2000/07 Lifestyle

https://jungle.world/artikel/2000/07/no-such-agency-ist-ueberall

No Such Agency ist überall

Von **dirk franke**

Hacker? Script-Kiddies? Aktivisten? Der Geheimdienst? Nach ein paar Internet-Angriffen treten die Kontrollfreaks und die Paranoiker auf den Plan.

Das E-Commerce ist in Gefahr. Nach den Internet-Angriffen der letzten Woche, die einige große Firmen zwangen, vom Netz zu gehen, haben die Schlagzeilen gewechselt. Nicht mehr das Börsenwachstum der Branche ist das Thema, sondern der »Cyberwar« (ABC News), der »Blitzkrieg« (Wired) oder schlicht die »moderne organisierte Kriminalität« (n-tv).

Dabei ist gar nicht so viel passiert: Eine ganze Reihe großer Anbieter wurde für ein paar Stunden gezwungen, vom Netz zu gehen. Ob dadurch tatsächlich ein größerer Schaden entstanden ist, und wenn ja, wie hoch er ist, ist noch unklar. Doch das Szenario bietet Raum für Spekulationen jeder Art. Auch das FBI behauptet, weder zu wissen, wer verantwortlich ist, noch wie viele Computer beteiligt waren, woher die Angriffe kamen und warum. Dennoch ist nicht auszuschließen, dass der Geheimdienst in die Aktion verwickelt ist. Und wie es der Zufall will, sind in William Clintons neuem Haushaltsentwurf massive Budget-Erhöhungen für elektronische Überwachung vorgesehen.

War nach dem Zusammenbruch der Yahoo-Site noch spekuliert worden, ob nicht vielleicht ein internes Problem vorliegen könne, so weitete sich die Krise schnell aus. Es erwischte den Buchgroßhändler Amazon, die Technikinformationen von ZDNet, die Kaufhäuser ETrade, Buy.com und eBay, außerdem CNN und das Telefonnetz der US-Staaten Oklahoma und Missouri. Sie alle wurden Opfer von Denial of Service (DoS)-Attacken.

Technisch ist solch ein Angriff relativ einfach zu bewerkstelligen und funktioniert ähnlich, als würden alle Teilnehmer eines Telefonnetzes gleichzeitig versuchen zu telefonieren - das Netz bricht zusammen. Im Internet genügen mehrere Computer, die gleichzeitig entsprechende Programme starten. Diese treten ununterbrochen über das Internet mit den Targetsites in Verbindung. Sind die Datenströme groß genug, überlastet das die Kapazitäten der angegriffenen Site, und sie stellt den Betrieb ein. Für normale Kunden ist es nicht mehr möglich, die entsprechende Homepage zu erreichen.

Natürlich darf der Angriff nicht vom eigenen Rechner aus erfolgen, es gilt, sich in andere Rechner einzuhacken, dort die entsprechenden Programme einzuschleusen und diese schließlich koordiniert loszulassen. Programme, die solche Attacken ermöglichen, kann man aus dem Netz herunterladen. Wer sie sucht, gebe »Triple Flood Network«, »Trinoo« oder »Stacheldraht« in eine Suchmaschine ein. Solche Angriffe können also von überall her kommen, und in Anbetracht der Vorliebe von Netzaktivisten für Verschwörungen aller Art, laden die DoS-Angriffe zu wilden Spekulationen geradezu ein.

Die erste Möglichkeit ist, dass Konkurrenten der angegriffenen Firmen zugeschlagen haben. Bei der Vielzahl der angegriffenen Ziele gibt es allerdings niemanden, dem all die Angriffe nutzen könnten. Insbesondere der Zusammenbruch des Telefonnetzes bleibt rätselhaft. Deshalb ist diese Variante in der Diskussion auch vom Tisch. Ebenfalls kaum verdächtig sind die traditionellen Hacker. Deren Szene-Publikationen (2 600, Hacker News Network) sind vor allem damit beschäftigt, darauf hinzuweisen, dass für die Angreifer das Wort »Hacker« nicht zuträfe, da es vielmehr »Vandalen« oder »Saboteure« seien.

