

TOP SECRET//COMINT//REL TO USA, AUS, AN, GBR, NZL

Network Analysis Center

SECURITY AGENCY
SIGDEV
SIGINT Development

(S//REL TO USA, FVEY) NSA: How Network Mapping is Helping to Target the Credit Card Authorization Networks

(U//FOUO)

NSA, Network Analysis Center
2010 SIGDEV Conference

09/13/13

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20330108

1

TOP SECRET//COMINT//REL TO USA, FVEY

(S//REL TO USA, FVEY) Document Collection Access Points

09/13/13 TOP SECRET//COMINT//REL TO USA, FVEY 35

SECRET//REL TO USA, FVEY

(U) Pursuit Goals

- (S//REL TO USA, FVEY) Collect, parse and ingest transactional data for priority credit card associations, focusing on priority geographic regions.
- (S//REL TO USA, FVEY) Identify the locations of large stores of cardholder data; identify and overcome the challenges to collection
- (S//REL TO USA, FVEY) Produce actionable intelligence from credit card data.

09/13/13 SECRET//REL TO USA, FVEY 6

NSA-Präsentation 2010: „Transaktionsdaten wichtiger Kreditkartenbetreiber“

SPIONAGE

„Folge dem Geld“

Der US-Geheimdienst NSA überwacht auch Banken und Kreditkartentransaktionen. Die europäische Swift-Genossenschaft, die den internationalen Geldverkehr abwickelt, wird gleich mehrfach angezapft.

Das Geld, das der Geschäftsmann aus dem Nahen Osten in ein anderes Land der Region überweisen wollte, sollte nicht auffallen. Gut 50 000 Dollar wollte er transferieren – und er hatte klare Vorstellungen, wie das zu geschehen habe. Die Aktion dürfe nicht über die Vereinigten Staaten von Amerika abgewickelt werden, und der Name seiner Bank müsse geheim gehalten werden – das waren die Bedingungen, die er stellte.

Der Geldtransfer, abgewickelt im Sommer 2010, fand genau so statt – und blieb trotzdem nicht unbeobachtet. Er findet sich in vertraulichen Unterlagen des US-Geheimdienstes NSA wieder, die der SPIEGEL einsehen konnte und die sich mit den Aktivitäten der Amerikaner im internationalen Finanzsektor beschäftigen. Die Dokumente zeigen, wie umfassend und effektiv der Geheimdienst sogar globale Geldströme verfolgt und in einer eigens dafür entwickelten mächtigen Datenbank speichert.

„Follow the Money“ heißt der NSA-Zweig, der sich darum kümmert. Sein Name erinnert an den berühmten Satz des ehemaligen FBI-Vizechefs Mark Felt, der einst als Informant „Deep Throat“ den Reportern Bob Woodward und Carl Bernstein bei der Aufklärung der Watergate-Affäre 1972 empfohlen hatte, immer der Spur des Geldes zu folgen.

Finanztransfers seien die „Achillesferse“ von Terroristen, schreiben die NSA-Analysten in einem internen Bericht. Als Aufklärungsfelder für ihre „Financial Intelligence“ nennen sie daneben das Aufspüren illegaler Waffenlieferungen sowie das prosperierende Feld der Cyber-Kriminalität. Das Ausspionieren internationaler Geldflüsse könne auch dazu dienen, Staatsverbrechen und Genozide zu enthüllen oder zu überwachen, ob Sanktionen eingehalten würden.

„Geld ist die Wurzel allen Übels“, scherzen die Geheimdienstler. Ihre Aktivitäten zielen den Unterlagen zufolge

im Kern auf Regionen wie Afrika oder den Mittleren Osten – und sie betreffen oft Ziele, die ihrem gesetzlichen Spähauftrag entsprechen. Doch wie in anderen Bereichen setzt die NSA auch im Finanzsektor auf maximale Datenausbeute – wodurch sie offenbar mit nationalen Gesetzen und internationalen Abkommen in Konflikt gerät.

Selbst Geheimdienstler sehen die Schnüffeleien im Weltfinanzsystem jedenfalls mit einer gewissen Sorge, wie aus einem Dokument des britischen Geheimdienstes GCHQ hervorgeht, das sich aus rechtlicher Sicht mit „Finanzdaten“ und der eigenen Zusammenarbeit mit der NSA in diesem Feld befasst. Das Sammeln, Speichern und Teilen der „politisch sensiblen“ Daten sei ein tiefer Eingriff, schließlich handle es sich um „Massendaten voller persönlicher Informationen“, von denen „viele nicht unsere Ziele betreffen“.

