1299/J
vom 25.03.2020 (XXVII. GP)

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen an den Bundeskanzler

betreffend Maßnahmen Cybersecurity

Am 4. Jänner 2020 hatte das Außenministerium (BMEIA) einen gezielten und hochprofessionellen Cyberangriff gemeldet, der am 13. Februar 2020 offiziell als beendet erklärt wurde. Laut eines FM4-Berichts sei es den Angreifer_innen zwei Tage lang möglich gewesen, unbemerkt Zugriff auf die E-Mail-Server des BMEIA zu erlangen, Passwörter von Konten zu sammeln und Korrespondenzen zu exfiltrieren. Dass die Attacke in der Frühphase entdeckt wurde, habe laut FM4 weniger mit Österreichs Cyberabwehr-Strategie als mit "einer Kombination aus günstigen Umständen, der Umsicht und Improvisationsfähigkeit der beteiligten Techniker sowie einem technischen Husarenstreich gegen die Kommunikation der Schadsoftware im Netz des BMEIA mit den externen Command-Control-Servern" zu tun. (https://fm4.orf.at/stories/2998771/)

In den Systemen des BMEIA laufen eine Reihe vertraulicher und höchst sensibler Daten zusammen, angefangen von konsularischen persönlichen Daten von Österreicher_innen über vertrauliche EU-Dokumente bis hin zu heiklen außenpolitischen Dokumenten. In den falschen Händen können diese Dokumente dem Staat, seinen internationalen Partner_innen und seinen Bürger_innen massiven Schaden zufügen.

Der Cyberangriff auf das BMEIA offenbart ernstzunehmende Schwachstellen in der Sicherheits- bzw. Verteidigungsarchitektur der Republik und beeinträchtigt die Integrität und Funktionsfähigkeit einer staatlichen Behörde. Es ist nicht auszuschließen, dass in Zukunft auch andere Ministerien Ziel eines solchen Angriffs werden. Es ist daher fraglich, welche Maßnahmen sowohl unmittelbar nach der Entdeckung des Cyberangriffs als auch vor der Attacke ergriffen wurden, um die IKT-Sicherheit Ihres Ressorts zu erhöhen.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Wurden seit Feststellung des Cyberangriffs auf das BMEIA vonseiten des Bundeskanzleramts 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?
2. Sind bereits vor Feststellung des Cyberangriffs auf das BMEIA vonseiten des Bundeskanzleramts 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?

3. Welche Beschaffungen zur Verbesserung der Sicherheit der eigenen IKT-Systeme wurden seit Feststellung des Cyberangriffs auf das BMEIA vonseiten des Bundeskanzleramts sowie 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 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.
4. Welche Beschaffungen zur Verbesserung der Sicherheit der eigenen IKT-Systeme wurden vor dem Cyberangriff auf das BMEIA vonseiten des Bundeskanzleramts sowie 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.

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?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-03-25T13:36:18+01:00
	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.	