

Gefälschte Zahlen

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



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 Geheimdienstgemeinschaft“ 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 „jahrrelang 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.

dem 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-Profilen 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 Telefonhacker 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