Sicherheitsbehörden lesen im Internet eifrig mit

Eine Zustandsbeschreibung der gegenwärtigen Geheimdienstaktivitäten in diversen Ländern

Von IT-Journalist Peter Welchering

Internetüberwachung ist nicht nur für die angelsächsische Geheimdienstallianz aus den USA, Großbritannien, Kanada, Neuseeland und Australien ein altes Thema, sondern auch für die Geheimdienste in China und Russland. In Deutschland mischen der Bundesnachrichtendienst, der Militärische Abschirmdienst und die Ämter für Verfassungsschutz in diesem Überwachungsgeschäft mit.

Die angelsächsischen Dienste tauschen dabei recht intensiv Daten und Überwachungsmethoden aus, China kooperiert hier sehr stark mit dem militärischen Nachrichtendienst Nordkoreas, der in der chinesischen Grenzstand Dandoong eine eigene Überwachungsstation unterhält.

Russland strukturiert nach der Integration des technischen Geheimdienstes SSSI in den Nachrichtendienst des Präsidenten die Überwachungsaktivitäten um und engagiert verstärkt Sicherheitsunternehmen für konkrete Überwachungs- und Analyseprojekte. Das macht übrigens der technische Geheimdienst der USA, die National Security Agency, ganz ähnlich. Insidern zufolge erledigen private Auftragnehmer mehr als 60 Prozent der Überwachungs- und Analysetätigkeit der NSA. Auch der ehemalige Überwachungsspezialist Edward Snowden war nicht direkt bei der NSA angestellt, sondern bei einem Sicherheitsunternehmen.

Privatfirmen verdienen viel Geld mit Spionage

Alle Geheimdienste unterliegen den gesetzlichen Regelungen ihrer Länder, arbeiten also in ihrer Spionagetätigkeit legal, verletzen aber in der Regel entsprechende Gesetze in den Zielländern. Und die Geheimdienste arbeiten über die Sicherheitsbehörden ihrer Länder in der Regel auch mit Telekommunikationsunternehmen, Internet-Service-Providern und Kabelgesellschaften zusammen.

Telekommunikationsunternehmen erlauben den Zugriff auf ihr Leitungsnetz und halten eigens standardisierte Abhörschnittstellen vor. Internet-Service-Provider halten Verbindungsdaten bereit und Informationen darüber, welche Personen welche Internet-Protokoll-Adressen nutzen oder genutzt haben. Betreiber von sozialen Plattformen und Netzwerken liefern Rohdaten ihrer Nutzer so aufbereitet, dass Analyseprogramme sehr schnell Verhaltens- und Persönlichkeitsprofile

erstellen können. Softwarehersteller stellen ihr Wissen über Schwachstellen bereit, die ausgenutzt werden können, um Computersysteme zu infiltrieren und Online-Untersuchungen durchführen zu können.

Die Briten setzen Maßstäbe

Bei der Auswertung arbeitet das britische Government Communication Headquarter im wesentlichen mit zwei Methoden: Zum einen wird direkt nach Stichwörtern in Mails oder beim Abhören von Telefongesprächen gesucht. Angeführt wurde diese 150.000 sogenannte Verdachtswörter umfassende Stichwortliste vom Suchbegriff "Mostazafin", das ist die verdeckt arbeitende iranische Einkaufsorganisation für Rüstungsgüter.

Wer dieses Wort in seiner Mail stehen hatte oder in einem überwachten Telefongespräch erwähnte, der wurde dann gesondert überwacht. Zum zweiten haben die Briten ihnen bekannte IP-Adressen und Telefonnummern aus den 21 Petabyte Daten herausgefischt, um die damit verbundenen Mails und Telefongespräche gesondert inhaltlich auszuwerten. Und natürlich haben die Briten große Teile dieser Daten an die NSA weitergereicht. Denn die NSA hat das technisch ausgereiftere Analyseprogramm.

Die baut nämlich gerade ein Bluffdale, im US-Bundesstaat Utah, ein Rechenzentrum, dessen Server im Endausbau bis zu einer Trillion Terabyte verarbeiten und auswerten können sollen. Gestartet wird im Herbst 2013 mit etwas mehr als einer Billion Terabytes. Das ist aber immer noch erheblich mehr als die Briten mit ihrem Rechenzentrum in Cheltenham schaffen. Dort arbeiten sie mit Auswertungsservern, die gerade einmal eine Million Terabyte analysieren können.