4009/J
vom 04.03.2015 (XXV.GP)

Anfrage

der Abgeordneten Niko Alm, Kollegin und Kollegen

an den Bundesminister für Landesverteidigung und Sport

betreffend HEAT-Anfrage zu "Staatstrojanern"

Der Computer, der Laptop, Tablets, Smartphones oder sonstige mobile Geräte stellen für viele Menschen einen wichtigen Teil ihres Lebens dar. Darauf werden private Fotos gespeichert ebenso wie persönliche Nachrichten und Dokumente; man kommuniziert darüber via Chat, Videotelefonie und nutzt sie für viele weitere Dinge. Für die meisten Menschen wird mittlerweile ein Eingriff in diesen Bereich privater Lebensgestaltung mindestens genauso empfunden wie ein Eindringen in die eigene Wohnung. Trojanersoftware, die auf Computer geschleust wird, um dort unerkannt im Hintergrund zu operieren, stellt also einen tiefen Eingriff in die Privatsphäre einer Person dar.

Diese Anfrage ist in Kooperation mit dem Arbeitskreis Vorratsdatenspeicherung (AK-Vorrat) entstanden. Nach der erfolgreichen Abschaffung der Vorratsdatenspeicherung adressiert AKVorrat die Abschaffung der übrigen Massenüberwachungsgesetze in Österreich. Mit dem Projekt „Handlungskatalog zur Evaluierung von Anti-Terror-Gesetzen" (kurz: HEAT) wird ein annähernd vollständiges Bild der Überwachungsgesetzgebung und –technik in Österreich gezeichnet. Das Ziel ist eine verhältnismäßige und faktenbasierte Sicherheitspolitik. Aktuelle Informationen zum Projekt auf https://akvorrat.at/heat

Aus diesem Grund stellen die unterfertigten Abgeordneten nachstehende

Anfrage

1. Wird ein so genannter „Staatstrojaner", eine Software zur Datenerhebung auf Computersystemen von verdächtigten Personen (Remote-Forensik-Software), durch eine Ihnen unterstellte Behörde zum Einsatz gebracht?
    a. Wenn nein, gibt es Pläne für einen Einsatz einer derartigen Software? Falls ja, für wann?
    b. Falls ja, auf welcher Gesetzesgrundlage geschieht der Einsatz von Staatstrojanern?
2. Welche Software wird von den Ermittlungsbehörden für den Zweck der „Internetüberwachung (Keylogging, Screenshotting)" eingesetzt?
3. In wie vielen Fällen wurde ein Staatstrojaner durch physischen Zugang zu dem Rechner der Zielperson installiert?

4. In wie vielen Fällen wurde ein Staatstrojaner durch Manipulation einer Internetverbindung installiert?
5. In wie vielen Fällen wurde ein Staatstrojaner durch Manipulation eines Datenträgers installiert?
6. In wie vielen Fällen wurde ein Staatstrojaner über andere Wege installiert?
7. In wie vielen dieser unter Frage 3 bis 6 genannten Fälle kam es dabei
    a. zu Kooperationen mit österreichischen Firmen?
    b. zu Kooperationen mit europäischen Firmen?
    c. zu Kooperationen mit Firmen aus Drittstaaten?
    d. zu Kooperation mit europäischen Sicherheitsbehörden?
    e. zu Kooperation mit ausländischen Sicherheitsbehörden?
8. Welche Daten werden durch die oben genannte Software (Staatstrojaner, Software zur Internetüberwachung) erhoben?
9. Kann das Computersystem der verdächtigen Person dadurch „ferngesteuert" werden (insbesondere Tätigen von Internetzugriffen, Aktivieren von Kamera, Mikrofon, etc.)?
    a. Wenn ja, welche Auswirkungen hat dies auf die Beweiskraft der derart erhobenen Daten?
10. Mit welchen Anbietern von Antivirensoftware gibt es Vereinbarungen, welche die Erkennung der eingesetzten Software durch die Antivirensoftware verhindern?
11. Sind dem Ministerium Fälle bekannt, in welchen die mittels Trojanersoftware erhobenen Daten auf ausländischen Servern gespeichert wurden oder werden?
12. Besteht eine Geschäftsbeziehung zwischen einer Firma der Gamma Group oder einer ihrer Töchter und dem Ministerium bzw. einer seiner untergeordneten Stellen?
13. Besteht eine Geschäftsbeziehung zwischen der Firma DigiTask GmbH (Deutsche Handelsregisternummer: HRB 3177) und dem Ministerium bzw. einer seiner untergeordneten Stellen? (vgl. https://www.unwatched.org/20111012_Staatstrojaner_Oesterreich_auf_der_Kundenliste_von_DigiTask)
14. Besteht eine Geschäftsbeziehung zwischen dem Ministerium bzw. einer seiner untergeordneten Stellen und einer der folgenden Firmen oder einer ihrer Töchter: Ability, ACCESSDATA, ACME Packet, Advanced German Technology, AGNITIO S.L., Alcatel-Lucent, Allot Communications Ltd, Altron, AMESYS, AUDIOTEL International, AQSACOM, ARCADIA (ARC4DIA), Area Spa, ATIS systems GmbH (ATIS UHER), Audio Video Intelligence Corporation, B.E.A. S.r.l., BlueCoat, BRIGHTPLANET, Cambridge Consultants, Cellebrite Mobile Synchronization Ltd., ClearTrail, COBHAM, CommuniGate Systems, Comverse, Creativity Software, C Tech Bilişim Teknolojileri San. ve Tic. AS., Cyberoam, DATAKOM, DATONG, Cyttek Group, Delta SPE, Delma MSS, Detica, Dialogic, DigiVox B.V., DIGINT Srl, Dreamlab Technologies AG, EBS-Electronic GmbH, Elaman, Elbit Systems, Elta Systems Ltd., ENDACE accelerated, ERA IT Solutions AG, Ericsson, ETI A/S, Expert System S.p.A., FireDigit bvba, Fox-IT, Gigamon, Glimmerglass, Griff Comm Ltd, GROUP2000, GTEN DATAKOM, Gita Technologies Ltd., Guidance Software, Hacking Team, Harris Wireless Products Group, Hidden

