Bruce Schneier

Ein kritischer Blick auf den Sony-Hack

13.02.15 | Autor / Redakteur: Bernd Schöne / Stephan Augsten

Vor dem Hintergrund des Sony-Hacks diskutierte Bruce Schneier auf der Sicherheitskonferenz IT-Defense über die politische Seite der IT-Sicherheit. (Bild: Bernd Schöne)

Angriff mit Bits und Bytes, Reaktion mit Bomben? Die Hacking-Attacke auf den Sony-Konzern vor der Veröffentlichung des Streifens „The Interview" rückt die Diskussion um Beweislast und Sicherheit bei Cyber-Attacken in den Fokus der Öffentlichkeit. Die internationale Staatengemeinschaft lernt gerade erst, mit dem Phänomen umzugehen.

Der im November 2014 öffentlich gewordene elektronische Einbruch in die Server von Sonys Filmabteilung „Sony Pictures Entertainment" gilt als einer der schwersten der IT-Geschichte. Die Hacker erbeuteten unveröffentlichte Filme, massenweise interne Mails, 47.000 Sozialversicherungsnummern von Mitarbeitern, Passwörter und Zugangsdaten.

Die Täter griffen mehrere Terabyte an Daten ab. Die Folgen waren nicht nur für die Firma dramatisch, sondern auch auf politischer Ebene. Die USA verhängten wirtschaftliche Sanktionen gegen Nordkorea, weil sie hinter dem Angriff das dortige Regime vermuten. Zuvor hatte das Land offiziell gegen die von Sony produzierte Spielfilm-Groteske „The Interview" protestiert, der von einem absurden Mordanschlag auf den Nord-Koreanischen Machthaber Kim Jong-Un handelt.

Unmittelbar vor den ersten Angriffen hatte sich im Juli 2014 der nordkoreanische UN-Botschafter Ja Song Nam beim UN-Generalsekretär Ban Ki-moon über die Handlung des geplanten Filmes beschwert. Im Januar 2015 reagierten die USA dann mit Sanktionen gegen koreanische Rüstungsfirmen. Einflussreiche Senatoren hatten zuvor gefordert, aktiv gegen das Land vorzugehen.

Der amerikanische Informatiker Bruce Schneier setzte sich auf der Sicherheitskonferenz „IT-Defense" der Cirosec GmbH in Leipzig mit den Vorgängen auseinander. Schneier ist als Krypto-Experte und Buchautor („Angewandte Kryptographie") bekannt geworden. Er ist aber auch Vorstandsmitglied in der Bürgerrechtsbewegung „Electronic Frontier Foundation" und Chief Technology Officer der Firma Co3Systems.

Im Zweifel gegen den Angeklagten

Bereits mehrfach hat Schneier sich mit der Regierung seines Heimatlandes angelegt. Im November 2007 beispielsweise hatte er bereits auf eine mögliche Backdoor im Zufallsgenerator „Dual Elliptic Curve Deterministic Random Bit Generator" hingewiesen. Dieser Verdacht sollte sich aber erst im Zuge der Veröffentlichungen durch Edward Snowden bestätigen.

Auch im Falle des Sony-Hacks ist die Beweislage ernüchternd schlecht. „Die Sanktionen beruhen im wesentlichen auf einer menschlichen Geheimdienstquelle im Regierungsapparat von Nordkorea", so Schneier. An elektronischen Spuren wurde wenig Brauchbares gefunden, von einem verräterischen Spuren einmal abgesehen.

Die Angreifer benutzten ein koreanisches Sprachpaket von Microsoft Windows, um ihre Trojaner zu produzieren. Solche Spuren können aber auch absichtlich gelegt werden, um Angriffe unter falscher Flagge zu durchzuführen. Der Angreifer schadet dann doppelt, nämlich dem eigentlichen Opfer und dem vermeintlichen Täter, der politische Nachteile in Kauf nehmen muss.

Ein reiner Indizienprozess

„Vor einem ordentlichen Gericht würden die vorgelegten Beweise wohl kaum ausreichen, einen Schuldspruch zu erwirken“, so Schneier. „Unser Rechtssystem beruht darauf, dass wir wissen, wer angreift und warum er einen Schaden verursacht hat, doch bei Cyberattacken ist diese Frage so nicht eindeutig zu klären.“

Was bleibt, sind also Geheimdienstinformationen – und die haben seit dem Irak-Krieg und der Suche nach Saddam Husseins angeblichen Massenvernichtungswaffen einen faden Beigeschmack. Auch die Wissenschaft kann nicht weiterhelfen. Die Computer-Forensik steht gerade bei massiven Angriffen mit hochentwickelten Werkzeugen vor erheblichen Problemen.

„Es ist sogar schwierig, im Nachhinein die Verantwortung für einen Angriff zu übernehmen“, so Schneier, „etwa um abschreckend zu wirken oder seine Macht zu demonstrieren“. Der Angreifer müsse in erheblichem Umfang Insider-Wissen über den Hack zur Verfügung stellen, um glaubhaft zu sein. Nationale und internationale Rechtssysteme, Diplomatie und die Gesellschaften müssen sich erst langsam an das neue Phänomen der „Computer-Schädlinge“ gewöhnen.

Aus den Fehlern der Vergangenheit lernen

„Wir wissen heute noch nicht einmal, wie wir das nennen sollen, was dort passiert ist“, so Schneier. Cyber-Terrorismus, Vandalismus oder doch Internet-Kriminalität? Die Gesellschaft muss wohl noch eine Weile warten, bis sie gelernt hat, mit diesen Vorfällen umzugehen. Denn eines ist sicher: Es wird wieder geschehen.

Schon 2011 ist Sony zum Ziel massiver Attacken geworden. Seinerzeit waren es Anonymous-Sympathisanten gewesen, die sich an Sony wegen des juristischen Kampfes gegen „Jailbreaker“ der PlayStation 3 rächen wollten. Die IT-Sicherheitsabteilung galt damals als hoffnungslos unterbesetzt. Daran scheint sich wenig geändert zu haben.

Die „Incident Response“ von Sony war mindestens so schlecht wie die Firewall und „Intrusion Detection“. Trotz der Ereignisse von 2011 schien es keinen ausgearbeiteten Notfallplan zu geben. „Die Reaktion von Sony war chaotisch und unkoordiniert“, resümiert Bruce Schneier, „sie wussten einfach nicht, was sie tun sollten“.