Anders sieht es mit einer jüngeren Gruppe aus. Die sogenannten Hacktivisten wissen die Abstürze durchaus zu schätzen: »Das Web ist kein einfaches Einkaufszentrum. Gemessen an ihrem Maßstab spiele ich nur eine furchtbar kleine Rolle für die anvisierten Firmen. Aber warum sollte man nicht eine permanente DoS-Attacke gegen das Rieseneinkaufszentrum starten?« fragt etwa der bekannte Hacktivist und Anarchist Chuck. Diese Gruppe hätte zumindest ein Motiv für die Internet-Angriffe. Sind doch DoS-Attacken ein beliebtes Mittel, um Forderungen Nachdruck zu verleihen. Erst vor wenigen Wochen konnte der juristische Angriff des Net-Spielzeughändlers eToys gegen die kleinere aber ältere Site der Netzaktivisten Etoys abgewehrt werden, indem der E-Commerce-Riese massiv attackiert wurde. Allerdings ist fraglich, ob Hacktivisten über die technischen Mittel für solch eine konzertierte Aktion verfügen: Immerhin blieben die Angriffe auf den WTO-Server vor zwei Monaten fast ergebnislos. Und ebenso ungewöhnlich ist es, dass sich niemand zu den Angriffen bekennt.

Der Hauptverdacht der offiziellen Stellen richtet sich auf »kriminelle Teenager«. FBI-Chef Ron Dick etwa glaubt, dass »ein 15jähriger diese Attacken starten könnte«. Die Programme sind frei verfügbar und nach Lektüre des »readme»-Files einsatzbereit. Deswegen wird diese Gruppe von Verdächtigen auch Script-Kiddies genannt. Allerdings bleibt auch hier die Frage nach dem Motiv. Für gewöhnlich schielen die Script-Kiddies auf Ruhm und Anerkennung, so dass ein Täterpseudonym mittlerweile bekannt wäre.

Es bleibt aber noch eine Organisation, die sowohl das Motiv als auch die technischen Möglichkeiten zu der Aktion hätte: die National Security Agency der USA (NSA). Die Agentur gilt als der meistunterschätzte Geheimdienst der Welt. Zum einen, weil die technischen Operationen der NSA wesentlich weniger öffentlichkeitswirksam sind als die Agententätigkeit der Geheimdienstschwester CIA. Aber auch wegen ihrer - selbst für einen Geheimdienst - restriktiven Informationspolitik. So lautet der Spitzname der NSA auch »No Such Agency«. Andererseits sind die Ergebnisse der NSA kaum zu unterschätzen. Immerhin kam in den letzten Monaten heraus, dass die NSA mit dem Echelon-System weltweit den E-Mail-Verkehr auf geheimdienstrelevante Informationen filtert. Auch gab die NSA vor wenigen Wochen bekannt, dass sie mit einigen ihrer Computer Probleme hatte,

ein bisher einmaliger Vorfall in der Geschichte der Organisation.

Ziel der NSA könnte es sein, das Bedürfnis nach besserer Überwachungstechnik zu lancieren. Die Methoden zur geheimdienstlichen Nutzung der neuen Informationstechnologien sind noch unterentwickelt, viele Möglichkeiten elektronischer Überwachung gilt es noch zu entdecken und auszureizen. »Wenn es nach dem FBI und der NSA geht, sind das einzige nicht-abhörbare Kommunikationsmittel zwei Büchsen und ein Faden«, sagt Barry Steinhardt, Direktoriumsmitglied der American Civil Liberties Union.

Da möchte auch der US-amerikanische Präsident nicht abseits stehen: In seinem Budget für das Jahr 2001 beantragt William Clinton mehr Geld für Abhöranlagen, Polizeidatenbänke und Computer-Crime-Forensik. Mit die größten Zuwächse im Budget - von ehemals 15 Millionen auf jetzt 240 Millionen US-Dollar - werden benötigt, um die technische Umrüstung der Telefonfirmen zu finanzieren. Diese sollen ihre Networks neu verkabeln, um staatliches Abhören zu ermöglichen. Die Hälfte dieses Geldes kommt aus dem Haushalt des Verteidigungsministeriums für nationale Sicherheit, also aus dem Geheimdienstbudget.

Egal, wer für die Angriffe verantwortlich ist, die NSA wird die Aufmerksamkeit auf jeden Fall dazu nutzen, ihre Computer und Planstellen kräftig aufzustocken, um das E-Commerce vor »Cyber-Vandalen«, »Script-Kiddies« oder »Hacktivisten« zu schützen. Denn nach den Worten der US-Justizministerin Janet Reno ist das Internet vor allem für eines wichtig: »Wir werden dafür sorgen, dass das Netz eine sichere Umgebung für Geschäftsabschlüsse bietet.«