1309/AB
vom 25.05.2020 zu 1308/J (XXVII. GP)

Bundesministerium
Kunst, Kultur,
öffentlicher Dienst und Sport

bmkoes.gv.at

Mag. Werner Kogler
Vizekanzler
Bundesminister für Kunst, Kultur,
öffentlichen Dienst und Sport

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.203.935

Wien, am 25. Mai 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 25. März 2020 unter der Nr. **1308/J** an mich eine schriftliche parlamentarische Anfrage betreffend Rahmenvereinbarung Cybersecurity gerichtet.

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

Zu 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 Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) wurden durch den interministeriellen Einsatzstab sowohl laufende Risikoeinschätzungen als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert.

Diese Maßnahmen waren bzw. wurden zeitnah durch die verantwortlichen Technikerinnen und Techniker des Bundesministeriums für Kunst, Kultur, öffentlichen Dienst und Sport (BMKÖS) umgesetzt. Ich ersuche um Verständnis, dass aus Sicherheitsgründen keine näheren Details zu den Maßnahmen und damit auch keine Kostenangaben erfolgen können.

Ein bestehendes ISMS-System (Information Security Management System) bewertet jede Anwendung und Hardware, die im Ressort verwendet wird. Darüber hinaus finden in enger Zusammenarbeit mit dem Bundesrechenzentrum Auswertungen und forensische Analysen statt.

Darüber hinaus darf auf die Beantwortung des Herrn Bundeskanzlers zu der an ihn gerichteten parlamentarischen Anfrage Nr. 1299/J verwiesen werden.

Zu 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. Neue Anwendungen werden und wurden im BMKÖS auf Sicherheit geprüft, bevor sie zum Einsatz kommen. Dies wird in einem vorgegebenen ISMS-Prozess umgesetzt und dokumentiert. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur vorgenommen. Auch hier darf ich um Verständnis bitten, dass aus Sicherheitsgründen keine näheren Ausführungen zu den Maßnahmen und damit auch keine Kostenangaben möglich sind.

Im Übrigen darf auf die Beantwortung des Herrn Bundeskanzlers zu der an ihn gerichteten parlamentarischen Anfrage Nr. 1299/J verwiesen werden.

Zu den Fragen 3 und 4:

- *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.*

- *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.*

Unter Federführung des Bundeskanzleramtes und unter Mitwirkung der Finanzprokuratur wurde 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. Ich darf diesbezüglich auf die Beantwortung des Herrn Bundeskanzlers zu der an ihn gerichteten parlamentarischen Anfrage Nr. 1299/J verweisen.

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

Die Bestimmungen des Vergaberechts finden auch im Bereich Cybersecurity Anwendung.

Zu 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 Dienstnehmer/innen*

iv. *Werkvertrag*

v. *Arbeitskräfteüberlassung*

vi. *Sonstige*

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

Im Bereich „IT-Sicherheit, IKT-Infrastruktur und –Betrieb“ sind im BMKÖS zehn Personen tätig, es darf in diesem Zusammenhang auf die Geschäftseinteilung verwiesen werden: https://www.bmkoes.gv.at/dam/jcr:19b58635-473d-47b5-a6ea-69d81a79c984/Pro_Gesch%C3%A4ftseinteilung_29.1.2020.pdf

Die Mitarbeiterinnen und Mitarbeiter der IKT-Sicherheit arbeiten in einem sensiblen Bereich und müssen vor kriminellen Aktivitäten und nachrichtendienstlicher Ausspähung geschützt werden, es muss daher von einer konkreten Nennung von Anzahl und Einstufung Abstand genommen werden.

Mag. Werner Kogler

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR KUNST, KULTUR, ÖFFENTLICHEN DIENST UND SPORT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport
	Datum/Zeit	2020-05-25T08:47:05+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.	2099471880
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-05-25T08:49:48+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.	