

10.02.2011

## Industriespionage

### Hacker aus China spähnten Ölkonzerne aus

**Industriespione aus dem Netz: Einer US-Firma für IT-Sicherheit zufolge sind fünf große Öl- und Gaskonzerne zum Opfer gezielter Hacker-Angriffe auf ihre Infrastruktur geworden. Die Cyber-Diebe stahlen wertvolle Unternehmensinterna. Und sie operierten offenbar von China aus.**

Peking/Washington - Die Diebe aus dem Netz pflegten reguläre Büroarbeitszeiten einzuhalten. Zwischen neun Uhr morgens und fünf Uhr Nachmittags - Pekinger Ortszeit - seien die Hack-Attacken auf die Rechnersysteme internationaler Ölmultis stets erfolgt. So steht es in dem [Bericht \(PDF\)](#), den das renommierte US-Sicherheitsunternehmen McAfee jetzt veröffentlichte. Welche Unternehmen konkret betroffen sind, teilte McAfee nicht mit.

"Seit November 2009 wurden verdeckte und gezielte Cyberattacken gegen globale Öl-, Energie- und Petrochemie-Unternehmen durchgeführt", heißt es in dem Papier. Dabei sei eine ganze Reihe unterschiedlicher Angriffstechniken angewandt worden: Social Engineering, also der Versuch, sich das Vertrauen von Mitarbeitern mit bestimmten Zugriffsrechten zu erschleichen, sei ebenso zum Einsatz gekommen wie Hack-Attacken, die auf bekannte Sicherheitslücken in Microsoft-Windows-Betriebssystemen zielten. Daneben wurde eine Reihe weiterer Techniken eingesetzt, etwa solche, die auf Schwachstellen in Systemen zur Fernwartung von Rechneranlagen zielten.

Die Täter waren augenscheinlich auf der Suche nach ganz bestimmten, wirtschaftlich relevanten Materialien. So seien Informationen über Projektfinanzierungen, Gebote für Aufträge und Lizenzverhandlungen für neu zu erschließende Gas- und Ölfelder entwendet worden. Solche Informationen wären "für Wettbewerber von unschätzbarem Wert", so ein McAfee-Manager.

#### **"Keine Beweise für Regierungsauftrag"**

Man habe den Angreifern den Projektnamen "Night Dragon" zugewiesen. Die Angriffe seien "in erster Linie von China aus" erfolgt. Einen der mutmaßlichen Täter haben man namentlich identifizieren können - es handele sich um einen chinesischen Staatsbürger aus der ostchinesischen Stadt Heze in der Provinz Shandong, über dessen Server die Computer der angegriffenen Firmen kontrolliert worden seien.

Die Angriffe seien über Server in den USA und den Niederlanden geleitet worden. Die Ereignisse würfen ein trübes Licht auf "den traurigen Zustand der Sicherheit unserer kritischen Infrastruktur", erklärte McAfee-Manager Dmitri Alperovitch. Die Angriffe seien "nicht sehr ausgefeilt" gewesen, aber "sehr erfolgreich bei der Erreichung ihrer Ziele." Man habe aber "keine Beweise, dass hier im Regierungsauftrag gehandelt wurde", so Alperovitch. Ob es sich also um Spionage im Dienste Pekings, um Datensammelei im Auftrag von Wettbewerbern oder um freiberuflichen Diebstahl mit der Hoffnung auf zahlungskräftige Interessenten handelt, ist unklar. Dass mit derartigen Informationen Geld zu verdienen ist, steht jedoch außer Zweifel.

Täglich von 9 Uhr morgens bis 17 Uhr abends Pekinger Zeit seien die Informationen abgerufen worden, erklärte McAfee. Das deute darauf hin, dass die Männer einem festen Beruf nachgingen und keine Freiberufler oder Amateur-Hacker seien. Sie seien in der Regel entweder über die

öffentlichen Websites der entsprechenden Unternehmen in die Rechnersysteme eingedrungen, oder aber über infizierte Täuschungs-E-Mails, die an Manager geschickt worden seien.

Die US-Bundespolizei FBI wolle den "Night Dragon"-Bericht gegenüber Reuters nicht kommentieren. Es sei bekannt, dass derartige Bedrohungen existierten, zum konkreten Fall aber könne man sich nicht äußern. Die chinesische Regierung selbst wollte am Donnerstag zu den Vorwürfen keine direkte Stellung beziehen. Ein Sprecher des Außenministeriums sagte vor Journalisten: "Ich weiß wirklich nichts über diese Situation, aber wir hören öfter von solchen Berichten."

Tatsächlich gibt es immer wieder Berichte über Hackerangriffe aus China. Google schloss im vergangenen Jahr seine Suchmaschine in China - als Begründung gab der Konzern an, es sei zu Hackerangriffen auf das eigene E-Mail-System gekommen. Auch in europäischen und US-amerikanischen Unternehmen ist man an den Versuch digitaler Industriespionage mittlerweile gewöhnt.

*cis/dapd/reuters*

Zugriff am 27.04.2011 <http://www.spiegel.de/netzwelt/netzpolitik/0,1518,744802,00.html>