Gute oder böse Hacker?

Die Hackergruppe Lulzsec erklärt den Regierungen und den sogenannten „Whitehat-Sicherheits-Terroristen“ den Krieg und das Hackerkollektiv Anonymous zu ihrem Verbündeten. Welche Bedrohung geht von ihnen aus? Kämpfen sie für eine gute Sache? Ich sprach dazu mit dem IT-Sicherheitsexperten Ralph Langner.

Angeblich griffen heute Mitglieder der beiden Hackergruppen Anonymous und Lulzsec in einer ersten konzertierten Aktion Internet-Präsenzen der brasilianischen Regierung an. So sollen für mehrere Stunden im Rahmen der Operation Anti-Security (#AntiSec) die Webseiten des Präsidenten, der Regierung und des Finanzministeriums mittels etwa zwei Milliarden Datenanfragen per DDoS-Attacke innerhalb kurzer Zeit lahmgelegt worden sein. Meldungen dieser Art werden zurzeit fast täglich verbreitet. Mutmaßliches Hauptziel der neuerdings verbrüderten Hackerbewegungen soll es jedoch in Zukunft sein, Informationen von Regierungen, Großkonzernen oder Banken zu stehlen und offenzulegen, die aufzeigen, was hinter dem Rücken der Bürger so getrieben werde. Auf ihrem Twitter-Kanal, dem immerhin schon mehr als 250.000 Nutzer folgen, kündigte Lulzsec für den morgigen Tag die Operation Anti-Security Payload #1 an.

Video von Anonymous zur Operation AntiSec:

Hier klicken, um das Video auf YouTube anzusehen…

Beide Gruppen hatten in der Vergangenheit bereits erfolgreich Hacker-Angriffe auf Institutionen und Unternehmen wie CIA, Mastercard, Visa, Sony, GEMA, GVU oder die türkische Telekommunikationsbehörde TIB durchgeführt. Laut dem IT-Sicherheitsexperten Ralph Langner geht es Anonymous und Lulzsec in erster Linie darum, Aufmerksamkeit zu erzeugen. Die Ankündigung des Zusammenschlusses liege ebenso wie die intendierte Dramatik ganz auf dieser Linie. Er rechnet beide Gruppen den sogenannten Hacktivisten, also Hackern mit

einer weltanschaulichen Agenda, zu. Ernst zu nehmen seien sie, weil einige ihrer Akteure über sehr gute technische Fähigkeiten verfügten. „Wir erwarten ein weiteres Anwachsen solcher Gruppierungen, da es für den normalen Freizeit-Hacker offenbar attraktiver ist, sich einer derartigen Gruppe anzuschließen, als zu versuchen, alleine in die immer stärker gesicherten IT-Systeme potenzieller Opfer einzudringen“, so Langner. Aus seiner Sicht tragen die Aktionen der Hackergruppen zwar dazu bei, dass die Öffentlichkeit für die Gefahren von Cyber-Angriffen sensibilisiert wird, das Vorgehen sei jedoch zu verurteilen: „Zugespitzt könnte man sagen: Hacker sind Teil des Problems, dessen Lösung sie vorgeben zu sein“, bringt er es auf den Punkt. Nicht nur vor diesem Hintergrund begrüßt Langner grundsätzlich die Errichtung von staatlichen Cyber-Abwehrzentren wie in der vergangenen Woche in Deutschland: „Das Cyber-Abwehrzentrum war überfällig. In der jetzigen Form ist es allerdings eher ein Feigenblatt, wo eigentlich ein warmer Pullover gebraucht würde. Wenn das Abwehrzentrum einmal eine dreistellige Personalbasis hat, kann man beginnen, es Ernst zu nehmen. Die Aufgaben sollten in der Prävention massiver Cyber-Angriffe auf die deutsche Industrie und Infrastruktur liegen. Zum gegenwärtigen Zeitpunkt sind wir gegen ernsthafte Angriffe völlig unzureichend geschützt.“ Derzeit wäre es einem Angreifer möglich, Deutschlands Wirtschaft für Tage bis Wochen in weiten Teilen lahmzulegen. Hierzu könnten Cyber-Angriffe auf Kraftwerke, Wasserversorgung, Straßenverkehr (Ampelanlagen), Flugsicherung usw. zählen, ebenso gegen Schlüsselindustrien wie Autobau und Chemie. Darüber hinaus geht der IT-Sicherheitsexperte auch davon aus, dass Attacken in nationalen und internationalen politischen Auseinandersetzungen in Zukunft eine Cyber-Komponente haben werden.

So war beispielsweise das stark vernetzte Estland im Jahre 2007 das Ziel mehrwöchiger DDoS-Angriffe durch die Jugendorganisation des Kreml. Im Rahmen der Attacke gelang es den Hackern, Server der estnischen Regierung sowie von Banken, Medien und Unternehmen über längere Zeit lahmzulegen. Daraufhin hatten die Esten eine Freiwilligen-Armee aus IT-Experten zur Cyber-Abwehr ins Leben gerufen, um zukünftig besser gewappnet zu sein. Birgit Johannsmeier berichtete in einem Beitrag bei DRadio Wissen gar von Überlegungen zur Einführung einer Cyber-Wehrpflicht in dem baltischen Staat. Auf die Frage, ob öffentlichkeitswirksame Cyber-Attacken wie die von Lulzsec und Anonymous dazu beitragen könnten, dass Staaten und Unternehmen mit Verweis auf die Abwehr von vermeintlichem Cyber-Terrorismus bestimmte Zensur-

Maßnahmen bzw. Netz-Einschränkungen rechtfertigen, antwortete Langner, dass in der Politik natürlich vieles möglich sei, man aber damit das Symptom anstelle der Krankheit bekämpfen würde. „Es ist ja keineswegs so, dass es unmöglich wäre, Cyber-Systeme sicher zu betreiben. Darum hat man sich in der Vergangenheit leider nicht ausreichend gekümmert, weil Sicherheit Geld kostet. Was wir heute sehen, war insofern vorhersehbar."

Neben Lulzsec und Anonymous gibt es noch viele weitere Hackergruppen, doch erhalten beide durch ihre öffentlichkeitswirksamen Aktionen derzeit besonders großes mediales Interesse. Zumal sie daran interessiert sind, ihr Handeln öffentlich anzukündigen und zu erklären. Auf der anderen Seite gibt es unzählige Cyber-Angriffe durch Hacker, die im Verborgenen stattfinden: sei es auf eine Infrastruktur wie mittels des Computerwurms Stuxnet, zur eigenen finanziellen Bereicherung oder für einen vermeintlich guten Zweck. Doch egal von welcher Tragweite, politischer Motivation und weltanschaulicher Gesinnung solche Cyber-Angriffe auch sein mögen: Eine simple Trennung zwischen guten und bösen Hackern ist nur schwer möglich, da die Grenzen häufig fließend sind. Und letztlich ist es immer auch eine Frage des Standpunkts!