
Lobban

Prinz Charles, Herzogin Camilla bei Geheimdienstvisite, GCHQ-Chef Lobban, LinkedIn-Website

AP / DPA (O.R.)

GEHEIMDIENSTE

Ein Quantum Spionage

Elite-Teams des GCHQ nahmen gezielt Mitarbeiter von Mobilfunkfirmen und Abrechnungsdiensten ins Visier, um tief in deren Firmennetze vorzudringen. Die Spione nutzten dazu unter anderem manipulierte Kopien von LinkedIn-Seiten.

Die Belgacom-Mitarbeiter ahnten wohl nichts Böses, als sie wie üblich ihre Profile bei dem Business-Netzwerk LinkedIn aufriefen. Die Seiten sahen aus wie immer, auch die Ladezeiten fielen nicht weiter aus dem Rahmen.

So war es für die Opfer nicht zu bemerken, dass sie nicht die Originalseite zu sehen bekamen – sondern eine exakte Kopie, die mit einem unsichtbaren Extra versehen war, einer kleinen Software, die ihre Rechner fortan zum Werkzeug des britischen Geheimdienstes GCHQ machte.

Die Spione von der Insel hatten die Ingenieure bereits zuvor gründlich ausgespäht. Man habe zunächst Mitarbeiter des halbstaatlichen belgischen Telekommunikationsunternehmens Belgacom „identifiziert“, die im Bereich Wartung und Sicherheit tätig sind, heißt es in einer „streng geheim“ eingestuften GCHQ-Präsentation.

Dann habe man festgestellt, welche der in Frage kommenden Zielpersonen LinkedIn oder die in IT-Kreisen beliebte Nachrichtenseite Slashdot.org nutzten.

Die Rechner dieser „Kandidaten“ habe man dann mit einer Infiltrationstechnik namens „Quantum Insert“ infiziert, um über die Mitarbeiter tief ins interne Netz von Belgacom und des Tochterunternehmens Bics vorzudringen, das ein sogenanntes GRX-Router-System betreibt. Diese Router kommen zum Einsatz, wenn Nutzer mit ihrem Handy im Ausland telefonieren oder online gehen wollen.

Als der SPIEGEL erstmals über die „Operation Socialist“ gegen Belgacom berichtete (39/2013), löste das in Belgien staatsanwaltliche Ermittlungen aus. Gleich zwei Ausschüsse des EU-Parlaments befassen sich mit dem Angriff eines EU-Mitglieds auf den führenden Telekommunikationsanbieter eines Partnerlandes.

Dabei ist die Operation kein Einzelfall, sie ist nur eines der Prestigeprojekte einer Elite-Einheit der britischen Internetspione, die in einer Bürogemeinschaft namens MyNOC zusammenarbeitet. Die Abkürzung steht für „My Network Operations Centre“. An diesen Arbeitsplätzen kooperieren Mitarbeiter diverser GCHQ-Sparten, um besonders knifflige Aufträge auszuführen. Ein MyNOC ist eine Art Spezialeinheit für das Eindringen in fremde Netze. Die Mitarbeiter hacken im Dienste Ihrer Majestät.

Am vorigen Donnerstag gab sich der Chef des GCHQ, Iain Lobban, im britischen Parlament Mühe, die von den bisherigen Enthüllungen aufgeschreckten Abgeordneten zu beruhigen. Großbritannien sei Opfer von Industriespionage, dem könne man nicht tatenlos zusehen. „Nur wer eine Bedrohung darstellt oder in Kontakt mit so jemandem ist“, gerate ins Visier seiner Behörde, so Lobban.

Offenbar machen sich auch Vertreter des Königshauses dann und wann persönlich ein Bild von der Schnüffelarbeit. Ein Foto zeigt den Prinzen von Wales, Charles, samt seiner Gattin Camilla, Herzogin von Cornwall, die an einem MyNOC-Arbeitsplatz namens „A Space“ umgeben von Monitoren einer Präsentation lauschen. „Eindringlinge im A Space“ ist das Bild in der GCHQ-Präsentation ironisch überschrieben.

