4953/J
vom 08.05.2015 (XXV.GP)

Anfrage

der Abgeordneten Peter Pilz, Freundinnen und Freunde an den Bundesminister für Verkehr, Innovation und Technologie

betreffend Abwehr der NSA Spionage im BMVIT

BEGRÜNDUNG

Mit zunehmender Aufarbeitung der von Edward Snowden aufgedeckten Dokumente über die internationalen Spionagetätigkeiten der NSA und ihrer Partnerdienste wie insbesondere dem britischen GCHQ wird das wahre Ausmaß der stattfindenden Massenüberwachung immer besser erkennbar. In den letzten Wochen haben diesbezüglich einige äußerst besorgniserregende neue Enthüllungen Licht auf die technischen Fähigkeiten von NSA & Co geworfen. Diese übersteigen die ursprünglichen Annahmen bei weitem, und zeigen, dass es höchst an der Zeit wäre, dass auch österreichische Behörden diese leider sehr reale Bedrohung endlich ernst nehmen.

Zunächst wurde im November 2014 bekannt, dass mit der Malware „Regin" ein dem gegen den Iran gerichteten Wurm „Stuxnet" ähnliches Produkt seitens der NSA gezielt gegen Regierungen, Behörden, Kryptologen und Mathematiker weltweit eingesetzt wurde. Bemerkenswert war dabei aus österreichischer Sicht, dass neben den Hauptzielländern wie Russland, Iran und anderen, rund 5% der Einsatzfälle dieser Schadsoftware Computersysteme in Österreich betrafen[1].

Im Februar 2015 berichtete ein renommiertes Computersicherheitsunternehmen über weitere Formen von Cyberschädlingen, die von der sogenannten „Equation-Group", die zumindest seit 2001 aktiv sei, eingesetzt worden seien[2]. Aufgrund von übereinstimmendem Code zwischen diesen Programmen und dem mittlerweile ebenfalls der NSA zugeordneten Stuxnet-Wurm, gelangten die Sicherheitsforscher zu dem überzeugenden Verdacht, dass auch die „Equation-Group" der NSA zuzurechnen ist. Das Besondere an den nunmehr aufgedeckten Schadprogrammen ist, dass diese auf der niedrigsten technischen Stufe, der Firmware von Computern und Festplatten agieren, und so vor der Entdeckung durch Antivirensoftware geschützt sind. Auf diese Art können unter anderem verdeckt auch die Verschlüsselung umgangen und sogar vollständige Löschvorgänge von Festplatten

[1] http://diepresse.com/home/techscience/internet/4602940/SpionageSoftware-Regin-auch-in-Osterreich-aktiv-

[2] Siehe etwa diesen Bericht der New York Times: http://www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html?_r=1

(Wipe) unterlaufen werden. Ein derart befallenes Computersystem kann nur noch komplett ersetzt werden.

Die von dem Sicherheitsunternehmen veröffentliche Karte[3] wies diesmal zwar keine Fälle in Österreich aus, was aber natürlich keineswegs bedeutet, dass es solche nicht gibt oder dass sie sich nicht noch ereignen könnten.

Schließlich berichtete die Internetplattform The Intercept[4], dass der britische GCHQ in enger Kooperation mit der NSA durch systematische Angriffe auf den niederländischen SIM-Karten Erzeuger Gemalto zumindest Millionen von elektronischen „Ki-Schlüsseln" illegal entwendete, mit deren Hilfe verschlüsselte Handytelefonate, SMS und Internetdienste problemlos abgefangen werden können. Soweit über passive Funkmasten der NSA, wie etwa jenen der US-Vertretung bei der UNO gegenüber der Wiener UNO-City[5], verschlüsselte Mobiltelefonate abgefangen und massenweise gespeichert wurden, können diese auch noch weit im Nachhinein mit diesen Schlüsseln entschlüsselt und ausgewertet werden. Laut The Intercept ergibt sich aus den ausgewerteten Geheimdokumenten auch, dass neben Gemalto auch ein weiterer Anbieter von SIM-Karten, die deutsche Firma Giesecke & Devrient ins Visier des GCHQ geriet. Ob der Angriff auch hier erfolgreich war, ist nicht bekannt.

Durch die Schlüssel ist es für NSA und GCHQ möglich, illegale Telefonüberwachungen international durchzuführen, ohne dass die jeweiligen Betreiber oder die nationalen Regierungen in irgendeiner Form eingebunden werden.

NSA und GCHQ gingen hier gezielt gegen ein Unternehmen aus einem EU- und NATO-Mitgliedstaat vor. Die ausgewerteten Dokumente belegen, wie diese Geheimdienste weltweit einfache Mitarbeiter von Gemalto auf ihre Überwachungslisten setzten und mithilfe der ebenfalls von Edward Snowden aufgedeckten Systeme wie etwa XKeyScore deren privaten und beruflichen E-Mail Verkehr systematisch überwachten, um Ansatzpunkte für ihren großangelegten Cyberangriff zu finden.

