Denial of Service Attacks

Vortrag: *Fefe* <felix@ccc.de>

Bericht: *ISCS* <iscs@ailis.com>

Seit dem Internet-Boom sind mehr und mehr User minderer Hacker-Ehtik auf den Datenfeldwegen unterwegs, die scheinbar Befriedigung dabei empfinden, alles außer Betrieb zu setzen, was ihnen unter die Tastatur gerät. Kurz: der "Denial of Service" (DoS) macht von sich reden.

Unter einer DoS-Atacke versteht man nichts anderes als das Außerbetriebsetzen eines bestimmten Services: z.B. das Ziehen des Steckers eines Bankautomaten, das Verkleben eines Münzeinwurfschachts mit Kaugummi oder eben den Abschuß eines ganzen Rechners, bequem vom eigenen Computer aus.

In der jüngeren Vergangenheit machten besonders DAU-feste Tools auf sich aufmerksam, mit der jeder, der auch nur weiß, was eine IP ist, einen fremden Rechner dazu überreden kann, sich "aufzuhängen". Was aber steckt hinter diesen Techniken wie Teardrop, Winnuke und wie sie alle heißen? Meistens nicht mehr als ein Programmierfehler in der IP-Implementation der Betriebssysteme oder Möglichkeiten, an die man nicht gedacht hatte ... Die einfachste Möglichkeit, einen feindlichen Rechner zu "erschießen", ist sicherlich der gute alte Flood-Ping. Ping ist ein Test-Programm, das nichts weiter macht, als ein Test-Paket zu versenden, das daraufhin vom Zielrechner wieder zurückgeschickt wird. Sendet man nun sehr viele Ping-Pakete, so müssen auch sehr viele Pakete zurückgesendet werden - das belastet die Leitung des Zielrechners, und ehe er sich versehen hat, kann er nichts anderes mehr machen. Nun - eigentlich sehr ungeschickt, wenn man bedenkt, daß auch die eigene Leitung dadurch belastet wird. Kein Angriff für Manfred Modem.

Geschickter ist es da schon, unter fremder Absender-Adresse einen Ping auf eine Broadcastadresse abzuschicken. Ein Ping geht raus, und hundert Rechner antworten und schicken ihre Antwort an das arme Opfer, das natürlich gar nichts mit hunderten von Ping-Antwort-Paketen anzufangen weiß. Die Leitung des angegriffenen Rechners ist überlastet, und er ist quasi vom Netz abgetrennt. Ein anderer bekannter Vertreter der DoS-Tools ist der Teardrop. IP-Pakete können, wenn sie zu lang sind, zerteilt (fragmentiert) werden. Man nehme also ein etwas größeres Fragment eines Pakets, und sorge dafür, daß der zweite Teil mitten in den ersten gehört. Unmöglich - sagt der angegriffene Rechner (womit er zweifellos recht hat), und schon rasselt der Kernel in einen undefinierten Zustand - und der Rechner stürzt ab. Der Fehler im Kernel war unter Unix schnell behoben, und innerhalb eines Tages waren Bugfixes erhältlich. Auch unsere Freunde der Firma Microsoft arbeiteten an einem Schutz, der nach einer Woche verfügbar war (die deutsche Version nach 3 Monaten). Allerdings machte dieser nichts anderes, als ein ganz bestimmtes Teardrop abzufangen. Teardrop 2, welches das Fragment innerhalb des Fragments nur um ein Byte verschoben hatte, ließ nach wie vor die Microsoft-Betriebssysteme in den Genuß der absoluten Verwirrung stürzen. Eine andere witzige DoS-Variante ist das Versenden eines Ping-Paketes mit dem Inhalt "+++ATH0" - das ist der Befehl, der das Modem zum Auflegen veranlaßt. Der angegriffene Rechner nimmt das Paket entgegen, schickt es zurück, das Modem fühlt sich durch "+++ATH0" angesprochen und legt auf. Viele nette Spielchen beginnen auch mit dem Fälschen der Absender-Adresse des Angreifers. Ein Opfer, das die Anfrage erhält, eine TCP-Verbindung zu sich selbst herzustellen (da seine eigene Adresse unter ungeklärten Umständen in die Quell-Adresse geraten ist), wird dieses tun und sich damit selber eine Anfrage zum Aufbau einer TCP-Verbindung schicken, woraufhin er dieses tut und sich selber eine Anfrage zum Aufbau einer TCP-Verbindung schickt, woraufhin er dieses tut ...

Ein wirksamer Schutz gegen solche Angriffe ist schwierig. Man sollte ständig nach Bugfixes Ausschau halten und nie auf seine Firewall vertrauen, denn sie filtert lange nicht alle Angriffe heraus.

Es gilt also: "Kein ungeschützter Datenverkehr!"