Wie detailliert die Mitglieder der königlichen Familie über laufende Spähaktionen unterrichtet wurden, geht aus der Präsentation nicht hervor – angeblich soll es aber nicht um Belgien, sondern um Afghanistan gegangen sein.

Dem Geheimdokument zufolge hätten Charles und Camilla allerdings an Ort und Stelle neben der im Material mehrfach als „höchst erfolgreich“ beschriebenen Operation gegen Belgacom auch mehr über die ebenfalls von einer MyNOC-Abteilung gesteuerten „Operation Wylekey“ erfahren können.

Auch hier geht es um ein Thema, das die Briten zum Schwerpunkt ihrer Aufklärungsbemühungen erhoben haben: möglichst umfassende Zugänge zu den Mobilnetzwerken der Gegenwart, den kritischen Infrastrukturen für das digitale Zeitalter.

Das mobile Netz ist für Spione weltweit Fluch und Segen. Ein Fluch, weil die mobilen Netzwerke zersplittert sind, die großen Mobilfunkunternehmen betreiben jeweils eigene, das macht das Anzapfen aufwendiger. Zugleich sind die mobilen Alleskönner in unseren Hosentaschen für Geheimdienste ein Segen, weil sie oft noch mehr persönliche Informationen preisgeben können als stationäre Computer, im Zweifel sogar die Lebensgewohnheiten und den aktuellen Aufenthaltsort. Sie lassen sich auch in Abhörwanzen verwandeln, die von ihren Herren aus der Ferne jederzeit eingeschaltet werden können, um die Gespräche des Besitzers zu belauschen.

„Wir können wertvolle mobile Geräte und Dienste vollständig konvergent und auf unsere Zielperson fokussiert orten, sammeln und ausbeuten (wo angebracht, auch in Echtzeit)“, heißt es in einem GCHQ-Dokument aus dem Jahr 2011. Die britischen Spione streben bereits seit Jahren danach, potentiell jedes Handy auf dem Planeten jederzeit in ein Überwachungswerkzeug verwandeln zu können.

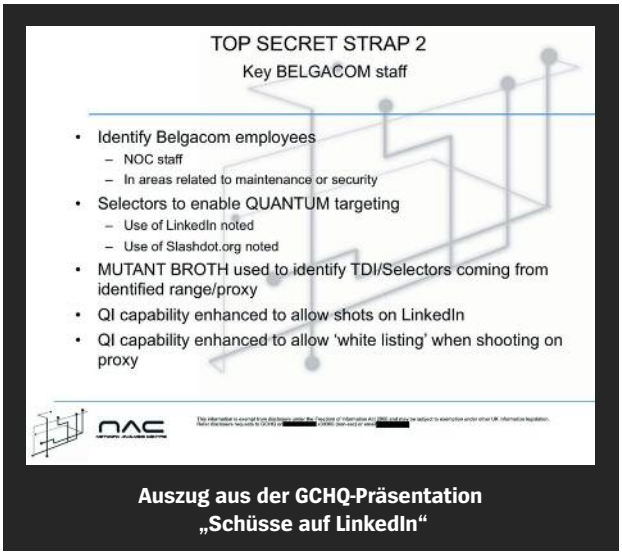
Um aber in die schwerzugänglichen Mobilnetze einzudringen, müssen die Staats-Hacker offenbar Umwege gehen.

Im Fall von Belgacom ging es der Präsentation zufolge um die „Ausbeutung von GRX-Routern“, um von dort aus sogenannte Man-in-the-Middle-Attacken auf die Smartphones der Zielpersonen zu starten. „Über diesen Weg könnte ein Geheimdienst die gesamte Internetkommunikation einer Zielperson mitlesen, deren Aufenthaltsorte bestimmen und sogar Spionage-Software auf deren Handys schmuggeln“, erklärt der Mobilfunkexperte Philippe Langlois dazu. Es handle sich um einen effektiven Ansatz – schließlich gebe es weltweit nur etwa zwei Dutzend GRX-Anbieter, aber viele hundert mit ihnen verbundene Mobilfunkanbieter.

