683/AB
vom 24.03.2020 zu 643/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.141.145

Wien, am 23. März 2020

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 24. Jänner 2020 unter der Nr. **643/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberattacke auf das Außenministerium“ gerichtet.

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

Zur 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 Schad-software 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 **Zie**l 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.)*

Es darf auf die Stellungnahme des zuständigen Bundesministers für Europäische und internationale Angelegenheiten vom 22. Jänner 2020 im Plenum des Nationalrates sowie auf seine Beantwortung der parlamentarischen Anfrage Nr. 646/J vom 22. Jänner 2020 verwiesen werden, sowie auf die Sitzungen des ständigen Unterausschuss Inneres und den Nationalen Sicherheitsrat.

Zur 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?*

Derzeit liegen keine Indizien vor, dass auch Systeme anderer Bundesbehörden durch gleiche oder ähnliche Schadsoftware kompromittiert wurden.

Hierzu darf ausgeführt werden, dass eine Infektion von Systemen niemals zu 100% ausgeschlossen werden kann. Die technischen Indikatoren für eine potentielle Infektion durch die vorliegende Schadsoftware wurden den Einrichtungen des Bundes übermittelt. Außerdem wurden Maßnahmen zur Erhöhung der Sicherheit der technischen Systeme den Bundesministerien empfohlen, um potentielle Angriffe frühzeitig zu erkennen.

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 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?*

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

Es wurden und werden auch weiterhin spezifische Sicherheitsvorkehrungen zum Schutze der IKT-System des Ressorts gegen Angriffe iSd § 118a Strafgesetzbuch eingesetzt. Ich ersuche aber um Verständnis, dass gerade im Hinblick auf die Effektivität dieser Maßnahmen es nicht möglich ist, sie im Detail öffentlich mitzuteilen.

Dessen ungeachtet darf angemerkt werden, dass das Bundeskanzleramt eine Rahmenvereinbarung für alle Ressorts abgeschlossen hat - somit auch für das Bundesministerium für Inneres. Hinsichtlich der geplanten Maßnahmen, welche die Verteidigungsfähigkeit und Sicherheit der Republik Österreich im Cyberbereich verbessern soll, darf auf das Regierungsprogramm, insbesondere auf den Punkt „*Cybersicherheit und Digitalisierung*“, verwiesen werden.

Karl Nehammer, MSc

	Datum/Zeit	2020-03-24T15:05:39+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1710479
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-03-24T15:07:20+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.	