

 Bundeskanzleramt

bundeskanzleramt.gv.at

Sebastian Kurz
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2020-0.053.454

Wien, am 24. März 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 24. Jänner 2020 unter der Nr. **647/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberattacke auf das Außenministerium“ gerichtet.

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

Zu Frage 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.)

Ich darf auf die Beantwortung der parlamentarischen Anfrage Nr. 646/J vom 24. Jänner 2020 durch den Bundesminister für europäische und internationale Angelegenheiten verweisen.

Zu Frage 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?

Ich darf auf die Beantwortung der parlamentarischen Anfrage Nr. 643/J vom 24. Jänner 2020 durch den Bundesminister für Inneres verweisen.

Zu den Fragen 3 bis 8:

- 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.)
- Welche (Zeit-) **Aufwendungen** sind Ihrem Ressort durch die Analyse, Bekämpfung und Abwehr des Angriffes bisher entstanden? (Um detaillierte Erläuterung wird ersucht.)
- Welche bezifferbaren **Kosten** sind Ihrem Ressort durch die Analyse, Bekämpfung und Abwehr des Angriffes bisher entstanden? (Um detaillierte Erläuterung wird ersucht.)
- 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?
- 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 Expert_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?
- Welche **konkreten Maßnahmen** planen Sie, um die Verteidigungsfähigkeit und Sicherheit der Republik im Cyberbereich zu verbessern? (Um detaillierte Erläuterung wird ersucht.)

Es werden spezifische Sicherheitsvorkehrungen zum Schutz der IKT-Systeme des Ressorts gegen Angriffe im Sinne des § 118a StGB eingesetzt. Ich ersuche Sie aber um Verständnis, dass es gerade im Hinblick auf die Effektivität dieser Maßnahmen nicht möglich ist, diese im Detail öffentlich mitzuteilen.

Sebastian Kurz

