1300/AB
vom 22.05.2020 zu 1301/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.250.618

Wien, am 22. Mai 2020

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 25. März 2020 unter der Nr. **1301/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Rahmenvereinbarung Cybersecurity“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur 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 Vorfallsbehandlung im BMEIA wurden durch den interministeriellen Einsatzstab sowohl laufende Risikoeinschätzungen, als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert.
Alle diese Maßnahmen wurden zeitnah durch die verantwortlichen Techniker im Bundesministerium für Inneres umgesetzt. Weiters wurden die jeweiligen kritischen Systeme engmaschig überprüft und Maßnahmen ergriffen eine Kompromittierung weiterer Systeme hintanzuhalten. Darüber hinaus wurde durch das BMI der strategische

Lessons Identified/Lessons Learned Prozess durchgeführt, welcher basierend auf den Erfahrungen des gesamtstaatlichen Krisenmanagements strategische Handlungsempfehlungen vorlegt.

Zur 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 wird als fortlaufender Prozess verstanden. 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.

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

Zu den Fragen 3 und 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 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 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.*

- *Welche Beschaffungen zur Verbesserung der Sicherheit der eigenen IKTSysteme wurden vor dem Cyberangriff aul das BMEIA vonseiten Ihres Ressors 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 Ressors bzw. nachgelagerten Stellen oder Behörden möglich, alle vereinbaren Leistungen selbst zu erbringen?*

v. *Mussten Leistungen vom Aufragnehmer 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 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?*

iii. *Wenn ja, für welche Leistungen?*

iv. *Wenn nein, warum nicht? Bitte um Übermittlung der vergaberechtlichen Bestimmungen.*

Durch das BMEIA wurde im Verlauf der Incident-Response spezifische Software zur Unterstützung der Vorfallsbehandlung beschafft. Basierend auf den Ergebnissen der Vorfallsuntersuchung erlaubt die beschaffte Software das Scannen von komplexen IT-Systemen auf spezifische Schadsoftware. Im Cyberkrisenmanagement-Koordinationsauschuss wurde durch die dort vertretenen Ministerien der zeitnahe Bedarf

an der Software artikuliert, um eine Infektion der eigenen Netze schnellstmöglich ausschließen zu können.

Als Begleitmaßnahme wurde das BMI informiert und unter Federführung des Bundeskanzleramtes 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, 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 gleichfalls 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.

Zur Frage 5:

- *Welche internen Abteilungen sind für die IKT-Sicherheit Ihres Ministeriums zuständig?*
  a. Wie viele Mitarbeiterinnen 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:

v. Beamtendienstverhältnis

vi. Vertragsbedienstetenverhältnis

1. befristet
2. unbefristet

vii. Freie Dienstnehmerinnen

viii. Werkvertrag

ix. Arbeitskräfteüberlassung

x. Sonstige

c. Wie viele dieser Personen sind/waren mit spezifischen "Cybersecurity Tätigkeiten" im technischen Sinn befasst?

Es darf in diesem Zusammenhang auf die Geschäftseinteilung 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.

Karl Nehammer, MSc

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2020-05-22T10:53:14+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1710479
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-05-22T10:55:13+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.	