

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

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2022-0.575.216

Ihr Zeichen: BKA - PDion (PDion)12019/J-NR/2022

Wien, am 7. Oktober 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Dr. Stephanie Krisper, Kolleginnen und Kollegen haben am 9. August 2022 unter der Nr. **12019/J-NR/2022** an mich eine schriftliche parlamentarische Anfrage betreffend „Wurde die Spionagesoftware Subzero der österreichischen Firma DSIRF illegal eingesetzt?“ gerichtet.

Vorweg wird um Verständnis gebeten, dass im Rahmen einer öffentlichen Anfragebeantwortung keine Namen und sonstige personenbezogene Daten sowie sonstige individualisierbare Merkmale von angezeigten Personen in strafrechtlichen, nichtöffentlichen Ermittlungsverfahren (§ 12 StPO) genannt werden können und die Grenzziehungen des Daten- und Persönlichkeitsschutzes von Amts wegen zu beachten sind.

Unter dieser Prämisse beantworte ich die an mich gerichteten Fragen auf Grundlage der mir zur Verfügung stehenden Informationen wie folgt:

Zu den Fragen 1 und 5:

- *1. Wurden aufgrund der parlamentarischen Anfrage (8753/J) zu der Firma DSIRF aus dem Jahr 2021 oder den aktuellen Medienberichten und eingebrachten Sachverhaltsdarstellungen Ermittlungen eingeleitet?*
 - a. Falls ja, aufgrund welcher Straftatbestände?*
 - b. Fall ja, von welcher Staatsanwaltschaft werden diese geführt?*

c. Falls nein, warum nicht?

- *5. Die Frage, ob gegen die genannten Firmen Anzeige erstattet wurde, wurde von Seiten des BMI in unserer Anfrage (8753/J) damit beantwortet, dass jede Antwort Ermittlungen gefährden könnte; nun wurde bekannt, dass vonseiten epicenter.works Strafanzeige erstattet wurde. Es stellt sich daher die Frage: Wurde Strafanzeige gegen Firmen die Überwachungs- und Spionagesoftware anbieten, erstattet?*

a. Wenn nein, warum nicht?

Von der Staatsanwaltschaft Wien wurde ein Ermittlungsverfahren wegen des Verdachtes des widerrechtlichen Zugriffs auf ein Computersystem nach § 118a Abs 1 und Abs 4 erster Fall StGB, der Datenbeschädigung nach § 126a Abs 1, Abs 2 und Abs 4 Z 3 StGB sowie der Vergehen nach §§ 79 Abs 1 Z 2 und 80 Abs 1 Z 1 AußWG eingeleitet.

Zu den Fragen 2 und 8 bis 10

- *2. Welche Schritte wurden von Ihrem Ministerium nach Bekanntwerden eines Angriffs auf eine Anwaltskanzlei und zum Schutz des Mandantengeheimnisses unternommen?*
- *8. In welchen Ländern wurde die Spionagesoftware von DSIRF eingesetzt?*
- *9. Was unternimmt Ihr Ministerium, um dem Hacking der Wiener Firma in anderen Ländern Einhalt zu gebieten?*
- *10. Hat das Hacking aus Österreich eine Auswirkung auf die diplomatischen Beziehungen zu anderen Ländern?*

Wie oben ausgeführt, wurde ein strafrechtliches Ermittlungsverfahren eingeleitet. Soweit diese Fragen über die hier dargestellten strafrechtlichen Ermittlungen der staatsanwaltschaftlichen Behörden hinausgehen, betreffen sie nicht (mehr) den Vollzugsbereich der Bundesministerin für Justiz.

Zu den Fragen 3 und 4:

- *3. Die Fragen 1-8 der Anfrage 8753/J betrafen das Unternehmen Palantir, mit welchem es, laut Antwort des Innenministers, im Rahmen einer Dienstreise 2017 ein Treffen gab.*
 - a. Wann war besagtes Treffen genau?*
 - b. Wer waren die Teilnehmer innen?*
- *4. Gab es Kontakt von Ihrem Ressort mit dem Bundeskanzleramt zum Thema Palantir?*
 - a. Wenn ja, was wurde wann genau mit wem besprochen?*

b. Wurden diesbezügliche Vorgänge veraktet?

Mir sind keine Kontakte mit dem Unternehmen Palantir bzw. diesbezügliche Kontakte mit dem Bundeskanzleramt bekannt.

Zur Frage 6:

- *Wurden Schritte zur Ausforschung der Verbindungen der Firma DSIRF mit dem flüchtigen Jan Marsalek oder im Hinblick auf die aufrechten Russlandsanktionen eingeleitet?*

Im Hinblick darauf, dass sich die Anfrage auf ein noch nicht abgeschlossenes Ermittlungsverfahren bezieht und das Ermittlungsverfahren gemäß § 12 StPO nicht öffentlich ist, wird um Verständnis dafür ersucht, dass die Beantwortung dieser auf den Inhalt des Verfahrens gerichteten Frage nicht möglich ist, zumal dadurch einerseits Rechte von Verfahrensbeteiligten verletzt und andererseits der Erfolg der Ermittlungen gefährdet werden könnten.

Zur Frage 7:

- *Sind Infektionen der Software Subzero in Netzwerken Ihres Vollziehungsbereichs entdeckt worden?*
 - a. Wenn nein, wurde danach gesucht?*

Das Bundesrechenzentrum GmbH (BRZG) ist der zentrale IKT-Dienstleister des Bundesministeriums für Justiz. Die BRZG betreibt ihre Sicherheitssysteme am Stand der Technik und passt diese laufend an neue Entwicklungen und Bedrohungen an. Informationssicherheit ist ein wesentlicher Grundpfeiler in der BRZG. Das eigene interne Computer Emergency Response Team (BRZ-CERT) hat die Aufgabe, Sicherheitsvorfälle durch präventive Maßnahmen zu vermeiden. Infektionen des Netzwerks der Justiz (mit) der Software Subzero wurden dabei bislang nicht entdeckt.

Dr.ⁱⁿ Alma Zadić, LL.M.

