Dirk Fox

PRISM und TEMPORA

Hintergrund

Staatliche Überwachung erfordert nicht unbedingt einen „Staatstrojaner" – ein solcher Mechanismus ist, ähnlich dem „großen Lauschangriff", eher Ultima Ratio: nicht allein wegen der Tiefe des Eingriffs in den persönlichen Schutzbereich der Betroffenen, sondern vor allem wegen des mit dessen Einsatz verbundenen Aufwands.

Überwachung – insbesondere geheimdienstliche – erfolgt, wie bereits aus den Erkenntnissen um Echelon bekannt, in erster Linie flächendeckend: Erst werden die Kommunikationsbeziehungen analysiert, dann etwaige „Datensammlungen", und erst zuletzt die Endsysteme der Kommunikation („Quellen-TKÜ"). Dabei liefert die Rasterfahndung im (Telefon- und Daten-)Netz, die sich auf Schlüsselworte und Kontaktnetzwerke konzentriert, erste Hinweise, die dann durch vertiefte Analysen erhärtet oder widerlegt werden.

Die Programme PRISM und TEMPORA wurden durch Berichte des britischen Guardian und der Washington Post öffentlich. Sie basieren auf Materialien des Amerikaners Edward Snowden, Mitarbeiter der Beratungsgesellschaft Booz Allen Hamilton, der als IT-Techniker in einem NSA-Büro Zugriff auf entsprechende geheime Unterlagen hatte und diese Anfang Juni 2013 an die Presse weitergeleitet hatte.

Technische Möglichkeiten

Bereits seit einer Weile ist bekannt, dass die NSA (*National Security Agency*) Zugriff auf Telefonie-Verbindungsdaten der Anbieter Verizon, AT&T und Sprint Nextel hat, sowie auf E-Mail-Metadaten, durchgeführte Internetrecherchen und Kreditkartenzahlungen. Nach Angaben der New York Times wird im Auftrag der Nachrichtendienste auch der internationale Briefverkehr zur Gewinnung der Adressdaten mit Hilfe des Programms „Mail Isolation Control and Tracking" (MICT) gescannt.

Aber der Zugriff erfolgt auch direkt über zentrale Netzknoten, wie u. a. einem AT&T-Datacenter in San Franzisco, bei dem die Daten aus Glasfaserleitungen ausgeleitet und (in Echtzeit) analysiert werden. Auch der britische Geheimdienst GCHQ (*Government Communications Headquarters*) verfügt über einen Zugang zu transatlantischen Glasfaserkabeln und hat damit Zugriff auf E-Mails, Telefongespräche oder auch WWW-Seitenzugriffe und Einträge in Soziale Netze.

Alle diese Rasterfahndungs-Analysen über Schnittstellen bei TK- und Internet-Providern oder zentrale Interkontinental-Verbindungen werten – soweit bekannt – überwiegend Verbindungsdaten aus und suchen nach Schlüsselworten: wer verwendete wann in Verbindung mit wem welches Schlüsselwort?

Die Programme PRISM (NSA) und TEMPORA (GHCQ) gehen hingegen weit über solche Verkehrsanalysen hinaus. Soweit bekannt, erhält die NSA auf Wunsch direkten Zugriff auf Kundendaten von US-Anbietern – insbesondere Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL und Apple. Dieser Zugriff umfasst E-Mails, Chats, Videos, Fotos, Datenübertragungen und Videokonferenzen. Hinzu kommt die Bereitstellung der in Sozialen Netzen publizierten Daten, gepflegte Kontakte und auf Servern der Anbieter gespeicherte Daten (Backups etc.). Voraussetzung für den Zugriff: Die Zielperson ist „wahrscheinlich" ein Ausländer.

Dabei handelt es sich nicht um geringe Betroffenenzahlen: Bekannt[1] ist, dass Anfang April 2013 mehr als 110.000 Personen unter einer solchen Überwachung der NSA standen – ohne richterlichen Beschluss, ja selbst ohne erhärteten Tatverdacht, sondern offenbar lediglich aufgrund der Einschätzung eines NSA-Analysten.

Das seit 2011 betriebene Programm TEMPORA des britischen GHCQ analysiert mehr als 200 Glasfaserverbindungen – und geht weit über eine Schlüsselwort-Suche hinaus: Die Kommunikationsdaten werden vollständig ausgeleitet und über 30 Tage gespeichert. Angeblich werden dabei neben E-Mails, Einträgen in Sozialen Netzwerken und Internet-Nutzungen auch Telefongespräche in Text konvertiert und analysiert.

Anders als beim deutschen Äquivalent, dem Auslandsgeheimdienst BND, stehen die Aktivitäten der NSA und des GHCQ weder unter parlamentarischer Kontrolle, noch sind – wie in Deutschland – die Schlüsselwort-Analysen auf maximal 20% der Übertragungskapazität der Auslandsverbindungen beschränkt.

Fazit

Überraschend an den jüngsten Veröffentlichungen ist weniger die Tatsache der Überwachung an sich, als vielmehr deren Umfang. Hunderttausende Menschen werden – unter Umgehung jeder rechtsstaatlichen Unschuldsvermutung – in erheblichem Umfang in ihren Netz- und Kommunikationsaktivitäten überwacht. Durch den regen internationalen Austausch der Erkenntnisse zwischen den Diensten wird zudem das rechtstaatliche Verbot der nachrichtendienstlichen Inlandsüberwachung ausgehöhlt.

1 Holger Bleich: *Globaler Abhörwahn*. c't magazin für Computertechnik, Heft 16/2013, 15.07.2013, S. 112-117.