1224/J
vom 05.03.2020 (XXVII. GP)

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an den Bundesministerin für Landesverteidigung

betreffend Personelle Ausstattung der Cyberdefence

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 einer 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 Partnern 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. Österreich benötigt besser koordinierte staatliche Strukturen, um Cyberangriffe frühzeitig erkennen und abwehren zu können. Derzeit sind die Kompetenzen jedoch zwischen dem BVT im Innenministerium und dem Ministerium für Landesverteidigung aufgeteilt. Im Computer Emergency Response Team (Cert) sind Expert_innen von BMI, BMLV, dem Bundeskanzleramt und IT-Expert_innen aus der privaten Szene verbunden. In Anbetracht der vielen düsteren Prognosen von Expert_innen - u.a. des renommierten Kaspersky Labs - wonach die Attacken auf unsere IT-Systeme immer ausgefeilter und spezifischer werden, ist es für den Schutz von kritischen Institutionen und Infrastrukturen sowie die Sicherheit der Bevölkerung unerlässlich, effiziente staatliche Strukturen zu schaffen, um die Resilienz Österreichs gegen Cyberattacken zu erhöhen.

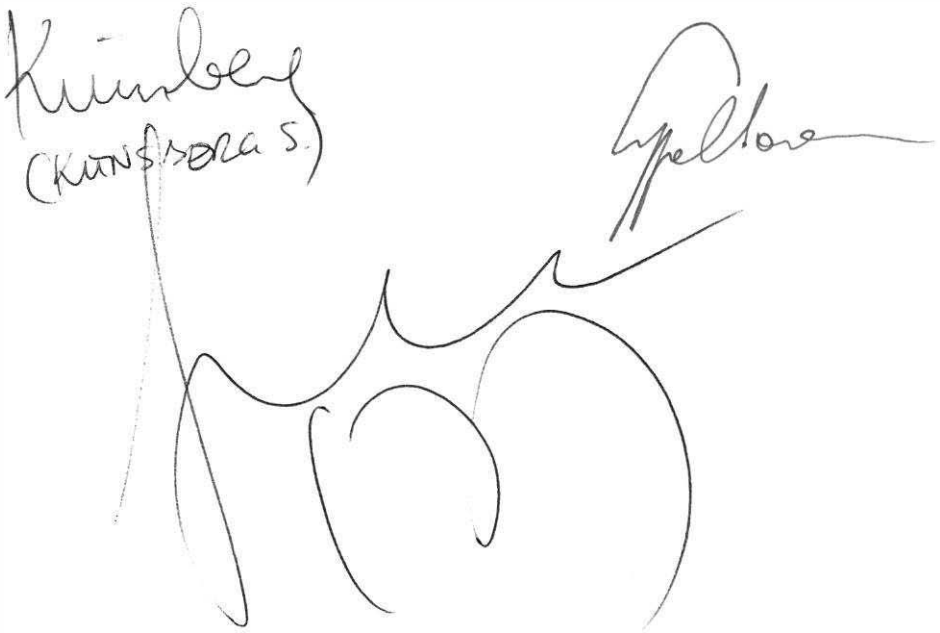
Am 28.2.2020 sprach der Nationale Sicherheitsrat in seiner Sitzung gegenüber der Bundesregierung die Empfehlung aus, die allzeitige Verfügbarkeit von einsatzfähigen mobilen Elementen seitens des Bundesheeres sowie des Innenministeriums, jeweils mit ausreichender personeller und technischer Ausstattung und Know-How sicherzustellen.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Wie viele Personen sind mit Stichtag der Anfragebeantwortung in der Abteilung Cyberdefence im Kommando Führungsunterstützung beschäftigt?
2. Auf welcher Rechtsgrundlage basierten diese Arbeitsverhältnisse: Um Angabe der Zahl der Beschäftigten nach Art der Rechtsverhältnisse wird ersucht:
    a. Beamtendienstverhältnis
    b. Vertragsbedienstetenverhältnis
        i. befristet
        ii. unbefristet
    c. Freie Dienstnehmer
    d. Werkvertrag
    e. Arbeitskräfteüberlassung
    f. Sonstige
3. Wie viele dieser Personen waren im engeren Sinne mit "Cyberdefence-Tätigkeiten" im technischen Sinne befasst?
4. Wie viele externe Dienstleister_innen waren seit dem Jahr 2017 sowie zum Stichtag der Anfragebeantwortung vom BMLV in Zusammenhang mit "Cyberdefence-Aufgaben" beauftragt? (Um getrennte Darstellung nach Jahr wird ersucht.)
    a. Welche Dienstleistungen wurden dabei in Anspruch genommen?
    b. Warum war es notwendig, diese Dienstleistungen von externen Dienstleister_innen erbringen zu lassen?
        i. Konnten diese Tätigkeiten von Mitarbeiter_innen des BMLV nicht aus eigenem durchgeführt werden?
            1. Wenn nein, warum nicht?
5. Wie hat sich der Personalstand der Cyberdefence seit deren Einrichtung entwickelt? (Um Angabe der Zahl der Beschäftigten nach Art der Rechtsverhältnisse analog Frage 1 wird ersucht.)
6. Wie viele Planstellen waren seit Einrichtung der Cyberdefence jeweils vorgesehen? (Bitte um getrennte Darstellung nach Jahr.)
7. Wie hat sich die Anzahl der Planstellen seit der Einrichtung entwickelt? (Bitte um getrennte Darstellung nach Jahr.)
    a. Wurde die Anzahl der Planstellen reduziert?
        i. Wenn ja, wie wird dies begründet?
8. Beabsichtigen Sie die personelle wie technische Ausstattung der Cyberdefence in Zukunft zu verstärken?
    a. Wenn ja, wie und in welchem Ausmaß?
9. Wie viele Planstellen sind für die kommenden Jahre vorgesehen? (Bitte um getrennte Darstellung nach Jahr.)
10. Halten Sie die derzeitige organisatorische Eingliederung der Cyberdefence-Einheit für sinnvoll?
    a. Wenn ja, weshalb?
    b. Wenn nein, inwiefern nicht?
11. Werden Sie die "Organisationsreform" 2018 rückgängig machen, in der das Kommando Cyberdefence als eigenes Kommando aufgelöst wurde und in die Streitkräftebasis eingegliedert wurde?
    a. Wenn ja, inwiefern?
    b. Wenn nein, weshalb nicht?