Tatsächlich enthielt allein die zentrale NSA-Finanz-Datenbank namens Tracfin,

in der die „Follow the Money“-Ausspähergebnisse zu Überweisungen, Kreditkartentransaktionen und Geldtransfers gesammelt werden, geheimen Dokumenten zufolge 2011 bereits 180 Millionen Datensätze. 2008 waren es lediglich 20 Millionen gewesen. Die meisten Tracfin-Daten würden fünf Jahre gespeichert, heißt es darin.

Laut den internen Unterlagen hat der Geheimdienst sogar mehrere Zugänge zum internen Datenverkehr der Swift-Genossenschaft, über die mehr als 8000 Banken weltweit ihren Zahlungsverkehr abwickeln. Andere Institute nimmt die NSA gezielt und individuell ins Visier. Zudem hat der Dienst offenbar tiefe Einblicke in die internen Prozesse von Kreditkartenfirma wie Visa und Mastercard. Und selbst neue, alternative Währungen und vermeintlich anonyme Zahlungsmittel wie die Internetwährung Bitcoin gehören zu den Zielen der amerikanischen Späher.

Die gesammelten Erkenntnisse liefern dabei oft ein komplettes Bild zu Individuen, inklusive Reisebewegungen, Kontaktpersonen und Kommunikationsverhalten. Als Erfolgsbeispiele nennt der Geheimdienst unter anderem Vorgänge, in denen Banken aus der arabischen Welt auf schwarze Listen des US-Finanzministeriums gesetzt wurden.

In einem Fall hatte die NSA Belege für deren Beteiligung an illegalem Waffenhandel geliefert, in einem anderen ging es um die Unterstützung eines autoritären afrikanischen Staats. Politisch brisant sind aber vor allem die heimlichen Zugriffe auf Swift-Netzwerke. Die EU hatte 2010 nach langen Debatten das sogenannte Swift-Abkommen mit den Vereinigten Staaten geschlossen. Swift sitzt in Belgien und wickelt für Banken und andere Finanzinstitutionen deren internationalen Zahlungsverkehr ab. Jahrelang hatten die USA nach den Terroranschlägen vom 11. September 2001 darauf gedrängt, Zugang zu diesen internationalen Finanzdaten zu erhalten, auf die Swift ein Quasi-Monopol besitzt.

Ein erstes Abkommen scheiterte Anfang 2010 am Veto des Europäischen Par-

laments. Einige Monate später wurde ein leicht entschärftes Swift-Abkommen unterzeichnet – mit dem Segen der Berliner Bundesregierung.

Unterlagen der NSA, die aus dem Archiv des Whistleblowers Edward Snowden stammen, zeigen nun, dass die USA den mit der EU erzielten Kompromiss offenbar unterlaufen. Ein Dokument aus dem Jahr 2011 bezeichnet das Swift-Computernetzwerk klar als „Ziel“. Unter anderem beteiligt ist an den Spähaktionen die NSA-Abteilung für „maßgeschneiderte Operationen“.

Einer der verschiedenen Zugangswege zu den Swift-Informationen besteht den Dokumenten zufolge seit 2006. Seither

der Forderung nach Aussetzung des Abkommens angeschlossen.

Der Konflikt ist auch deshalb so heikel, weil aus den Dokumenten hervorgeht, wie eng das US-Finanzministerium bei der Auswahl der Ausspähziele für das Programm eingebunden ist. So gibt es den Unterlagen zufolge einen personellen Austausch, bei dem NSA-Analysten für jeweils mehrere Monate in die zuständige Abteilung des US-Finanzministeriums wechseln.

Ähnlich brisant ist das Ausspähen von Kreditkartentransaktionen. Unter dem Codenamen „Dishfire“ sammelt der Nachrichtendienst beispielsweise Infor-

Die NSA scheint auch im Finanzsektor alles mitzunehmen, was sie kriegen kann.

könne man den „Swift-Druckerverkehr zahlreicher Banken“ auslesen.

Nach der Verwanzung der EU-Botschaften in New York und Washington könnte der NSA-Angriff auf Swift der nächste große Stresstest für die Beziehungen zwischen amerikanischer Regierung und Europäischer Union werden. Die NSA äußerte sich bis zum SPIEGEL-Redaktionsschluss am Freitag vergangener Woche nicht zu den jüngsten Vorwürfen.

