12064/J XXVII. GP

Eingelangt am 31.08.2022

Anfrage

der Abgeordneten Katharina Kucharowits,
Genossinnen und Genossen
an die Bundesministerin für Landesverteidigung

betreffend **Österreichische Spionagetechnologie im Einsatz der Republik?**

Im Jahr 2019 sollte eine Technologie etabliert werden, die der Öffentlichkeit als Bundestrojaner besser bekannt wurde und zum Ziel gehabt hätte, ohne das Wissen der Nutzer*innen von digitalen Endgeräten, Daten zu sammeln und in Richtung von Ermittlungsbehörden abzuziehen bzw. auch Inhalte auf den Geräten zu verändern. ÖVP und FPÖ hätten damit einen massiven Eingriff in die Privatsphäre unter dem Deckmantel der Sicherheitspolitik begangen – der Verfassungsgerichtshof stoppte das Überwachungspaket 2019 jedoch schließlich und erkannte es als verfassungswidrig.

Nun dürfte ein österreichisches Unternehmen aber im Besitz einer Software sein, die genau für derartige Zwecke eingesetzt werden kann und diese auch vertreiben. Unter dem Namen „Subzero“ verbirgt sich laut den Datenschutzexpert*innen von Epicenter.Works „eine Spionagesoftware der höchsten Klasse“, ihre Möglichkeiten sind weitreichend: „Screenshots, die Aufzeichnung von Tastatureingaben, Abgreifen von Dateien, Ausführen von Systembefehlen, Herunterladen von weiteren Softwareteilen bis hin zum Stehlen von Passwörtern, Location-Tracking und schlussendlich der kompletten Kontrolle des Zielgeräts“ sollen im Bereich des Möglichen liegen. Die Software soll kürzlich auf Windows-Geräten gefunden worden sein, die von Unternehmensberatungen, Anwaltskanzleien und Banken genutzt werden, neben mehreren anderen Ländern auch in Österreich, berichtet Epicenter.Works. Aus diesem Grund hat die Organisation auch eine Strafanzeige eingebracht.[1]

Dass sich die Spionagesoftware als Produkt vor allem an Staaten richtet, sagt auch die Herstellerfirma DSIRF und spricht von behördlicher Anwendung von „Subzero“ in Staaten der EU.[2]

Die Fakten rund um das Produkt, aber auch rund um die Firma DSIRF, die bekannt sind, können nur als besorgniserregend erkannt werden und bedürfen einer gründlichen Untersuchung sowie der politischen Kontrolle. Aus diesem Grund stellen die unterfertigten Abgeordneten folgende

Anfrage

1) Ist Ihnen persönlich die Firma DSIRF bekannt?
2) Ist Ihnen persönlich die Software „Subzero“ ein Begriff?

[1] https://epicenter.works/sites/default/files/epicenter.works-anzeig_dsrif-_on.pdf
[2] https://futurezone.at/b2b/dsirf-knotweed-subzero-spyware-microsoft-windows-exploits/402090520