Technology Systems International Ltd, HSS Development, Huawei Technologies, IBH Impex, Innova S.p.A., Intelligentias Inc., INVEA-TECH, IPOQUE, IPS Intelligence & Public Security S.p.A., ISKRATEL, IVIGNERI, KBI Optronics GmbH, Kommlabs Dezign Pvt. Ltd., LOQUENDO, Macro System, Medav GmbH, Meganet Corporation, MERA Systems, Motec, Micro Systemation AB, Narus, NEOSOFT, NETOPTICS, NETRAGARD, NETSWEEPER, NETI, Netquest Corporation, NetWitness, Newport Networks, Nice Systems, @one IT GmbH, ONPATH Technologies, OPENET, PAD Datentechnik GmbH, Panoptech, PKElectronic, Plath GmbH, Pen Link, Phoenix, Phonexia s.r.o., Polaris Wireless, Proximus (Belgacom Mobile N.V./S.A), QOSMOS, RCS, Rohde & Schwarz, retentia, REUTER, Seartech, Selectronic, Septier, SHOGI Communications, Siemens, SS8 Networks, Syborg, Spectronic Systems A/S, Speech Technology Center, Spektra srl, Suntech Intelligence, Stratign FZCO, Tamara Electronic Ltd. Sti, telesoft TECHNOLOGIES, Teletel, Thales, Tinex, TraceSpan Communications, Trovicor, Ultrareach, Unispeed A/S, Utimaco Safeware, VASTech, VERINT (früher: Comverse Infosys), Vervis COMINT Services GmbH, VigiTrust, Vineyard Networks, Vixtel, VOCAL Technologies, VUPEN, OMNI Wildpackets, YTRAIL, ZTE oder 3M Services?

a. Wenn ja, seit wann und welche Aufgabengebiete umfassen diese Geschäftsbeziehungen jeweils?

b. Wenn ja, welche Abteilungen, welcher Behörden sind in diesen Geschäftsbeziehungen bzw. Kooperationen jeweils involviert?

c. Wenn ja, welche Kosten sind jeweils für diese Geschäftsbeziehungen bisher angefallen?

d. Wenn nein, ist eine solche Geschäftsbeziehung zwischen dem Ministerium bzw. einer seiner untergeordneten Stellen und einer der unter Frage 14 genannten Firmen oder einer ihrer Töchter geplant? Wenn ja, mit welcher Firma, für wann und welche Aufgabengebiete umfassend?

15. Welche Observations- und Ermittlungstechnik wurde im Rahmen des "Sicherheitspakets" nach den Anschlägen in Paris im Jahr 2015 angeschafft bzw. ist geplant angeschafft zu werden?

16. Wie hoch sind die genauen Kosten dafür? (Bitte um möglichst detaillierte Aufschlüsselung der Kostenpunkte)

17. Welche Synergien sind im Rahmen des "Sicherheitspakets" nach den Anschlägen in Paris im Jahr 2015 zwischen Verteidigungsministerium und Innenministerium geplant?

(ACM)

(SCHENNAK)

(Strolz)