1315/J XXVII. GP

Eingelangt am 26.03.2020

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen an die Bundesministerin für Digitalisierung und Wirtschaftsstandort

betreffend Rahmenvereinbarung Cybersecurity Bundeskanzleramt

Am 4. Jänner 2020 hatte das Außenministerium 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 Außenministeriums 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 Außenministeriums 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 Außenministerium offenbart ernstzunehmende Schwachstellen in der Sicherheits- bzw. Verteidigungsarchitektur der Republik und beeinträchtigt die Integrität und Funktionsfähigkeit einer staatlichen Behörde. Es ist daher fraglich, welche Maßnahmen unmittelbar nach der Entdeckung des Cyberangriffs ergriffen wurden, um die IKT-Sicherheit des BMEIA möglichst rasch wiederherzustellen.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Welche Schritte wurden ab dem Zeitpunkt der Entdeckung des Cyberangriffs auf das BMEIA vonseiten des BMDW bzw. des Bundesrechenzentrums gesetzt, um die Sicherheit der IT-Systeme des BMEIA wiederherzustellen?
2. Welche Beschaffungen wurden ab dem Zeitpunkt der Entdeckung des Cyberangriffs auf das BMEIA vonseiten des BMDW bzw. des Bundesrechenzentrums 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 des BMDW bzw. des Bundesrechenzentrums möglich, alle vereinbarten Leistungen selbst zu erbringen?
        v. Mussten Leistungen vom Auftragnehmer in Kooperation mit Dritten erbracht werden?
            1. Waren/sind folgende Unternehmen unter diesen Kooperationspartnern? (1) SEC Consult GmbH, (2) Ikarus Security Software GmbH
            2. Welche Leistungen wurden von den Kooperationspartnern erbracht? Bitte um getrennte Darstellung 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 getrennte Darstellung 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.