Bundesministerium
Justiz

bmj.gv.at

Dr.in Alma Zadić, LL.M.
Bundesministerin für Justiz

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2020-0.054.044

Ihr Zeichen: BKA - PDion (PDion)644/J-NR/2020

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 Nr. **644/J-NR/2019** an mich eine schriftliche parlamentarische Anfrage betreffend „Cyberattacke auf das Außenministerium“ gerichtet.

Diese Anfrage beantworte ich nach den mir von der Fachsektion vorgelegten 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 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.)*

Mit dieser Frage werden Vorgänge im Wirkungsbereich des Herrn Bundesministers für europäische und internationale Angelegenheiten angesprochen. Ich verweise daher insoweit auf die Beantwortung der wortgleichen Anfrage Zl 646/J durch den zuständigen Bundesminister für europäische und internationale Angelegenheiten.

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?*

Ich habe dazu keine Wahrnehmungen.

Zu den Fragen 3 bis 7:

- *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 Resssort 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 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?

Die Fragen 3 bis 7 beziehen sich auf Angelegenheiten der Gefahrenabwehr und somit den Wirkungsbereich des Bundesministers für Inneres oder der Bundesministerin für Landesverteidigung, an die zu den 643/J und 645/J auch entsprechende Anfragen ergangen sind. Ich verweise daher auf die Anfragebeantwortungen durch die zuständigen Bundesminister.

Was die Frage 7a betrifft, so wird der IT-Betrieb der Justiz bereits seit mehreren Jahrzehnten gänzlich durch die Bundesrechenzentrum GmbH wahrgenommen, deren Expertise sich auch im IT-Sicherheitsbereich niederschlägt.

Zur Frage 8:

- *Laufen derzeit **strafrechtliche Ermittlungen** iZh mit dem Angriff?*

a. *Wenn ja, seit wann unter der Leitung welcher Staatsanwaltschaft und aufgrund welcher konkreten Delikte?*
b. *Wie ist der Stand der Ermittlungen?*
c. *Werden die Ermittlungen gegen „Unbekannt" geführt oder gegen bekannte Personen?*
    i. *Wenn ja, gegen wie viele bekannte Personen?*

Seit 7. Jänner 2020 ist in diesem Zusammenhang bei der Staatsanwaltschaft Wien ein Verfahren gegen einen unbekannten Täter wegen § 118a StGB anhängig. Ich bitte um Verständnis, dass ich zu den laufenden Ermittlungen keine näheren Angaben machen kann.

Dr.[in] Alma Zadić, LL.M.

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2020-03-24T12:32:07+01:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.justiz.gv.at/amtssignatur

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-03-24T15:00:54+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.	