EU-Innenkommissarin Cecilia Malmström forderte Ende der Woche jedenfalls, die Amerikaner sollten „uns sofort und präzise sagen, was passiert ist, und alle Karten auf den Tisch legen“. Wenn es wahr sei, „dass sie die Informationen mit anderen Behörden teilen, für andere Zwecke, als das Abkommen vorsieht ... müssen wir darüber nachdenken, das Abkommen zu beenden“, drohte die Schwedin, nachdem der brasilianische Sender TV Globo am vorvergangenen Wochenende erstmals über den Angriff auf Swift berichtet hatte.

Von einem „offenen Rechtsbruch“ spricht der Grüne Jan Philipp Albrecht. Mittlerweile haben sich vier der sieben Fraktionen im Europäischen Parlament

mationen über Kartentransaktionen von etwa 70 Banken weltweit, die meisten aus Krisenstaaten. Betroffen sind aber auch Banken in Italien, Spanien und Griechenland. Dabei machen sich die Amerikaner zunutze, dass viele Banken ihre Kunden per SMS über ihre Transaktionen unterrichten. Das Programm läuft seit dem Frühjahr 2009.

Der Dienst nimmt den Unterlagen zufolge ebenfalls große Kreditkartenbetreiber selbst ins Visier – nach eigenen Angaben etwa den US-Konzern Visa. So beschrieben NSA-Analysten auf einer internen Konferenz im Jahr 2010 ausführlich und detailliert, wie sie im komplexen Netz, über das der US-Konzern seine Transaktionen abwickelt, nach möglichen Anzapfpunkten forschten – angeblich erfolgreich.

Ziel seien die Transaktionen von Visa-Kunden in Europa, dem Nahen Osten und in Afrika gewesen, heißt es in einer Präsentation. Es gehe darum, „die Transaktionsdaten von führenden Kreditkartenunternehmen zu sammeln, zu speichern und zu analysieren“. Eine Folie zeigt detailliert, wie der Autorisierungsprozess jeder Transaktion, ausgehend vom Kartenlesegerät in einem Laden, über die Bank und einen Datenverarbeiter bis hinauf zur Kreditkartenfirma selbst abläuft. Eine weitere Darstellung führt dann mögliche „Sammelstellen“ auf.

Auf Anfrage schloss eine Visa-Sprecherin aus, dass Daten aus den vom Unternehmen selbst betriebenen Netzen abfließen könnten. „Visa Inc. besitzt keine Rechenzentren im Nahen Osten oder in Großbritannien.“ Im Übrigen sei es Politik des Unternehmens, nur auf richterlichen Beschluss oder gemäß den jeweils geltenden rechtlichen Grundlagen Informationen an Behörden weiterzugeben.

Visa-Daten aus dem Nahen Osten landen jedenfalls in der NSA-Datenbank – über das Spähprogramm XKeyscore wür-



Swift-Zentrale bei Brüssel: „Die Wurzel allen Übels“

CHRISTIAN WEIDEMANN, RICARDO BOFILL, TALLER DE ARQUITECTURA / AP

den regionale Daten aus dem Visa-Netzwerk abgeschöpft, heißt es in einem Dokument.

Die Schnüffel-Bemühungen betreffen indes nicht nur einen Anbieter. In die NSA-Finanzdatenbank Tracfin fließen einem weiteren Dokument zufolge Transaktionsdaten verschiedenster Kreditkartenfirmen ein. Unter anderem seien darin auch Daten aus den Zahlungsautorisierungsprozessen von Visa und Mastercard enthalten. Insgesamt machen „Kreditkartendaten“ und diesbezügliche SMS im September 2011 84 Prozent der Datensätze innerhalb von Tracfin aus.

Mastercard äußerte sich bis zum Redaktionsschluss dieser Ausgabe nicht.

Um sich im Dschungel der Informationen zurechtzufinden, gibt es für Tracfin-Analysten sogar einen eigenen Leitfaden für die „Kreditkarten-Suche“. Die Geheimdienstler verfügen obendrein über ein elektronisches Werkzeug, mit dem sie eigenständig und sehr schnell die Echtheit von Kreditkarten prüfen können.

Die NSA scheint jedenfalls auch im heiklen Finanzsektor alles mitzunehmen, was sie kriegen kann. So zumindest liest sich eine Präsentation aus dem April. Aufgabenstellung der NSA sei es gewesen, den „Zugang zu einer großen Menge von Finanzdaten“ zu finden, um sie in die Tracfin-Datenbank einzuspeisen, heißt es darin. Man sei durch Netzwerkanalysen und den Einsatz des Spähprogramms XKeyscore auf den verschlüsselten Datenverkehr eines großen Finanz-Netzwerkbetreibers im Nahen Osten gestoßen.

