645/J
vom 24.01.2020 (XXVII. GP)

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an die Bundesministerin für Landesverteidigung

betreffend Cyberattacke auf das Außenministerium

Seit 3. Jänner 2020 ist bekannt, dass ein gezielter und hochprofessioneller Cyberangriff auf das Österreichische Außenministerium stattfindet.

In den IT-Systemen eines der Schlüsselressorts der Republik operiert seit geraumer Zeit ein feindliches System, hinter dem ein staatlicher bzw. staatsnaher Akteur zu stehen scheint.

(https://fm4.orf.at/stories/2997349/; https://futurezone.at/netzpolitik/warum-der-cyberangriff-auf-das-aussenministerium-so-lange-dauert/400733796)

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 Österreich, seinen internationalen Partnern und seinen Bürger_innen massiven Schaden zufügen.

Der Angriff auf das Außenministerium offenbart ernstzunehmende Schwachstellen in der Sicherheits- bzw. Verteidigungsarchitektur der Republik und beeinträchtigt die Integrität und Funktionsfähigkeit einer staatlichen Behörde und schadet damit der nationalen Sicherheit.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Welche Information oder Erkenntnisse haben Sie über:
    a. die **Urheberschaft** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
        i. Handelt es sich um einen staatlichen/staatsnahen Akteur oder nicht?
            1. Wenn ja, welcher Staat steht hinter dem Angriff?
            2. Welche Informationen haben Sie, um das zu bestätigen bzw. auszuschließen?
    b. den **zeitlichen Beginn** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
        i. Seit wann genau ist das IT-System des Außenministeriums durch die Schadsoftware kompromittiert?
            1. Erst seit 3. Jänner 2020 oder schon davor?
                a. Seit welchem Jahr?
        ii. Aufgrund welcher konkreten IT-Vorgänge wurde der Angriff im Ministerium wann genau (Datum) entdeckt?
    c. die **Art und Vorgangsweise** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
        i. Handelt es sich um einen "Schläfervirus/Schläfersoftware"?

d. die **Dauer** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
    i. Ist der Angriff zum Zeitpunkt der Anfragebeantwortung beendet?
        1. Wenn ja, seit wann ist der Angriff beendet?
        2. Wenn nein, wann kann mit einer erfolgreichen Abwehr gerechnet werden?
e. das **Ziel** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
f. den **Umfang** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
    i. Wurden auch Backups des Ministeriums durch die Schadsoftware kompromittiert?
        1. Wenn ja, inwiefern?
        2. Wenn nein, wie kann das ausgeschlossen werden?
g. den **Gegenstand** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
h. die **Hintergründe** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
i. die **betroffenen Daten/Dokumente** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
    i. wurden Daten/Informationen aus den Systemen abgezogen?
        1. wenn ja, welche Daten/Informationen in welchem Ausmaß?
j. die verursachten **Schäden (Schadenshöhe sofern bereits eruierbar)** des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)

2. Haben Sie Kenntnis davon, ob auch die **Systeme anderer Bundesbehörden** durch gleiche oder ähnliche Schadsoftware kompromittiert sind? (Um detaillierte Erläuterung wird ersucht.)
    a. Wenn ja, welche?
    b. Kann ausgeschlossen werden, dass auch die Systeme anderer Bundesbehörden durch gleiche oder ähnliche Schadsoftware kompromittiert sind?
3. Welche konkreten **Abwehrmaßnahmen** und Schritte wurden jeweils wann genau zur Analyse, Bekämpfung und Abwehr des Angriffes von wem getroffen und mit welchem konkreten Ergebnis/Erfolg? (Um detaillierte Erläuterung wird ersucht.)
4. Welche (Zeit-)**Aufwendungen** sind Ihrem Ressort durch die Analyse, Bekämpfung und Abwehr des Angriffes bisher entstanden? (Um detaillierte Erläuterung wird ersucht.)
5. Welche bezifferbaren **Kosten** sind Ihrem Ressort durch die Analyse, Bekämpfung und Abwehr des Angriffes bisher entstanden? (Um detaillierte Erläuterung wird ersucht.)
6. Welche Stellen und wie viele Personen Ihres Ressort sind bzw. waren in die Analyse, Bekämpfung und Abwehr des Angriffes in welcher Weise und wann jeweils eingebunden?
7. Welche **externen Experten bzw. Unternehmen** wurden für die Analyse, Bekämpfung und Abwehr des Angriffes in welcher Weise und wann jeweils zugezogen? (Um detaillierte Erläuterung wird ersucht.)
    a. Verfügt Ihr Ressort über einen Rahmenvertrag mit externen Exptert_innen/Unternehmen für die rasche Bewältigung von IT-Vorfällen dieser Art?
        i. Wenn ja, seit wann mit welchen Expert_innen/Unternehmen?
        ii. Wenn nein, weshalb nicht?

8. Welche **konkreten Maßnahmen** planen Sie, um die Verteidigungsfähigkeit und Sicherheit der Republik im Cyberbereich zu verbessern? (Um detaillierte Erläuterung wird ersucht.)

Sollte eine detaillierte Beantwortung einzelner Fragen aus Geheimhaltungsgründen nicht möglich sein, so wird dennoch um eine Beantwortung mit möglichst hohem Informationsgehalt im Sinne des parlamentarischen Interpellationsrechts ersucht. Allenfalls ersuchen die Abgeordneten um eine Beantwortung in klassifizierter Weise nach dem Bundesgesetz über die Informationsordnung des Nationalrates und des Bundesrates - InfOG.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-01-24T14:52:01+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.	