3) Gibt bzw. gab es in Ihrem Ministerium Kontakt mit dem Unternehmen DSIRF, seinen Muttergesellschaften, Vertreter*innen oder Vermittler*innen?
4) Gibt bzw. gab es in Ihrem Ministerium Überlegungen Geschäfte mit der Firma DSIRF oder seinen Muttergesellschaften einzugehen?
    a. Falls ja: Sind diese eingegangen worden, bzw. ist es geplant, diese einzugehen?
    b. Falls nein: Warum nicht?
5) Wird die Spionagesoftware „Subzero“ im Geltungsbereich Ihres Ministeriums, in seinem Auftrag oder durch das Ministerium selbst bzw. eine nachgelagerte Dienststelle Ihres Ministeriums eingesetzt?
    a. Falls ja: Von wem konkret wird die Software eingesetzt?
    b. Falls ja: Auf Basis welcher rechtlichen Grundlage geschieht der Einsatz der Software?
    c. Falls ja: Wie hoch sind die Kosten und sind diese budgetiert?
    d. Falls ja: Wie viele Personen können auf die Software selbst zugreifen?
    e. Falls ja: Wie viele Personen werden mithilfe der Software überwacht und welche Daten werden abgegriffen?
    f. Falls ja: Wie viele Personen können auf die abgegriffenen Daten zugreifen?
    g. Falls ja: Seit wann ist die Software im Einsatz?
    h. Falls nein: Können Sie einen Einsatz ausschließen?
6) Ist geplant, die Spionagesoftware „Subzero“ zukünftig im Geltungsbereich Ihres Ministeriums, in seinem Auftrag oder durch das Ministerium selbst bzw. eine nachgelagerte Dienststelle Ihres Ministeriums einzusetzen?
    a. Falls ja: Durch wen soll diese Software eingesetzt werden und aus welchem Grund?
    b. Falls ja: Auf Basis welcher rechtlichen Grundlage soll der Einsatz geschehen?
    c. Falls ja: Wie hoch sind die Kosten und sind diese bereits budgetiert? Nennen Sie dazu bitte die konkreten Untergliederungen im Budget.
    d. Falls ja: Wie viele Personen sollen dann auf die Software selbst zugreifen können?
    e. Falls ja: Wie viele Personen werden mithilfe der Software überwacht werden und welche Daten sollen abgegriffen werden?
    f. Falls ja: Wie viele Personen werden auf die abgegriffenen Daten zugreifen können und wer werden diese Personen sein?
    g. Falls ja: Ab wann wird die Software im Einsatz sein?
    h. Falls nein: Können Sie einen zukünftigen Einsatz ausschließen?
7) Halten Sie den Einsatz eines Staats- oder Bundestrojaners, oder einer Art von Software, die man darunter gemeinhin versteht, für die Bekämpfung von Kriminalität für notwendig?
8) Gibt es Pläne zum Einsatz einer derartigen Software?
    a. Falls ja: Wie soll sich der Einsatz dieser Software gestalten, nachdem der Verfassungsgerichtshof zu dem Schluss kam, dass der Einsatz derartiger Lösungen nicht verfassungskonform ist? Sind dazu Gesetzesänderungen geplant?
9) Gibt es derzeit eine rechtlich zulässige Methode für den Fernzugriff auf die Kommunikationsinhalte von verschlüsselten Messengern wie WhatsApp?
10) Wäre eine Überwachung verschlüsselter Nachrichten gemäß § 134 Z 3a StPO zulässig?
    a. Falls ja, welche technischen Maßnahmen wären dafür geeignet?
11) Können Sie ausschließen, dass die Software „Subzero“ gegen staatliche Institutionen in Österreich eingesetzt wurde?
12) Welche Maßnahmen haben Sie gesetzt, oder werden Sie setzen, die Daten der Österreicher*innen gegen den Einsatz von „Subzero“ und ähnlichen Staatstrojanern anderer Staaten zu schützen?
13) Welche Maßnahmen werden Sie setzen, um die bisher in Österreich durch Überwachung von „Subzero“ betroffenen Unternehmen gegen Angriffe mit dieser Software zu schützen?

14) Können Sie ausschließen, dass „Subzero“ erfolgreich gegen Ihr Ministerium oder den Heeresnachrichtendienst eingesetzt wurde?
15) Ist Ihnen bekannt, welche Länder die Software „Subzero“ nutzen?
    a. Falls nein: Haben Sie dazu Auskunft vom Bundesministerium für Arbeit und Wirtschaft erbeten, nachdem es sich um ein Dual-Use-Gut handelt, deren Ausfuhr genehmigungs- bzw. mitteilungspflichtig wäre? Wie wurde diese Auskunft beantwortet?
    b. Falls ja: Welche sind das?
16) Können Sie ausschließen, dass die Software „Subzero“ direkt oder über den Umweg über ein anderes EU-Land für die Kriegsführung zwischen Russland und der Ukraine eingesetzt wird?