Massiver DDoS auf weite Teile des Internets

Ein großer Distributed-Denial-of-Service-Angriff (DDoS) hat am Wochenende zeitweise die Server des DNS-Anbieters Dyn lahmgelegt. Da Dyn für Kunden wie Twitter, Netflix, Spotify und PayPal die Namensauflösungs-Server verwaltet, waren auch diese Dienste zum Teil nicht erreichbar. Der Angriff erreichte solche Ausmaße, dass sich der Sprecher des Weißen Hauses zu den Betriebsstörungen äußerte. Mittlerweile gehen Sicherheitsforscher davon aus, dass die Angreifer sich bei der Attacke des Mirai-Botnetzes bedienten, das zum großen Teil aus gehackten Geräten aus dem Internet der Dinge (IoT) wie Kameras und smarten Haushaltsgeräten besteht. Dieses Botnetz machte auch schon beim Angriff auf Security-Blogger Brian Krebs im September (siehe c't 21/16, S. 16) Schlagzeilen.

Sicherheitsforscher haben außerdem aufgedeckt, dass die Drahtzieher hinter Mirai die Dienste des Botnetzes in einem Untergrundforum verkaufen. Gleichzeitig wurde bekannt, dass mehrere große Hosting-Anbieter in der Woche vor dem Angriff Erpresserschreiben erhalten hatten. Solche Erpresserbriefe sind an sich nichts Neues, bisher versuchten Kriminelle aber eher kleine Firmen zu erpressen. Die schiere Menge an IoT-Geräten, aus denen Mirai besteht, scheint die Erpresser nun allerdings mit genug Feuerkraft versorgt zu haben, um auch die Dienste großer Firmen ins Visier nehmen zu können.

Dass schlecht gesicherte IoT-Geräte früher oder später zu gefährlichen DDoS-Waffen werden, war absehbar. Auf vielen Geräten läuft steinalte Firmware. Ansätze, diese abzusichern, scheitern meist an der schieren Anzahl der beteiligten Parteien. Ebenso warnen Experten schon seit geraumer Zeit davor, dass wichtige Teile der Netzinfrastruktur gegen DDoS-Angriffe verwundbar sind. Hier ist eine Verteidigung zwar möglich, aber teuer. Beides führt dazu, dass ähnliche Angriffe in der Zukunft wahrscheinlich häufiger werden. *(fab@ct.de)*

Linux-Kernellücke wird für Angriffe missbraucht

Eine Sicherheitslücke im Linux-Kernel, die es lokalen Angreifern erlaubt, alle Dateien zu überschreiben, für die sie Leserechte haben, wird aggressiv für Angriffe missbraucht. Linux-Kernelentwickler Phil Oester fand die Dirty Cow getaufte Lücke durch die Analyse von Schadcode auf einem seiner Webserver. Unklar ist, wie lange genau die Schwachstelle schon Ziel von Angriffen ist. Die Lücke klafft seit neun Jahren im Kernel; mindestens seit Version 2.6.22. Zwar kann ein Angreifer auf diesem Weg nicht in das Zielsystem eindringen, laut Oester ist die Lücke allerdings sehr einfach auszunutzen, wenn man einmal eingebrochen ist, und stellt deswegen eine große Gefahr dar.

Webserver können kompromittiert werden, wenn ein Angreifer es über eine andere Schwachstelle schafft, bösartige Daten einzuschleusen. Im Zuge eines solchen Uploads kann er sich mit Dirty Cow eine Root-Shell verschaffen und den ganzen Server kapern. Linux-Distributionen, die Schreiboperationen auf /proc/self/mem einschränken, sind gegen den bisher veröffentlichten Exploit immun. Das ist zum Beispiel bei einigen Versionen von Red Hat Enterprise Linux (RHEL) der Fall, welche diese Datei mit SELinux-Regeln abschotten. Aber auch bei so geschützten Systemen sollten Administratoren die bereits veröffentlichten Updates, die die Lücke stopfen, so schnell wie möglich installieren. Millionen von billigen Routern und IoT-Geräten werden aber wohl noch über Jahre hin angreifbar sein, da deren Hersteller keine Updates veröffentlichen und die auf den Geräten eingesetzten Kernel nicht manuell abgesichert werden können.

Laut Kernel-Chef Linus Torvalds handelt es sich um einen „uralten Bug“, der schon vor elf Jahren einmal „schlecht“ von ihm selbst gefixt worden war. Diese Änderung habe man wieder rückgängig machen müssen; mit dem neuen Update wurde die Sicherheitslücke endgültig gestopft. *(fab@ct.de)*