Früher habe man dort nur Zahlungsverkehre von Bankkunden entschlüsseln können, nun habe man zudem Zugriff auf die interne verschlüsselte Kommunikation der Unternehmensniederlassungen. Das Sorge für „einen neuen Strom von Finanzdaten und möglicherweise auch verschlüsselter interner Unternehmenskommunikation“ des Finanzdienstleisters, frohlocken die Analysten. Die Bankdaten, die so auslesbar würden, kämen aus Ländern, die von „großem Interesse“ seien. Ganz nebenbei ist das Unternehmen einer der vielen Servicepartner von Swift.

Die Unterlagen zeigen allerdings auch, wie kurzlebig die Zugänge der Geheimdienste in die Finanzwelt sein können – und dass Verschlüsselung die Schnüffler eben doch vor Probleme stellen kann, zumindest zeitweise. Lange habe man Zugang zu den Daten von Western Union gehabt, heißt es in einem Dokument. Das Unternehmen organisiert Geldtransfers in mehr als 200 Ländern. Doch 2008 habe Western Union damit begonnen, seine Daten hochgradig zu verschlüsseln. Der Zugriff sei dadurch fast unmöglich geworden, klagen Mitarbeiter der NSA in einem der Papiere.

Laura Poitras,
Marcel Rosenbach, Holger Stark



Emirates-Mitarbeiterinnen: Keine Steuern, aber leben wie im Schwesternwohnheim

LUFTFAHRT

Von wegen Saftschubse

Wie wird man Stewardess – und warum eigentlich noch? Die arabische Airline Emirates veranstaltet in Deutschland Castings – und demütigt damit den Konkurrenten Lufthansa.

Das Tor zur Welt ist an diesem Samstagmorgen der Eingang eines nüchternen Hotelkonferenzraums am Stuttgarter Hauptbahnhof. 17 junge Frauen und 2 Männer warten auf Einlass. Die Frauen tragen roten Lippenstift und schwarze Pumps. Sie sind nicht zum Spaß hier, sondern wollen sich einen Traum erfüllen, den Traum vom Fliegen.

Und die arabische Fluggesellschaft Emirates will ihnen dabei helfen. Sie sucht zurzeit nicht nur 500 Aushilfs-Stewardessen wie die Lufthansa, sondern 3800 Flugbegleiter und Flugbegleiterinnen, in Vollzeit.

Einen besseren Beweis für die fulminante Expansionsfreude der Airline aus dem arabischen Emirat Dubai könnte es kaum geben – und wohl auch kaum eine bessere Möglichkeit, den deutschen Konkurrenten Lufthansa zu ärgern, der von einem Sparprogramm ins nächste trudelt. Neue Stewardessen werden von den Deutschen derzeit allenfalls als befristete Saisonkräfte eingestellt.

Emirates dagegen lässt es krachen – mit international veranstalteten Casting-Events, die wellenweise auch in deutschen Metropolen abgehalten werden. Sie dürften wohl alle ähnlich ablaufen wie die Auslese, die jüngst in Stuttgart zu besichtigen war.

Vorne steht dann oft Helena el-Haber, 30, dunkle Locken und Zwölfzimeterabsätze. Die gebürtige Libanesin ist so etwas wie die Heidi Klum der Luftfahrtbranche und eine von 30 Talentscouts der Airline. Auf einen PR-Film über die Metropole Dubai folgt eine Info-Runde über das Leben in dem arabischen Land. Dann warten diverse Tests. Nach jedem Schritt wird ausgesiebt, bis sechs Stunden später noch fünf Kandidaten übrigbleiben: ein Mann und vier Frauen.

Der aufwendige Prozess zeigt, welche Faszination der Job offenbar noch immer ausübt. Zudem verdeutlicht er, wie sich die Rangordnung in der internationalen Zivilluftfahrt verändert hat – und damit das Berufsbild des Flugbegleiters.

Bis in die neunziger Jahre galt eine Anstellung als Steward oder Stewardess bei der Lufthansa als Glamourjob. Die blauen Uniformen hatten fast das Prestige eines Arztkittels. Niemand wäre auf die Idee gekommen, die Servierkräfte abfällig „Saftschubsen“ zu nennen.

Dass das Image gerade bei den etablierten Airlines mittlerweile aber arg leiden musste, hat ausgerechnet mit jungen Angreifern wie Emirates und Billigfliegern wie Easyjet oder Ryanair zu tun.

Fliegen ist fast so gewöhnlich geworden wie Brötchenholen. Der Kostendruck ist gestiegen, die Privilegien der Beschäftig-