13156/J XXVII. GP

Eingelangt am 29.11.2022

ANFRAGE

des Abgeordneten David Stögmüller, Freundinnen und Freunde,

an die Bundesministerin für Landesverteidigung

betreffend Geschäftsverhandlungen mit dem Software-Unternehmen DSIRF

Wie aus mehreren Medienberichten der letzten Woche hervorging, wurde ein von dem österreichischen Software-Unternehmen DSIRF GmbH (ATU71409246) entwickelter Staatstrojaner namens ‚Subzero' dafür missbraucht, um prominente Anwaltskanzleien in Österreich, aber auch quer durch Europa und Südamerika zu bespitzeln.[1] Das Wiener Unternehmen hat zudem beste Kontakte nach Russland und Berührungspunkte mit dem flüchtigen Wirecard-Chef Jan Marsalek.[2,3] Laut dem aktuellen Informationsstand soll in Marsaleks Emails eine Präsentation der österreichischen Firma gefunden worden sein, die laut DSIRFs Angaben zuvor dem Bundesministerium für Inneres geschickt worden war. In derselben Präsentation sollen mehrere prominente russische Firmen als Kunden angeführt worden sein.[4]

Bereits im August dieses Jahres kamen die Fälle der Bespitzelung mehrerer österreichischer und internationaler Anwaltskanzleien ans Licht, nachdem das Software-Unternehmen Microsoft, auf dessen Betriebssystem die ‚Subzero'-Technologie spezialisiert ist, eine Warnung aussprach. Diese Woche stellte sich heraus, dass infolge dieser Warnung die Direktion für Staatsschutz und Nachrichtendienst (DSN) Ermittlungen einleitete. Diese führten sogar zu einer kurzfristigen Verhaftung eines Ex-Mitarbeiters von DSIRF GmbH aufgrund von Verdunkelungsgefahr.[5]

---

[1] Thalhammer, Anna und Manuel Reinartz. „Microsoft bezichtigt Wiener Firma der Spionage." *Die Presse*, 28.7.2022. Abgerufen am 24.11.2022. https://www.diepresse.com/6170945/microsoft-bezichtigt-wiener-firma-der-spionage.

[2] Hein, Jan-Philipp. „Im Rätsel um gruselige Spionage-Software führt die Spur über Wirecard in den Kreml." *FOCUS Online*, 19.11.2021. Abgerufen am 28.11.2022. https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html.

[3] Siehe auch: Meister, Andre. „Wir enthüllen den Staatstrojaner „Subzero" aus Österreich." *Netzpolitik.org*, 17.12.2021. Abgerufen am 28.11.2022. https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/#netzpolitik-pw.

[4] Thalhammer, Anna. „Staatstrojaner "Subzero": Anwälte bespitzelt, mit Geheimdiensten verhandelt." *Die Presse*, 24.11.2022. Abgerufen am 24.11.2022. https://www.diepresse.com/6219330/staatstrojaner-subzero-anwaelte-bespitzelt-mit-geheimdiensten-verhandelt.

[5] Ibid.

Trotz dieses Sachbestands stellt sich nun heraus, dass das Heeresnachrichtenamt (HNaA) an einer Zusammenarbeit mit DSIRF und scheinbar am Kauf von deren ‚Subzero'-Software interessiert war.[6]

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Hat es Gespräche zwischen Mitarbeiter*innen Ihres Ministeriums, insbesondere des Heeresnachrichtenamts und/oder des Abwehramts, und dem Unternehmen DSIRF GmbH (ATU71409246), bzw. folgenden nahestehenden Unternehmen gegeben?
   a) DSR Decision Supporting Information Research Forensic GmbH (ATU74983627)
   b) Deep Dive Research Lab AG[7] (Handelsregister: FL-0002.576.355-2), Lichtenstein
   c) MLS Machine Learning Solutions GmbH (ATU75038317)
   d) Guardian GmbH (ATU75671701) bzw. deren Mutter "Guardian AG (Handelsregister: FL-0002.639.291-6)" in Lichtenstein
   e) Code Arch Platform GmbH (Firmenbuch-Nr.: 592761h)

   Geben Sie bitte an mit welchen dieser Unternehmen Mitarbeiter*innen Ihres Hauses, insbesondere des HNaA, Kontakt hatten, sowie wann und zu welchem Zweck diese Gespräche geführt wurden.

2) Laut den uns vorliegenden Informationen (Schriftverkehr) gab es in Ihrem Haus, insbesondere im HNaA die Absicht, Software von zumindest einem der oben angeführten Unternehmen zu erwerben. Ist dies zutreffend?
   a) Wenn ja, wann wurden Sie darüber in Kenntnis gesetzt? Bitte für jedes Projekt separat anführen.

