



Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2023-0.011.464

Wien, am 7. Februar 2023

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Dr. Nikolaus Scherak, MA, Kolleginnen und Kollegen haben am 19. Dezember 2022 unter der Nr. **13223/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Datenschutz und DSIRF“ gerichtet.

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

Zu den Fragen 1 bis 3:

- *Ist/war Ihr Ministerium Kunde DSIRFs oder anderen Tochterfirmen der NSO Group seit 23.09.2021?*
 - a. *Wenn ja, welche/s Produkt/e wird/werden bezogen?*
 - b. *Wenn nein, ist eine Zusammenarbeit mit DSIRF oder anderen Tochterfirmen der NSO Group in Planung?*
- *Steht/stand Ihr Ministerium im Austausch mit DSIRF?*
 - a. *Wenn ja, welcher Zweck wird mit diesem Austausch verfolgt?*
 - b. *Wenn ja, was ist der aktuelle Stand des Austauschs?*
 - c. *Wenn nein, ist ein Austausch mit DSIRF in Planung?*

- *Bestehen Verträge zwischen dem Bundesministerium für Inneres und/oder nachgeordneten Dienststellen Verträge mit DSIRF oder anderen Tochterfirmen der NSO Group?*
 - a. *Wenn ja, welche und seit wann? Bitte um Angabe der Einrichtung oder Dienststelle und des genauen Datums.*
 - b. *Bitte um genaue Auflistung des Vertragsgegenstandes*

Nein. Darüber hinaus ist zum jetzigen Zeitpunkt keine zukünftige Zusammenarbeit geplant.

Zu den Fragen 4 und 5:

- *Welche aktuellen Bedrohungen und Herausforderungen sehen Sie für Cybersicherheit in Österreich?*
- *Welche Maßnahmen setzt Ihr Ministerium und Ihre nachgeordneten Dienststellen, um den Einsatz von Spionagesoftware gegen öffentliche Einrichtungen zu verhindern?*

Cybersicherheit ist in Österreich ein gesamtstaatliches Thema. Es handelt sich auch rechtlich um eine Querschnittsangelegenheit. Folglich gibt es keine Stelle, die österreichweit verbindliche Vorgaben geben kann. Aus diesem Grund ist eine starke Koordinierung und Bündelung von Kräften notwendig. Hauptzuständig sind die folgenden Ministerien: Bundeskanzleramt (BKA), Bundesministerium für Inneres (BMI), Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) und Bundesministerium für Landesverteidigung (BMLV).

Dabei koordiniert das Bundeskanzleramt nationale und internationale strategische Cybersicherheitsthemen und kooperiert in verschiedenen Arbeitsgremien mit nationalen, europäischen und internationalen Akteurinnen und Akteuren. Darüber hinaus führt es das Ausweichrechenzentrum des Bundes (ZAS) sowie das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT Austria).

Das Bundesministerium für Inneres ist zur Abwehr von Cyberattacken im eigenen Bereich durch technische und organisatorische Sicherheitsmaßnahmen in den Bereichen Prävention, Absicherung, Erkennung und Incident Response entsprechend dem Stand der Technik bestmöglich vorbereitet. Es findet eine enge Abstimmung mit Personen aus der Wissenschaft und der Zivilgesellschaft statt, um deren Expertise einfließen zu lassen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikern des Ressorts zeitnahe umgesetzt.

Darüber hinaus muss von einer detaillierten Auflistung der Maßnahmen zur Erhöhung und dem Erhalt eines hohen IKT-Sicherheitsniveaus im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Des Weiteren darf auf den jährlich erscheinenden „Bericht Cybersicherheit“ des Bundeskanzleramts verwiesen werden.

Zur Frage 6:

- *Sind zusätzliche Maßnahmen zu denen in der ÖSCS 2021 geplant?*
 - a. *Wenn ja, für wann?*
 - b. *Wenn ja, welche?*

Die neue ÖSCS 2021 bildet den strategischen Rahmen für die nationale Cybersicherheitspolitik sowie zur langfristigen Schaffung eines sicheren Cyberraums als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz.

Die ÖSCS 2021 stellt die Basis und den Rahmen für diverse Tätigkeiten und Projekte im Bereich der Cybersicherheit dar. Da aber besonders die Thematik Cybersicherheit ein volatiles Umfeld darstellt, werden im Bundesministerium für Inneres aktuelle Risikofaktoren, als auch sinnvolle Maßnahmen laufend neu bewertet, um gegebenenfalls auf aktuelle Entwicklungen rasch reagieren zu können. Dabei handelt es sich um einen stetigen Prozess der sich an den jeweiligen Bedürfnissen, aber auch an vorhandenen Ressourcen orientiert und entsprechend laufend evaluiert wird.

Zur Frage 7:

- *Ist Ihr Ministerium mit Ihren Amtskolleg_innen aus anderen EU-Mitgliedsstaaten in Bezug auf den Einsatz und den Umgang mit Spionageprogrammen im Austausch?*
 - a. *Wenn ja, welche Position vertreten Sie dort?*
 - b. *Wenn ja, was ist der aktuelle Stand des Austauschs?*
 - c. *Wenn nein, ist ein solcher Austausch in Planung?*

Aus polizeitaktischen Gründen und auf Grund der verfassungsrechtlich normierten Verpflichtung zur Amtsverschwiegenheit (Art. 20 Abs. 3 Bundes-Verfassungsgesetz) muss von einer Beantwortung der Fragen Abstand genommen werden. Durch die Bekanntgabe von Informationen - und sei es auch eine verneinende Beantwortung - können Rückschlüsse gezogen und die Aufgabenerfüllung der Sicherheitsbehörde, vor allem im

Hinblick auf die internationale Zusammenarbeit, erschwert beziehungsweise in gewissen Bereichen unmöglich gemacht werden.

Zu den Fragen 8 bis 10:

- *Gibt es Gründe, weshalb Österreich kein Mitglied der Surveillance Technology Expert Group der Europäischen Kommission ist?*
 - a. *Wenn ja, welche?*
- *Welche Position nimmt Österreich gegenüber strengeren Import- und Exportkontrollen von Trojaner-Technologie ein?*
- *Setzen Sie oder die Bundesregierung sich aktiv für ein Exportverbot von Trojaner-Technologie in autoritäre Staaten ein?*
 - a. *Wenn nein, warum nicht?*

Diese Fragen betreffen jedoch keinen Gegenstand der Vollziehung des Bundesministeriums für Inneres und sind daher im Sinne des Art. 52 Bundes-Verfassungsgesetz in Verbindung mit § 90 Geschäftsordnungsgesetz 1975 keiner Beantwortung durch mich zugänglich.

Gerhard Karner

