Private Rasterfahndung

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Profiling und Geolocation mittels Open-Source-Tool und GSM-Daten

Ob Terrorist, Mafiosi oder ganz normaler Facebook-Nutzer: In Computernetzen verrät sich letztlich jeder. Wer das nicht will, sollte zu allererst sein Handy abmelden. Genau über derartige Privatsphäre- und Datenschutz-Aspekte sprachen internationale IT-Experten auf der IT-Defense 2011.

Der Schwerpunkt der diesjährigen IT-Defense 2011 in Seeheim bei Frankfurt lag auf der alltäglichen Datenspur, die Handy-Nutzer und Facebook Freunde hinterlassen. Die Tools zur Analyse solcher Daten stehen für jedermann kostenlos im Netz.

Einer Open-Rasterfahndung steht somit nichts im Wege, wenn man nur die richtige Software besitzt. Der Deutsch-Südafrikaner Chris Böhme entwickelt zusammen mit Kollegen dazu das Informationsbeschaffungs- und Visualisierungstool „Maltego“, ein mächtiges Werkzeug, um aus E-Mail- und Netzwerk-Adressen Rückschlüsse über soziale Netze zu gewinnen.

Maltego basiert auf einer Client-Server Infrastruktur. Der Server steht beim Hersteller Paterva, der auch APIs zu sozialen Netzwerken besitzt. Ursprünglich war das Tool nur dazu gedacht, vernetzte Webseiten und Whois-Daten graphisch anzuzeigen. Inzwischen sind Google, PGP sowie Linkedin und Facebook als Datenquellen hinzugekommen.

Über die Domain und die E-Mail-Adresse arbeitet sich das Programm zu immer mehr Informationen durch. Die Programmierer haben gezeigt, dass man mit etwas Aufwand die in den USA so wichtige Sozialversicherungs-nummer eines Bürger knacken kann, die ihrerseits wieder als Ausweis für viele Behörden dient.

Dank der graphischen Ausgabe liefert Maltego Art und Umfang von Vernetzungen. So sieht Google China graphisch klar anders aus als ein Google-Vernetzungsbild von anderen Ländern. Der Internet-Verkehr in der Volksrepublik läuft nämlich über zentrale Gateways und wird kontrolliert. Das alles wussten wir zwar schon vorher, jetzt lassen sich aber alle Staaten und Unternehmen überprüfen – und zwar immer wieder aufs Neue.

Networking-Tool für jedermann

Eine kostenlose Version von Maltego steht auf der Paterva-Website für die Allgemeinheit bereit, die kostenpflichtige Profi-Version ist vor allem für Firmen und Behörden gedacht. Da man um den Wert von Informationen weiß, zeichnet der Hersteller des Tools dieselben mit. Was er damit macht, weiß niemand.

Als Bündel wirken die Informationen fast schon wie eine Waffe. Denn die dynamische Netzwerk- und Textanalyse legt soziale Beziehungen von Menschen offen, von denen man nicht mehr weiß als den Namen. Was dann noch fehlt, liefert die moderne Kommunikationstechnik.

Die daraus entstehenden Graphiken sind höchst aufschlussreich. Wer kennt wen? Wer ist abhängig von wem? Von großer Wichtigkeit sind diese Methoden aktuell bei dem Versuch, in arabischen Terrornetzwerken die führenden Köpfe ausfindig zu machen, Kuriere und Mitläufer zu eruieren und schließlich potentielle Attentäter zu identifizieren.

Soziale Kontakte überführen Saddam Hussein

Major Brian J. Reed suchte mit diesen Techniken von März 2003 bis März 2004 im Irak nach Saddam Hussein und wurde fündig. Von entscheidender Bedeutung war dabei ein zufällig gefundenes Fotoalbum.

Anhand der Aufnahmen gelang es Reed und seinen Männern, ein präzises mathematisches Abbild der verwandtschaftlichen, freundschaftlichen und beruflichen Beziehungen des Diktators zu gewinnen. In diesem Netzwerk war der frühere Machthaber des Irak gefangen, ohne dass er es ahnte.

Die US-Streitkräfte überprüften jeden möglichen Fluchtort. Schließlich schnappte die Falle bei einem Bekannten zu und er wurde gefangengenommen. Wie die deutsche Software-Ingenieurin und Mathematikerin Jana Diesner unterstrich, sei es so bereits auch etlichen Mafiosi ergangen. Dank Open-Source-Projekten wie Maltego ist es heute aber nicht länger ein Privileg von Regierungsstellen, soziale Raster anzulegen.

Geolocation auf Basis der GSM-Einwahldaten

Auf ein weiteres Sicherheitsrisiko wies der Berliner IT-Berater und Krypto-Experte Karsten Nohl hin. Jeder Handy- oder Smartphone-Nutzer zieht – mehr oder weniger unwissentlich – eine breite Datenspur aus Geodaten hinter sich her.

Ursache sind laxe Regeln aus der Zeit des Post- und Fernmeldemonopols. Sie stammen aus einer Zeit, als alle Telekommunikationsanbieter (Telkos) noch staatlich waren und wie eine Behörde funktionierten. Das ist lange her.

Verantwortlich ist der SMS-Dienst des digitalen Mobilfunks: Jedes der zahlreichen Telko-Unternehmen weltweit hat das Recht, den Standort jedes GSM-Handys zu erfahren. Es fragt dazu die angeschlossenen Rechner, ob sich das entsprechende Handy irgendwo eingebucht hat. Ist das der Fall, so liefert die zuständige Telko fast immer gleich auch noch die Basisstation mit. Die Lokalisierung funktioniert auch dann, wenn gar keine SMS verschickt werden soll.

Neugierige, die einen auskunftswilligen Provider finden, können so jedes Handy im weltweiten GSM-Telko-Netz lokalisieren. Die verlangten Gebühren betragen gerade einmal Cent-Bruchteile je Anfrage. Der Nutzer ahnt von all dem nichts. Über die International Mobile Subscriber Identity (IMSI) ist zudem jedes Mobiltelefon weltweit eindeutig identifizierbar.

Wem vor so viel Big Brother schaudert, für den hat Chris Böhme einige Tipps parat: Keine Fotos mit Geo-Informationen versehen, die EXIF-Informationen kontrollieren, keine Bilder tauschen und natürlich viele, nicht vorhersagbare E-Mail-Adressen verwenden, die sich nicht vernetzen lassen. Vorname.Nachname@Firmenname ist megaout.

searchsecurity.de 17.03.11