Phalanx gegen Botnetze – gute Botnetze helfen gegen Attacken böser Botnetze

Informatiker an der Universität von Washington in Seattle haben ein System entwickelt, das Server vor verteilten Angriffe aus dem Internet schützen soll. Sie setzen dabei eine ähnliche Technik ein wie ihre Gegner: ein weit verzweigtes Netz von Computern.

Newsredaktion Golem – www.golem.de – vom 23.04.2008

Informatiker an der Universität von Washington in Seattle haben ein System entwickelt, das Server vor verteilten Angriffe aus dem Internet schützen soll. Sie setzen dabei eine ähnliche Technik ein, wie ihre Gegner: ein weit verzweigtes Netz von Computern.

Kürzlich verkündete der Anti-Viren-Software-Hersteller G Data, dass viele Botnetze aus gekaperten Computern bestehen, die in Europa stehen.

Den Spitzenplatz belegen dabei Deutschland und Italien. In diesen beiden Ländern stünden allein je 10 Prozent der "Zombie-PCs". G Data spricht von einer regelrechten eCrime-Industrie, die über die Botnetze Spam versendet, Phishing betreibt und Denial-of-Service-Attacken (DoS) durchführt. Gegen letztere haben Informatiker der Universität von Washington in Seattle nun ein Mittel entwickelt: Sie wollen die Botnetze mit ihren eigenen Waffen schlagen.

Phalanx nennen Colin Dixon, Arvind Krishnamurthy und Tom Anderson das von ihnen entwickelte System. Wie ein Botnetz besteht es ebenfalls aus einer Vielzahl von Computern. Allerdings ziehen die Wissenschaftler den Begriff Schwarm für ihr gutartiges Botnetz vor. "Phalanx geht von der einfachen Annahme aus, dass die vereinte Kraft des Schwarms die eines Botnetzes übertrifft", schreiben die Forscher in einem Aufsatz.

Bei einer DoS-Attacke dienen die Computer des Schwarms als Zwischenspeicher. In diese Zwischenspeicher, Mailboxen genannt, werden alle Seitenaufrufe an einen angegriffenen Rechner umgeleitet und gespeichert. Der Zielrechner ruft dann von sich aus die Datenpakete aus dieser Mailbox ab oder er ignoriert sie. Nicht abgerufene Datenpakete werden dann aus der Mailbox gelöscht. "Ein durch Phalanx geschützter Zielrechner bekommt nur die Pakete, die er ausdrücklich von der Mailbox angefordert hat", erklären die Forscher. Auf diese Weise habe der Zielrechner die Kontrolle und nicht der Angreifer.

Phalanx soll jedoch nur die Seitenaufrufe abwehren, die zu einem DoS-Angriff gehören. Berechtigte Anfragen hingegen sollen an den Server weitergeleitet und beantwortet werden. Dazu muss sich ein Rechner bei dem System über ein "Crypto-Puzzle" authentifizieren. Nur wenn der anfragende Computer es löst, bekommt er Zugang zum Server. Einem Rechner, der nur eine einzige Anfrage sendet, gelingt das einfach. Ein gekaperter Computer jedoch, der ständig Seitenaufrufe schickt, wird verlangsamt, weil er dauernd damit beschäftigt ist, das "Puzzle zu lösen".

Wie ein Botnetz braucht auch die Phalanx ein möglichst weit verteiltes Netz von Rechnern, auf denen die Mailboxen installiert sind. Nach Vorstellung der Forscher könnten zum Beispiel die Computer von Content Delivery Networks als Mailboxen dienen. Sie prüfen aber auch die Möglichkeit, einen beliebten BitTorrent-Client so zu verändern, dass die Computer von Millionen BitTorrent-Nutzern im Kampf gegen die Botnetze eingesetzt werden können.

Erste Tests seien, so die Forscher, erfolgreich verlaufen. So habe man einen funktionsfähigen Prototypen im weltweiten Forschungsnetz PlanetLab aufgesetzt. In einer Simulation sei zudem der Nachweis gelungen, dass es Phalanx mit einem Botnetz mit einer Millionen Rechnern aufnehmen könne.