Doch dies ist nicht das einzige Einfallstor in die Welt der globalen Mobilkommunikation, die das GCHQ für sich entdeckt hat. So zielt eine weitere MyNOC-Operation namens „Wylekey“ auf „internationale Abrechnungsfirmen für den Mobilfunk“.

Dahinter verbergen sich Unternehmen, deren Namen kaum jemand kennt. Sie wickeln den internationalen Zahlungsverkehr zwischen Mobilfunkanbietern ab und verfügen deshalb über gewaltige Mengen von Verbindungsdaten.

In der GCHQ-Präsentation, die der SPIEGEL einsehen konnte, findet sich eine ganze Liste dieser Abrechnungsunternehmen. Im Visier der Briten waren demnach primär der in Bern ansässige Anbieter Comfone und das Unternehmen Mach, das inzwischen in den Firmen Starhome Mach und Syniverse aufgegangen ist. Syniverse befand sich ebenfalls auf der Ausspähliste. Diese Unternehmen dominieren die Branche weltweit. Auch bei Mach hatten die GCHQ-Kräfte im Vorfeld gezielt „drei Netzwerkingenieure identifiziert“ – und wieder kam die „Quantum Insert“-Methode zum Einsatz.



Auszug aus der GCHQ-Präsentation „Schüsse auf LinkedIn“

Zunächst ermitteln die Spione, wer für das zum Ziel erklärte Unternehmen arbeitet – etwa über öffentliche Quellen wie das Kontaktnetzwerk LinkedIn. Besonders interessant sind für die Angreifer offenbar IT-Fachleute und Netzwerkadministratoren, denn deren Rechner versprechen weitgehende Zugriffsrechte zu den abgeschotteten Unternehmensinfrastrukturen.

Im Fall von Mach stießen sie so beispielsweise auf einen Computerfachmann, der bei der indischen Niederlassung der Firma arbeitete. Das streng geheime Dokument zeigt, wie weitgehend die britischen Geheimdienstler das Leben des unbescholtenen Mitarbeiters ausleuchteten, der fortan als „Ziel“ geführt wurde.

Eine verästelte grafische Darstellung seiner digitalen Existenz zeigt den Namen des Mannes in einem roten Fadenkreuz und listet auf, welchen Computer er dienstlich nutzt und welchen privat („vermutlich Tablet-PC“). Sein Skype-Nutzername ist aufgeführt, sein Gmail-Account und sein Profil bei einem sozialen Netzwerk, nicht einmal die Cookies auf den Rechnern des ahnungslosen Opfers blieben den Briten verborgen. Die staatlichen Hacker brachten zudem in Erfahrung, mit welcher IP-Adresse er dienstlich im Netz surft und mit welcher privat, einer indischen nämlich.

Kurz: Das GCHQ wusste alles über sein digitales Leben, er war für die Späher wie ein offenes Buch. Der SPIEGEL hat den Betroffenen kontaktiert, veröffentlicht den Namen zum Schutz seiner Privatsphäre jedoch nicht.

Das war nur die Vorbereitung, nun konnte die Abteilung Attacke übernehmen: Auf Basis dieser Informationen bauten die Spione für insgesamt sechs Mach-Mitarbeiter maßgeschneiderte digitale Angriffswaffen. „Targeting Packs für sechs Kandidaten entwickelt“, heißt es in dem Papier – individuelle Angriffsprogramme, maßgeschneidert für die Computer der Opfer.

Wie die Infektion mittels „Quantum Insert“ abläuft, hat der amerikanische IT-Sicherheitsexperte Bruce Schneier detailliert im „Guardian“ beschrieben: Danach verfügen die Dienste über superschnelle Server an zentralen Schaltstellen des Internets. Ruft ein Überwachungsziel eine bestimmte Website auf, springen diese Server an: Statt der gewünschten Seite liefern sie eine exakte Kopie aus, die aber zusätzlich den Schnüffelcode der Staats-Hacker auf den Zielrechner schmuggelt.

„Quantum“ ist weiteren Geheimdokumenten zufolge ein äußerst machtvolles Werkzeug, das in verschiedenen Varianten existiert und von der NSA entwickelt wurde. Die bei Belgacom verwendete „Quantum Insert“-Methode ist bei britischen und US-Spionen besonders beliebt. Sie kam auch bei der GCHQ-Spähattacke auf die Opec zum Einsatz (siehe Kasten Seite 98).

