4085/J
vom 06.03.2015 (XXV.GP)

Anfrage

der Abgeordneten Albert Steinhauser, Freundinnen und Freunde an die Bundesministerin für Inneres

betreffend Überwachung des Internets

BEGRÜNDUNG

Die NGO für BürgerInnenrechte Arbeitskreis Vorratsdatenspeicherung (kurz AK Vorrat) plant anhand eines Handlungskataloges zur Evaluierung von Anti-Terror-Gesetzen (HEAT) unterschiedlichste Formen von staatlicher Überwachung zu beleuchten. Im Rahmen dieses Projekts sind einige Fragen aufgetreten.

In der folgenden Anfrage geht es um die Überwachung des Internetverhaltens mit Methoden abseits einer Überwachung des Zielrechners. Dies umfasst Datenerhebung im Transit und bei DiensteanbieterInnen.

Die unterfertigenden Abgeordneten stellen daher folgende

ANFRAGE

1) Haben die österreichischen Behörden Zugriff auf die Internet-Backbones und Datencenter wie den Vienna-Internet-Exchange (VIX) und Interxion (VIE1)?
2) Wenn ja, von welcher Art ist dieser Zugriff?
3) Haben die österreichischen Behörden direkten Zugriff auf den Verkehr durch die Rechenzentren von Telekommunikationsunternehmen wie z. B. A1, UPC, Hutchinson 3, T-Mobile oder Tele2?
4) Wenn ja, von welcher Art ist dieser Zugriff?
5) Gibt es Equipment der Behörden in den Netzen oder Datencentern dieser Firmen?
6) Was ist die Position der österreichischen Bundesregierung bezüglich der Hinweise darauf, dass die NSA allen Verkehr, der über den VIX läuft, kopiert und auswertet?

7) Gibt es Erkenntnisse über die Unternehmen und/oder Behörden, welche der Trojaner „Regin“[1] in Österreich laut dem Bericht der Firma „Symantec“ infiziert haben soll?
8) Befinden sich unter den infizierten Zielen Firmen im Telekombereich?
9) Wenn ja, welche?
10) Welche Schutzmaßnahmen wurden nach dem Bekanntwerden von gezielten Trojaner-Attacken auf österreichische Ziele ergriffen?
11) Gibt es im BMI neue Überlegungen, von den Internetprovidern wie schon 2008 eine "österreichische Branchenlösung"[2] zur Internetüberwachung zu verlangen?
12) Gibt es im BMI Pläne, eigene Geräte in den Räumlichkeiten von Internetprovidern zu installieren, um den Aufbau einer verschlüsselten Verbindung mit einem sozialen Netz brechen bzw. verhindern zu können?
13) Welche Software kommt für den Zweck Open Source Intelligence (OSINT) zum Einsatz?
14) Welche Software kommt für den Zweck von Profiling zum Einsatz?
15) Welche Software wird zur Beobachtung von NutzerInnen und/oder nutzerInnengenerierten Inhalten im Internet eingesetzt?
16) Welche Software wird zur Identifikation speziell von Gefahrenpotentialen in social-media Plattformen eingesetzt?
17) Welche Software kommt zur Beobachtung von online Foren und sozialen Medien zum Einsatz?
18) Mit welchen social-media-, PR- oder Beratungsagenturen bestehen Geschäftsbeziehungen und welche Aufgabengebiete umfassen diese Geschäftsbeziehungen?
19) Mit welchen Sicherheitsfirmen, Beratungsagenturen und DienstleisterInnen im Bereich Netzwerk- und Kommunikationsüberwachung bestehen Geschäftsbeziehungen und welche Aufgabengebiete umfassen diese Geschäftsbeziehungen?
20) Inwiefern werden die Systeme DIANA/DIANGO in Ihrem Vollzugsbereich eingesetzt?
21) Wenn ja, mit welchen Mitteln in welcher Höhe wurden die Projekte DIANA/DIANGO[3] bereits gefördert und welche weiteren Ausgaben sind geplant?
22) Welche technischen Sicherheitsvorkehrungen hat das BMI getroffen, um die Daten der BesucherInnen von BMI.gv.at zu schützen?
23) Sind auf der Website des BMI externe DienstleisterInnen eingebunden, die ebenfalls Log-Dateien erheben?
24) Welche Daten über Besuche von Behördenwebseiten werden erfasst, und in welcher Form werden sie ausgewertet?

---

1 Siehe http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf http://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html#ref=nl-international

2 http://www.fuzo-archiv.at/artikel/293368v2

3 http://derstandard.at/2000004325700/Projekt-Diana-Bundesheer-testet-Internet-Beobachtungssystem

25) In welcher Form und für wie lange werden solche Daten und Auswertungen gespeichert und unter welchen Umständen werden sie mit Dritten geteilt?
26) Werden die Auswertungen über die BesucherInnen von Behördenwebseiten für Zwecke der Strafverfolgung verwendet?
27) An welchen Standorten und Veranstaltungen wurde bzw. wird das System „iObserve“[4], „iObserve NG”[5] oder ein darauf aufbauendes System eingesetzt oder getestet?

[4] http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=18&cHash=1b9806fd280d8f1b648047f8884714e2

[5] http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=37&cHash=f44685bc6dd8cbd27f9d664cf5ce64da