordneten Hoyos-Trauttmansdorff, Kolleginnen und Kollegen betreffend Rahmenvereinbarung Cybersecurity** wie folgt:

Frage 1:

- *Wurden seit Feststellung des Cyberangriffs auf das BMEIA vonseiten Ihres Ressorts sowie nachgelagerten Stellen oder Behörden spezielle Maßnahmen getroffen, um die eigenen IKT-Systeme besser abzusichern?*
  a. Wenn ja, welche? Bitte um Auflistung nach Maßnahmen und angefallenen Kosten.
  b. Wenn nein, warum nicht?

Im Zuge der Vorfälle im BMEIA wurden durch den interministeriellen Einsatzstab sowohl laufende Risikoeinschätzungen als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert. Weiters wurden die jeweiligen kritischen Systeme engmaschig überprüft und Maßnahmen ergriffen, eine Kompromittierung weiterer Systeme hintanzuhalten. Diese Maßnahmen waren bzw. wurden zeitnah durch die verantwortlichen Techniker und Technikerinnen des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK) umgesetzt.

Frage 2:

- *Sind bereits vor Feststellung des Cyberangriffs auf das BMEIA vonseiten Ihres Ressorts sowie nachgelagerten Stellen oder Behörden Maßnahmen getroffen worden, um die eigenen IKT-Systeme besser abzusichern?*
  a. Wenn ja, welche? Bitte um Auflistung nach Jahr, Maßnahmen und angefallenen Kosten.
  b. Wenn nein, warum nicht?

IKT-Sicherheit ist ein fortlaufender Prozess, bei dem der Aktualisierung und Absicherung der Systeme höchster Stellenwert zugesprochen wird. Dies wird vor allem durch Analysetools im Bereiche Update und Patch-Management erreicht. Dadurch können alle Systeme auf höchstem Sicherheitsniveau gehalten werden. Neue Anwendungen werden und wurden im BMSGPK auf Sicherheit geprüft, bevor sie zum Einsatz kommen. Es wird jede Anwendung und Hardware, die im BMSGPK verwendet wird, wiederholt bewertet. Dies wird in einem vorgegebenen ISMS-Prozess umgesetzt und dokumentiert. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur 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.

Es kann in diesem Zusammenhang auch auf das Projekt Cyber-Sicherheitsstrategie, Ermittlung „wichtiger Dienste“ und Notfallhandbuch hingewiesen werden. In diesem Projekten wurden Mindestsicherheitsstandards festgelegt, der Informationsaustausch abgestimmt, Sensibilisierungsinitiativen gestartet, die IKT-Sicherheitskompetenz gestärkt und die Cyber-Notfallvorsorge geplant. Die Projekte erfüllen die Anforderungen des NIS-Gesetzes, da

- alle Anwendungen identifiziert und bewertet und ihre Sicherheit geprüft wurden,
- Maßnahmen, die eine Kompromittierung der Systeme hintanzuhalten ergriffen wurden,
- sowie für wichtige Dienste Notfallpläne erstellt wurden.
- Darüber hinaus finden in enger Zusammenarbeit mit dem Bundesrechenzentrum permanent Auswertungen und forensische Analysen statt.

Von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018, muss ich im Hinblick auf die Sicherung der Effektivität dieser Maßnahmen Abstand nehmen.

Frage 3:

- *Welche Beschaffungen zur Verbesserung der Sicherheit der eigenen IKT-Systeme wurden seit Feststellung des Cyberangriffs auf das BMEIA vonseiten Ihres Ressorts bzw. nachgelagerten Stellen oder Behörden getätigt?*
  a. Bestehen Rahmenvereinbarungen bezüglich dieser Beschaffungen?
  i. Wenn ja, welche?
  ii. Zwischen welchen Parteien wurden diese Rahmenvereinbarungen geschlossen?
  iii. Welche Leistungen wurden in diesen Rahmenvereinbarungen vereinbart?
  iv. War es dem/den Vertragspartner/n Ihres Ressorts bzw. nachgelagerten Stellen oder Behörden möglich, alle vereinbarten Leistungen selbst zu erbringen?
  v. Mussten Leistungen vom Auftragnehmer in Kooperation mit Dritten erbracht werden?

1. Wenn ja, mit welchen Kooperationspartnern?
2. Welche Leistungen wurden von den Kooperationspartnern erbracht? Bitte um separate Aufschlüsselung nach Kooperationspartner.
vi. Welche Stundensätze wurden von den Unternehmen, die nach Bekanntwerden des Cyberangriffs auf das BMEIA Leistungen erbrachten, veranschlagt? Wie hoch waren die Gesamtkosten? Bitte um separate Aufschlüsselung der Stundensätze und Gesamtkosten pro Unternehmen.
b. Gab es hier Ausschreibungen laut Bundesvergabegesetz?
i. Wenn ja, für welche Leistungen?
ii. Wenn nein, warum nicht? Bitte um Übermittlung der vergaberechtlichen Bestimmungen.

Wie alle anderen Ressorts wurde auch das BMSGPK informiert, dass unter Federführung des Bundeskanzleramtes und unter Mitwirkung der Finanzprokuratur von der Bundesrechnungszentrum GmbH auf Grundlage des Dringlichkeitstatbestands gemäß § 25 Z 4 des Bundesvergabegesetzes für Verteidigung und Sicherheit 2012, BGBl. I Nr. 10/2012, mit einem geeigneten Anbieter eine Rahmenvereinbarung abgeschlossen wurde, da eine unmittelbare und unverzügliche Bewältigung und Beseitigung der „Cyberattacke“ zwingend notwendig war.