Wie diese Berichte zeigen, kann jedermann in den Fokus der Überwachungsmaschinerie gelangen. Das gilt umso mehr für staatliche Behörden und ihre Mitarbeiter. Es wurde bereits bei früherer Gelegenheit aufgezeigt, dass auch Österreich auf der Überwachungsliste der NSA steht[6]. Das wurde auch durch die

[3] http://derstandard.at/2000011797618/Sicherheitsforscher-NSA-schleuste-Spyware-auf-Festplatten
[4] https://firstlook.org/theintercept/2015/02/19/great-sim-heist/
[5] http://fm4.orf.at/stories/1746596/
[6] http://derstandard.at/2000002510301/Oesterreich-auf-der-offiziellenUeberwachungsliste-der-NSA

jüngsten Enthüllungen über Spionagetätigkeiten des deutschen BND gegen Österreich im Auftrag der NSA neuerlich bestätigt[7].

Es liegt daher im Interesse der österreichischen Behörden, aber insbesondere auch im Interesse der österreichischen BürgerInnen, deren Daten in der Verwaltung verarbeitet werden, dass endlich wirksame Maßnahmen zur Abwehr der vielfältigen Bedrohungen seitens der NSA und ihrer Partnerdienste ergriffen werden.

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Welche Maßnahmen haben Sie seit dem Beginn der Snowden Enthüllungen über die illegale Massenüberwachung durch die NSA und ihre Partnerdienste ergriffen, um die Informations- und Kommunikationstechnologie im Bereich Ihres Ressorts und seiner nachgeordneten Dienststellen gegen Angriffe zu sichern?
2) Haben Sie Hinweise darauf, dass im Bereich Ihres Ressorts oder seiner nachgeordneten Dienststellen Angriffe durch die Schadsoftware Stuxnet stattgefunden haben, und falls ja in welchem Ausmaß und was haben Sie dagegen unternommen?
3) Haben Sie Hinweise darauf, dass im Bereich Ihres Ressorts oder seiner nachgeordneten Dienststellen Angriffe durch die Schadsoftware Regin stattgefunden haben, und falls ja in welchem Ausmaß und was haben Sie dagegen unternommen?
4) Haben Sie Hinweise darauf, dass im Bereich Ihres Ressorts oder seiner nachgeordneten Dienststellen Angriffe durch die Installation von Schadsoftware der Equation Group (insbesondere auf der Firmware-Ebene) stattgefunden haben, und falls ja in welchem Ausmaß und was haben Sie dagegen unternommen?
5) Haben Sie Hinweise darauf, dass im Bereich Ihres Ressorts oder seiner nachgeordneten Dienststellen Angriffe durch andere Schadsoftware stattgefunden haben, und falls ja in welchem Ausmaß und was haben Sie dagegen unternommen?
6) Welche österreichischen Mobiltelefonieanbieter benutzen SIM-Karten von Gemalto?
7) Welche österreichischen Mobiltelefonieanbieter benutzen SIM-Karten von Giesecke & Devrient?
8) Welche Maßnahmen haben Sie bzw. die Kommunikationsbehörde Austria als Reaktion auf die Berichte über den illegalen Zugriff von GCHQ und NSA auf die

[7] http://www.faz.net/aktuell/politik/inland/nsa-spitzelei-bnd-soll-12-000-suchbegriffe-geloescht-haben-13569002.html

SIM-Schlüssel von Gemalto gesetzt, um eine Nutzung dieser Schlüssel zum illegalen Abhören österreichischer Mobilkommunikation zu verhindern?

9) Welche Maßnahmen haben Sie bzw. die Kommunikationsbehörde Austria ergriffen, um gegen den offensichtlich zum illegalen Abhören von Mobilkommunikation im Bereich der UNO-City installierten Sendemast bei der US-Vertretung bei der UNO im IZD-Tower rechtlich vorzugehen?
10) Welche Maßnahmen haben Sie bzw. die Kommunikationsbehörde Austria ergriffen, um gegen den auf der US-Botschaft in der Wiener Boltzmanngasse offensichtlich zum Zweck der illegalen Überwachung von Telekommunikation angebrachten Dachausbau rechtlich vorzugehen?
11) Welche Maßnahmen haben Sie bzw. die Kommunikationsbehörde Austria ergriffen, um gegen die auf der Liegenschaft Pötzleinsdorfer Straße 126 im Eigentum der USA mutmaßlich hinter einer auffälligen Fassadenverkleidung in Richtung Westen (somit mit Blick Richtung Richtfunkstation Exelberg) zum Zweck der illegalen Überwachung von Telekommunikation angebrachten Anlagen rechtlich vorzugehen?
12) Welche Maßnahmen haben Sie bzw. die Kommunikationsbehörde Österreich seit dem Beginn der Snowden Enthüllungen gesetzt um aufzuklären, inwiefern NSA, GCHQ und andere Partnerdienste in Österreich illegale Überwachung von Telekommunikation betreiben und was konnten Sie dabei bisher feststellen?
13) Welche Maßnahmen haben Sie bzw. die Kommunikationsbehörde Österreich gesetzt, um österreichische Telefonleitungen im Inland vor Abgriffen durch ausländische Geheimdienste zu schützen?
14) Welche Maßnahmen haben Sie bzw. die Kommunikationsbehörde Österreich gesetzt, um Leitungen österreichischer Telekommunikationsanbieter im Ausland vor Abgriffen durch ausländische Geheimdienste zu schützen?