Die Injektionsversuche werden dienstintern als „Schüsse“ bezeichnet. Insbesondere mit der LinkedIn-Variante sind die Briten wohl recht erfolgreich. „Bei LinkedIn sieht es so aus, als würde die Erfolgsquote pro Schuss bei über 50 Prozent liegen“, heißt es dazu in einem Dokument aus dem Jahr 2012.

Wie schon die Ausspähung von Belgacom gilt „Wylekey“ hausintern als voller Erfolg: Man habe damit Detailwissen über das Unternehmen Mach, seine Kommunikationsinfrastruktur, sein Geschäft und diverse Schlüsselpersonen gewonnen, heißt es in einer „Zusammenfassung“.

Insgesamt, so steht es in einem weiteren Dokument, habe die Operation noch viel mehr erbracht: Sie habe nicht nur „unser Wissen über verschiedene Abrechnungshäuser und ihre Kunden verbessert“, son-

Gefälschte Zahlen

NSA und GCHQ spähen beide die Opec aus – Energieversorgung ist eines der großen Themen für die Geheimdienste.

Opec-Pressekonferenz in Wien 2010

XINHUA / ACTION PRESS

Im Januar 2008 vermeldete die für Energiefragen zuständige Abteilung der NSA Vollzug. Zwar habe es zuvor bereits Erkenntnisse aus einzelnen erdölexportierenden Ländern gegeben. Aber nun sei es erstmals gelungen, die Organisation der erdölexportierenden Länder (Opec) als Ganzes zu infiltrieren.

Die Zentrale der 1960 gegründeten Opec residiert in einem kastenartigen Gebäude in Wien und hat vor allem ein Ziel: den Weltmarkt für Öl zu kontrollieren – und die Preise hochzuhalten. Zu den zwölf Mitgliedstaaten zählen Saudi-Arabien, Venezuela, Iran und Irak – Länder, denen die USA misstrauen. Dazu kommt, dass das Thema Energiesicherheit eine „Top-Priorität für die Geheimdienstgemeinde“ habe, wie es in einem NSA-Dokument von 2008 heißt. Die Dringlichkeit sei umso größer, je höher die Ölpreise auf dem Weltmarkt seien.

Über das Internet drang die NSA tief in die Computer der Opec ein. In der Forschungsabteilung stießen die Auswerter auf eine interne Studie, die darlegte, dass Opec-Offizielle die Schuld an den hohen Ölpreisen Spekulanten zuschieben wollten. Ein Blick in die Dateien der Rechtsabteilung der Opec legte offen, wie sich die Organisation auf eine Kartellklage in den USA vorbereitete. Und ein Streifzug in den Arbeitsbereich des Opec-Generalsekretärs dokumentierte, dass die Saudis auch innerhalb der Organisation mit verdeckten Karten spielten. Die Erhöhung der Ölproduktion habe Riad so lange wie möglich geheim halten wollen, so die NSA-Auswerter.

Auf der Liste der auszuspähenden Personen steht zudem der saudi-arabische Opec-Gouverneur. Die entsprechende Überwachung hat sich die NSA vom zuständigen geheim tagenden US-Gericht genehmigen lassen. Die Dokumente zeigen, wie penibel die Amerikaner darauf achteten, die Überwachung auszusetzen, sobald der Saudi die USA besuchte. Doch kaum war er zurück in Riad, drangen die NSA-Leute wieder in seine Kommunikation ein.

Eine der Erkenntnisse sei, dass die Saudis falsche Ölproduktionszahlen angegeben hätten, so ein Bericht von 2010. Typische „Kunden“ für derlei Informationen seien die CIA, das US-Außenministerium und das Energieministerium, das sich prompt für die „hervorragende Bestätigung“ eines „jahrelang gehegten Verdachts“ bedankte.

