685/AB
vom 24.03.2020 zu 646/J (XXVII. GP)

Bundesministerium
Europäische und internationale
Angelegenheiten

bmeia.gv.at

Mag. Alexander Schallenberg
Bundesminister

Minoritenplatz 8, 1010 Wien, Österreich

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2020-0.097.511

Wien, am 24. März 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 24. Jänner 2020 unter der Zl. 646/J-NR/2020 an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberattacke auf das Außenministerium“ gerichtet.

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

Hinsichtlich des Ersuchens um eine Beantwortung in klassifizierter Weise nach dem Bundesgesetz über die Informationsordnung des Nationalrates und des Bundesrates – InfOG darf ich auf die Erklärungen im Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten im Februar 2020 und des Nationalen Sicherheitsrates am 28. Februar 2020 verweisen.

Zu den Fragen 1 und 3 bis 8:

- *Welche Information oder Erkenntnisse haben Sie über:*
  a. die Urheberschaft des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)
  Handelt es sich um einen staatlichen/staatsnahen Akteur oder nicht?

Wenn ja, welcher Staat steht hinter dem Angriff?

Welche Informationen haben Sie, um das zu bestätigen bzw. auszuschließen?

b. den zeitlichen Beginn des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)

Seit wann genau ist das IT-System des Außenministeriums durch die Schadsoftware kompromittiert?

Erst seit 3. Jänner 2020 oder schon davor?

Seit welchem Jahr?

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.)

Handelt es sich um einen "Schläfervirus/Schläfersoftware"?

d. die Dauer des Cyberangriffes auf das Außenministerium? (Um detaillierte Erläuterung wird ersucht.)

Ist der Angriff zum Zeitpunkt der Anfragebeantwortung beendet?

Wenn ja, seit wann ist der Angriff beendet?

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.)

Wurden auch Backups des Ministeriums durch die Schadsoftware kompromittiert?

Wenn ja, inwiefern?

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.)

wurden Daten/Informationen aus den Systemen abgezogen?

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.)

- *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 Ressorts 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.)*

  Verfügt Ihr Ressort über einen Rahmenvertrag mit externen Expert_innen/Unternehmen für die rasche Bewältigung von IT-Vorfällen dieser Art?
  Wenn ja, seit wann mit welchen Expert_innen/Unternehmen?
  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.)*

Wie bei meinen Erklärungen im Plenum des Nationalrates vom 22. Jänner 2020 ausgeführt, wurden Ende Dezember 2019 erste Indikatoren für einen möglichen Angriff bekannt und Expertinnen und Experten des Bundesministeriums für Inneres (BMI) umgehend hinzugezogen. Nach derzeitigem Wissensstand handelte es sich bei diesem Angriff um eine gezielte Cyberattacke gegen das Außenministerium mit dem Ziel der Informationsbeschaffung. Es liegen aber derzeit noch nicht genügend Anhaltspunkte vor, um die Herkunft der Cyberattacke mit letzter Gewissheit zu benennen. Ob es zu einem Datenabfluss gekommen sein könnte, ist noch Gegenstand laufender Ermittlungen und kann noch nicht beantwortet werden. Ein Schaden ist nach dem bisherigen Stand der Ermittlungen nicht feststellbar. Überdies war die Funktionsfähigkeit des Bundesministeriums für Europäische und internationale Angelegenheiten (BMEIA) und insbesondere die konsularische Betreuung unserer Staatsbürger während des gesamten Zeitraums der Cyberattacke gewährleistet. Die Bereinigung der Systeme erforderte umfassende technische und vor allem organisatorische Vorbereitungen und konnte schlussendlich am 9. Februar 2020 abgeschlossen werden.

Es werden spezifische Sicherheitsvorkehrungen zum Schutze der IKT-Systeme des Ressorts gegen Angriffe iSd § 118a Strafgesetzbuch (StGB) eingesetzt. Ich ersuche aber um Verständnis, dass, um die Effektivität dieser Maßnahmen nicht zu beeinträchtigen, es nicht möglich ist, diese im Detail öffentlich mitzuteilen, genauso wenig wie Details zur Kooperation mit externen Experten bzw. Unternehmen. Im Regierungsprogramm wird im Bereich der Zuständigkeit meines Ressorts im Punkt „Cybersicherheit und Digitalisierung“ unter anderem die Intensivierung der Zusammenarbeit mit den Partnern in der Europäischen Union als Ziel definiert.

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.)*
  Wenn ja, welche?
  Kann ausgeschlossen werden, dass auch die Systeme anderer Bundesbehörden durch gleiche oder ähnliche Schadsoftware kompromittiert sind?

Ich verweise auf die Beantwortung der parlamentarischen Anfrage Zl. 643/J-NR/2020 vom 24. Jänner 2020 durch den Herrn Bundesminister für Inneres.

Mag. Alexander Schallenberg

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR EUROPÄISCHE UND INTERNATIONALE ANGELEGENHEITEN @ AMTSSIGNATUR	Unterzeichner	CN=Bundesministerium fü europäische und internationale Angelegenheiten,C=AT
	Datum/Zeit	2020-03-24T19:11:25+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	789818819
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmeia.gv.at/verifizierung	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-03-25T10:31:30+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.	