3) Um welche konkrete Software bzw. Dienstleistung handelte es sich (Namen, Zweck und Umfang der Leistung), und von welchem Unternehmen sollte diese jeweils geliefert bzw. erbracht werden? Führen Sie bitte jede einzeln an.
   a) Wie hoch waren die Kosten, die für die Software inkl. sonstiger Dienstleistung im Zusammenhang entstanden wären bzw. sind.
   b) Welche Projekte bzw. Dienstleistungen wurden durchgeführt und welche wurden nur geplant bzw. angedacht?
   c) Entstanden bereits Kosten für die angedachten bzw. geplanten Projekte mit dem entsprechenden Unternehmen? Wenn ja, in welcher Höhe? Bitte für jedes Projekt separat ausführen.

---

[6] Ibid.

[7] *Moneyhouse Handelsregister.* Abgerufen am 28.11.2022. https://www.moneyhouse.ch/de/company/deep-dive-research-lab-ag-12045214839/management.

4) Ist oder war ein Produkt der oben genannten Unternehmen im ÖBH, insbesondere HNaA oder AbwA, in Verwendung? Wenn ja, wann bzw. wie lange, und wie sowie wofür wird/wurde es eingesetzt?

5) Die Unternehmen bieten nicht nur „Staatstrojaner“ bzw. Software zur Computerüberwachung und zur Exfiltration sensibler Daten an, sondern auch eine Gesichtserkennungssoftware. Wird seitens des Heeresnachrichtenamts und/oder des Abwehramts eine derartige Software der oben genannten Unternehmen verwendet, oder wird bzw. wurde deren Verwendung angedacht?
   a) Wenn ja, wo, seit wann bzw. wie weit sind derartige Gespräche geführt worden?

6) Sind Mitarbeiter*innen des HNaA und/oder des AbwA aktiv an das Unternehmen „MLS Machine Learning Solutions GmbH“ herangetreten? Wenn ja, wann wer und wofür?
   a) Wurden entsprechende Aktenvermerke angelegt?
   b) Wurde das Kabinett darüber informiert?

7) Gab es in diesem Zusammenhang eine entsprechende Sicherheitsüberprüfung des Unternehmens bzw. dessen Umfeld? Wenn ja, durch wen und was war das Ergebnis?

8) Stand das HNaA mit Partnerdiensten im Zusammenhang mit Einkäufen von Software von oben genannten Unternehmen im Kontakt?
   a) Wenn ja, mit welchen, wann und zu welchem Schluss kamen diese?

9) Wann und von wem wurden Sie bzw. Ihr Kabinett über diese Causa DSIRF und das Interesse des HNaA am Erwerb einer Software informiert?

10) Wussten Sie bzw. Ihr Kabinett von den Ermittlungen der DSN betreffend das Unternehmen DSIRF? Wenn ja, wann erfuhren Sie bzw. Ihr Kabinett davon?

11) Gab es in dem Zusammenhang einen Informationsaustausch mit dem DSN? Wenn ja, wann fing dieser an?

12) Inwiefern ist der Erwerb dieser Software mit dem aktuellen Militärbefugnisgesetz und den darin im 2. Teil – 2. Abschnitt angeführten Befugnissen vereinbar?
   a) Wurden entsprechende interne Ermittlungen eingeleitet?
   b) Wurde die interne Revision eingeschaltet?
   c) Wurde Anzeige wegen Missbrauch der Amtsgewalt erstattet?
      i) Wenn ja, wann und gegen wen?

13) Wurde vor der Angebotseinholung durch das HNaA bereits die Rechtsgrundlage für den allfälligen Einsatz der Software geprüft (insbesondere nach dem MBG)?

14) Wurde der Rechtsschutzbeauftragte des HNaA vor der Einholung des Angebots über einen Erwerb entsprechender Software informiert?
   a) Wenn ja, wann?
   b) Wenn nein, warum nicht? Wäre es nicht seine Aufgabe entsprechend über derartiges unterwiesen zu werden?

15) Wurde eine interne Überprüfung von Ihnen im HNaA und/oder AbwA veranlasst, ob Software oder technische Möglichkeiten angeschafft wurden, deren Fähigkeiten über die Befugnisse nach dem MBG hinausgehen?
   a) Wenn ja, seit wann läuft diese und wann ist mit einem Abschluss und Bericht zu rechnen?
   b) Wenn nein, warum nicht?

Sollte eine detaillierte Beantwortung einzelner Fragen oder Unterfragen aus Geheimhaltungsgründen nicht möglich sein, so wird dennoch um eine Beantwortung mit möglichst hohem Informationsgehalt im Sinne des parlamentarischen Interpellationsrecht ersucht. Allenfalls ersuchen die Abgeordneten um eine Beantwortung in klassifizierter Weise nach dem Bundesgesetz über die Informationsordnung des Nationalrates und des Bundesrates (InfOG).