12. Trifft es zu, dass es in im Zusammenhang dieser "Organisationsreform" zu einem einem beträchtlichen Personalabgang im Bereich der IT-Fachkräfte der Abteilung kam?
    a. Wenn ja, in welchem Ausmaß kam es zu Personalabgängen von IT-Fachkräften?
    b. Wenn ja, was war der Grund für diese Personalabgänge?
13. Welche organisatorischen Maßnahmen planen Sie für die Cyberdefence-Einheit?
14. Welche Qualifikationen müssen Bewerber_innen im Rahmen von Stellenausschreibungen der Cyberdefence vorweisen können? (Bitte um Erläuterung für die jeweiligen Aufgabengebiete.)
15. Wie hoch waren die Gesamtkosten (inkl. Überstunden und sonstige Entgeltbestandteile) pro Jahr seit 2016, die sich aus der Beschäftigung aller Mitarbeiter_innen der Cyberdefence ergaben?
16. Wechselten Mitarbeiter_innen des Kommandos Cyber Defence des BMLV nach dessen Umbau ins CSC?
    a. Wenn ja, um wie viele Personen handelte es sich hierbei und welche Aufgabenbereiche waren ihnen im Kommando Cyber Defence zugeordnet?
17. Welche konkreten Maßnahmen planen Sie wann in Entsprechung der Empfehlungen des Nationale Sicherheitsrates vom 28.2.2020 zu treffen?



REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-03-05T15:56:26+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.	