Zum eigenständigen Abruf von Leistungen aus der Rahmenvereinbarung sind

(i) die Bundesrechenzentrum GmbH,
(ii) alle Bundesministerien sowie deren nachgeordneten Bereiche (Ämter und Dienststellen) und
(iii) jene Rechtsträger, an denen der Bund Anteile hält und die der Kontrolle durch den Rechnungshof unterliegen, berechtigt.

Da die Bekanntgabe technischer Details der zur Bekämpfung einer Cyberattacke und zur Beseitigung ihrer Auswirkungen erforderlichen Maßnahmen auch zu einem späteren Zeitpunkt den verfolgten Zweck gefährden könnten, sind der Inhalt der abgeschlossenen Rahmenvereinbarung sowie die bereits erbrachten Leistungen strikt vertraulich zu behandeln.

Sämtliche mit der „Cyberattacke“ unmittelbar in Verbindung stehenden Leistungen wurden daher entsprechend den Erfordernissen klassifiziert.
Es erscheint daher nicht angezeigt, technische Details der Rahmenvereinbarung und der bereits erbrachten Leistungen nachfolgend bekannt zu machen, da eine öffentliche Bekanntgabe dem evidenten Interesse an der Wahrung der wesentlichen äußeren und inneren Sicherheitsinteressen der Republik Österreich zuwiderlaufen würde.

Damit unterliegen diese Informationen auch der Amtsverschwiegenheit, welche im Rahmen der parlamentarischen Anfragebeantwortung zu wahren ist, weswegen von einer näheren Beantwortung der Fragen Abstand genommen werden muss.

Darüberhinausgehend hat das BMSGPK zur weiteren Steigerung der IKT-Sicherheit mehrere Projekte in Planung und Umsetzung.

Die Themenfelder zur Weiterentwicklung der IKT-Sicherheit im BMSGPK reichen von weiteren Awarenessmaßnahmen über Aktualisierung von Richtlinien bis zum Pilotprojekt eines neuen umfassenden ISMS-Systems.

Frage 4:

- *Welche Beschaffungen zur Verbesserung der Sicherheit der eigenen iKT-Systeme wurden vor dem Cyberangriff auf das BMEIA vonseiten ihres Ressorts bzw. nachgelagerten Stellen oder Behörden getätigt?*
  a. Bestehen bzw. bestanden Rahmenvereinbarungen bezüglich dieser Beschaffungen?

i. Wenn ja, welche?
ii. Zwischen welchen Parteien wurden diese Rahmenvereinbarungen geschlossen?
iii. Welche Leistungen wurden in diesen Rahmenvereinbarungen vereinbart?
iv. War es dem/den Vertragspartner/n ihres Ressorts bzw. nachgelagerten Stellen oder Behörden möglich, alle vereinbarten Leistungen selbst zu erbringen?
v. Mussten Leistungen vom Auftragnehmerin Kooperation mit Dritten erbracht werden?
1. Wenn ja, mit welchen Kooperationspartnern?
2. Welche Leistungen wurden von den Kooperationspartnern erbracht? Bitte um separate Aufschlüsselung nach Kooperationspartner.
vi. Welche Stundensätze wurden von diesen Unternehmen veranschlagt? Wie hoch waren die Gesamtkosten? Bitte um separate Aufschlüsselung der Stundensätze und Gesamtkosten pro Unternehmen.

b. Gab es hier Ausschreibungen laut Bundesvergabegesetz?
i. Wenn ja, für welche Leistungen?
ii. Wenn nein, warum nicht? Bitte um Übermittlung der vergaberechtlichen Bestimmungen.

Ich verweise auf die Ausführungen in Frage 3.

Frage 5:

- *Welche internen Abteilungen sind für die iKT-Sicherheit ihres Ministeriums zuständig?*
  a. Wie viele Mitarbeiter_innen hat/haben diese Abteilung/en?
  b. Auf welcher Rechtsgrundlage basieren/basierten diese Arbeitsverhältnisse? Um Angabe der Zahl der Beschäftigten nach Art der Rechtsverhältnisse wird ersucht:
  i. Beamtendienstverhältnis
  ii. Vertragsbedienstetenverhältnis
  1. befristet
  2. unbefristet
  iii. Freie Dienstnehmerinnen
  iv. Werkvertrag
  v. Arbeitskräfteüberlassung
  vi. Sonstige
  c. Wie viele dieser Personen sind/waren mit spezifischen "Cybersecurity-Tätigkeiten" im technischen Sinn befasst?

Es darf in diesem Zusammenhang auf die Geschäftseinteilung des BMSGPK verwiesen werden. Die Mitarbeiter und Mitarbeiterinnen der iKT-Sicherheit arbeiten in einem sensiblen Bereich und müssen vor kriminellen Aktivitäten und nachrichtendienstlicher Ausspähung geschützt werden. Daher muss von einer konkreten Nennung von Anzahl und Einstufung Abstand genommen werden.

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	2020-05-22T08:46:15+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	2020-05-22T08:49:15+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.	