Mindestens so erfolgreich wie die NSA waren auch die Briten – die ebenfalls das Wiener Hauptquartier ins Visier nahmen. Man habe bislang „traditionell schlechten Zugang“ zur Opec gehabt, heißt es in einem Geheimpapier des GCHQ. Nach längerer Tüftelphase sei es aber 2010 mittels der „Quantum Insert“-Methode gelungen, die Computer von neun Opec-Angestellten zu infiltrieren. Sogar Administratorenrechte für das Opec-Netzwerk hätten sie erlangt und sich Zugang zu zwei geheimen Servern verschafft, auf denen „viele interessante Dokumente abgelegt“ gewesen seien.

Die Opec taucht auch im „National Intelligence Priorities Framework“ auf, dem Rahmen für die Geheimdienstprioritäten, den das Weiße Haus den US-Diensten vorgibt. In der Liste vom April 2013 wird die Organisation zwar noch als Aufklärungsziel geführt – aber mit geringerer Priorität. Seit die USA aufgrund von Fracking und neuen Ölfunden weniger vom arabischen Öl abhängig sind, so kann man die Liste interpretieren, hat das Interesse an der Opec wohl nachgelassen.

dern auch „das Wissen über und den Zugang zu verschlüsselten Verbindungen zwischen den Abrechnungshäusern und verschiedenen Mobilnetzbetreibern“.

Noch enthusiastischer fielen die Zwischenberichte zum Verlauf der Belgacom-Operation aus. Man sei „tief ins Netzwerk“ der Belgier vorgedrungen und „bis an dessen Ränder“. Die Briten starteten deshalb zusammen mit den hauseigenen Verschlüsselungsspezialisten („Crypt Ops“) sogar eine „Operation Socialist II“ – um nun auch die vorgefundenen verschlüsselten Verbindungen (VPNs) zu knacken.

Auf Anfrage erklärte LinkedIn, das Unternehmen nehme die Privatsphäre und Sicherheit seiner Nutzer „sehr ernst“ und „billigt nicht, wenn seine Plattform oder falsche LinkedIn-Profile so wie beschrieben eingesetzt werden“. „Um es klar zu sagen: Wir würden eine derartige Aktivität niemals gutheißen, unabhängig welchem Zeck sie dient, und wurden über die angebliche Aktivität auch nicht unterrichtet.“

Ein Sprecher von Starhome Mach sagte, man werde „mit sofortiger Wirkung eine umfassende Sicherheitsüberprüfung starten“. Im Übrigen habe man erst kürzlich auf eine komplett neue Infrastruktur samt neuer Geräte umgestellt. Bei Comfone hieß es: „Uns liegen keine Kenntnisse vor, dass der britische Geheimdienst in unsere Systeme eingedrungen ist.“ Auch das zweite Mach-Nachfolgeunternehmen Syniverse erklärte, es sei „kein Eindringen durch Regierungsbehörden in die Rechenzentren von Syniverse oder Mach bekannt“.

Das GCHQ wollte zu Fragen des SPIEGEL keine Stellung nehmen.

Für die Briten war all das offenbar nur ein Zwischenschritt auf dem Weg zu einem größeren Ziel: Nach dem herkömmlichen Internet will das GCHQ nun auch das mobile zu einer allsehenden Überwachungsmaschine machen.

Ihre „Vision“ beschrieben die Späher des GCHQ 2011 jedenfalls so: „Jedes mobile Gerät, überall, jederzeit!“

Die Attacken auf Belgacom und die Abrechnungshäuser dienen hier nur als Türöffner. Sind die eigentlichen Mobilfunknetze der Telekommunikationskonzerne erst einmal infiltriert, bieten sich den Spionen völlig neue Ausspähchancen. „Wir sollten unsere operativen Möglichkeiten erweitern, so dass wir aus der Ferne Software implantieren können, auch wenn wir nur die MSISDN kennen“, heißt es in dem Briefing von 2011. Im Klartext: Die Telefon-Hacker vom GCHQ möchten gern jedes Handy auf der Welt zur Spionagewanze umfunktionieren können – allein auf Basis der Telefonnummer. „Das wäre bahnbrechend“, heißt es in dem Papier.

Laura Poitras, Marcel Rosenbach, Christoph Scheuermann, Holger Stark, Christian Stöcker

Wegweiser für Informanten: www.spiegel.de/briefkasten