

13.11.08, 19:00, Von FOCUS-Online-Autor [Torsten Kleinz](#)

|
E-Mail-Werbung

Schlag gegen die Spam-Mafia

So einfach lässt sich die Spam-Flut reduzieren: Seit ein einschlägig bekannter Internet-Provider vom Netz abgekoppelt wurde, geht der digitale Werbemüll zurück.



Digitaler Müll: Spam-Mails im Postfach

Seit Dienstag geht beim kalifornischen Internet-Provider McColo nichts mehr. Die Kunden des Unternehmens sind nicht mehr erreichbar, sogar die Web-Seite des in San José beheimateten Anbieters lässt sich nicht mehr aufrufen. Der Grund: Gleich zwei Dienstleister kappten den Zugang des Unternehmens ins Internet. Der Provider ist damit aus dem Internet verschwunden.

Unterbrechung der Spam-Flut

Zusammen mit dem Provider verschwanden auch Millionen Versender von unerwünschten Werbe-Mails aus dem Netz. „Seit Dienstag kommen bei unseren Kunden 37 Prozent weniger Spam an“, erklärt ein Sprecher des Berliner E-Mail-Dienstleisters Eleven im Gespräch mit FOCUS Online. „Bei Privat-Accounts sind es sogar bis zu 50 Prozent weniger.“ Besonders Nutzer aus den USA können sich freuen: Sie bekommen viel weniger Angebote für Potenzmittel und vermeintlich lukrative Aktien als noch vor wenigen Tagen. Auch beim deutschen E-Mail-Anbieter GMX bleibt seit Dienstag ein Drittel weniger Spam in den Filtern hängen.

Spam-Bekämpfern war der US-Provider schon lange ein Dorn im Auge: Vom Rechenzentrum des Providers wurde nach Angaben mehrerer Experten ein Großteil des weltweiten E-Mail-Spam-Aufkommens gesteuert.

Millionen Rechner infiziert

Der größte Teil des illegalen Spams wird heute nicht über die E-Mail-Server der großen Provider verschickt, sondern über Privatrechner. Virenprogrammierer finden immer neue Wege, Internetrechner in hemmungslose Spam-Schleudern zu verwandeln: Klickt ein Surfer auf einen manipulierten Link oder führt ein entsprechendes Programm aus, übernehmen Spammer die Kontrolle über den Rechner. Ist ein Virus besonders erfolgreich, kann er Tausende von Rechnern gleichzeitig steuern – ein sogenanntes **Bot-Netz** entsteht.

Spam-Bekämpfer können gegen diese Netze kaum ankommen, denn die E-Mails kommen von Millionen unbekannter Rechner. Welcher davon ein legitimer Versender ist und hinter welcher Adresse sich ein gehackter Privatcomputer verbirgt, ist von außen kaum feststellbar. Nur mit aufwendigen Filtern kann der Großteil des Werbemülls aussortiert werden.

Die größten Bot-Netze zählen mehrere Hunderttausend Rechner. Allein im sogenannten „Srizbi-Netz“ sind nach unterschiedlichen Schätzungen zwischen 300 000 und 600 000 Rechner organisiert – im letzten halben Jahr hat sich die Zahl der infizierten Rechner mehr als vervierfacht. Diese können für allerhand illegale Zwecke eingesetzt werden: vom Spam-Versand bis hin zum gezielten Angriff auf Rechner von Konkurrenten.



Namensgeber für Spam: Amerikanisches Dosenfleisch
Spam-Versender offline

Die Spammer installieren an verschiedenen Stellen virtuelle Server, die den gewaltigen Rechnerpark verwalten und den Rechnern Anweisungen geben. Nach Analyse des US-Sicherheitsunternehmens Secure Networks standen im Rechenzentrum von McColo gleich mehrere dieser Kontroll-Server.

Die Folge des Ausfalls von McColo: Millionen infizierter Rechner können nun nicht mehr von den Kriminellen kontaktiert werden – die Spam-Hydra ist geköpft. Allerdings wird der Sieg nicht allzu lange dauern – schon lange arbeiten kriminelle Hacker an Möglichkeiten, die Kommando-Server überflüssig zu machen oder besser vor Strafverfolgern zu verstecken.

Warum genau sich zwei Unternehmen gleichzeitig entschieden, McColos Netzzugang zu kappen, ist noch unklar. Laut einem Bericht der „Washington Post“ wurden über die Rechner von McColo nicht nur Bot-Netze kontrolliert, sondern auch andere illegale Geschäfte abgewickelt: So sollen hier unter anderem gefälschte Medikamente und sogar Kinderpornografie gehandelt worden sein.