2010/44 Lifestyle

https://jungle.world/artikel/2010/44/war-spam

Über das Geschäft mit Spam-Mails

War on Spam

Von **Burkhard Schröder**

Einer der weltweit größten Versender unerwünschter Werbemails ist untergetaucht. Das hört sich an wie eine gute Nachricht, bedeutet jedoch nicht das Ende des lukrativen Geschäfts mit Spam-Mails, das weiterhin von der Ignoranz vieler Internetnutzer lebt.

Als die Moskauer Polizei vor einer Woche die Wohnung des 31jährigen Igor A. Gusev durchsuchte, fand sie nur noch ein paar Rechner und einige Speichermedien. Die Website spamit.com, die dem Umfeld Gusevs zugeordnet wird, war bereits am 27. September abgeschaltet worden. Höhnisch ist dort jetzt nur noch auf Französisch zu lesen: »Der König ist tot! Es lebe der König!«

Sicherheitsexperten wie etwa die des US-amerikanischen Unternehmens M86 Security stellten fest, dass seit Gusevs Verschwinden das weltweite Spam-Aufkommen um ein Fünftel abgenommen hat. Das sind pro Tag etwa 50 Milliarden Werbe-E-Mails weniger. Es ist nicht sicher, ob der untergetauchte Moskauer Unternehmer wirklich persönlich dafür verantwortlich ist, dass die elektronischen Postfächer unzähliger Internet-Nutzer mit unerwünschter Werbung verstopft worden waren.

Die russische Wochenzeitung Newsweek, die zum Springer-Verlag gehört, hatte bereits im November 2009 eine Reportage mit dem hübschen Titel »Das Cyberreich des Bösen« publiziert und Gusev als einen der »führenden Spammer« der Welt tituliert. Der revanchierte sich, indem er eine Verleumdungsklage gegen Axel Springer Russia anstrebte und vor Gericht 700 000 Rubel Schadensersatz sowie den Abdruck einer Gegendarstellung einforderte.

Die russische Zeitung Kommersant behauptete, die Maßnahmen gegen den berüchtigten Spammer seien in Russland die ersten dieser Art gewesen und vor allem eine Reaktion auf die Klagen westlicher Länder. Der russische Präsident Dmitrij Medwedjew hatte im Juni das Silicon Valley besucht. Kurz bevor eine Delegation der kalifornischen Softwarefirmen Russland einen Gegenbesuch abstattete, nahm die russische Staatsanwaltschaft die Ermittlungen gegen Grusev auf, und spamit.com ging einige Tage darauf »zufällig« offline. Auch das einschlägige Forum spamdot.biz verschwand, ohne dass klar war, von wem und warum die Website abgeschaltet worden war.

Gusev wurde nicht vorgeworfen, die Welt mit Werbung für Potenzpillen wie Viagra, Cialis oder ähnlichen Substanzen überschwemmt zu haben, sondern die Internet-Apotheke glavmed.com ohne eine gültige Lizenz zu besitzen. Zu Glavmed gehören zahlreiche Online-Pharmahändler, die nicht auf Laufkundschaft angewiesen sind. Diese Methode funktioniert wie eine Art Franchise-Verfahren. Die Firmen nehmen die Dienste professioneller Spammer in Anspruch, wie das berüchtigte Partnerka-Netz, um auf ihre Produkte aufmerksam zu machen.
Das zeitweilige Abflauen des Spamaufkommens in aller Welt bedeutet jedoch nicht viel. Auch wenn die Polizei wieder einmal riesige Mengen an illegalen Drogen beschlagnahmt, reduziert das weder den Konsum noch den Profit der Hersteller, sondern treibt nur den Marktpreis kurz in die Höhe.
Werbemails sind ein lukratives Geschäft. Obwohl man einen Bedarf nicht unbedingt erkennen kann, wenn wahllos allen Menschen, die jemals eine E-Mail-Adresse irgendwo im Internet veröffentlicht haben, angeboten wird, ihren Penis zu verlängern, auch wenn sie zufällig weiblich sind – das Geschäftsmodell funktioniert. Es lebt jedoch nicht von einer Krankheit, einem Lebensgefühl oder einer Sucht wie bei psychotropen Substanzen, sondern ausschließlich von der Dummheit vieler Internetnutzer.
Zahlreiche empirische Studien wie etwa die der Anti-Abuse Working Group haben belegt, dass rund die Hälfte aller Nutzer Spam-Mails öffnen, häufig unter Missachtung der einfachsten Sicherheitsregeln. Glavmed erreichte täglich etwa geschätzte 20 Verkäufe nur durch Spam für zweifelhafte Produkte, die meistens angeblich dazu dienten, die männliche Potenz zu steigern. Bei einem durchschnittlichen Einkaufswert von 200 Dollar bringt Spam dieser Art damit 4 000 Dollar Umsatz pro Tag, die Provision von Glavmed betrüge dabei 1 600 Dollar.

Neben dem Verkauf diverser Pillen dient als zweites Standbein das Phishing durch E-Mails. Nutzer, die ihre elektronische Post fahrlässig statt in reinem Text im Html-Format lesen, also in Form einer Website, die schädlichen Code enthalten kann, ohne dass man das auf den ersten Blick merkt, werden auf kriminelle Seiten gelenkt und dazu verführt, persönliche Daten preiszugeben. Oder es werden, falls das Opfer sich um Sicherheit nicht kümmert, sogar aktive Programme implementiert, mit denen der Rechner – unbemerkt vom Nutzer – ferngesteuert und wiederum als Spam-Schleuder missbraucht werden kann. Das alles funktioniert nur, wenn alle Regeln über Sicherheit beim Surfen ignoriert werden. Aber die übergroße Mehrzahl aller Internetnutzer interessiert sich hierfür nicht – aus Bequemlichkeit, aus Gewohnheit oder schlicht aus Ignoranz. Auch Facebook-Accounts wurden auf diese Weise übernommen. Ein Gericht in Quebec verurteilte im November 2008 einen Kanadier zu 629 Millionen Euro Strafe, weil er per Phishing Facebook-Konten übernommen und über diese unzählige Spam-Mails verschickte hatte.
Im Internet wurde die erste unverlangte Werbung am 3. Mai 1978 gesichtet, im Usenet, dem ältesten Teil des Netzes, der aus Diskussionsforen besteht, zwei Jahrzehnte bevor das World Wide Web erfunden wurde. Damals waren die meisten Nutzer Wissenschaftler und IT-Fachleute, die sich über den »Missbrauch« des Internet für Kommerzzwecke empörten. Mit 600 E-Mails, die Werbung für ein Computersystem enthielten, erreichte der erste Spammer Gary Thuerk damals ein Fünftel aller Internet-Nutzer, verdiente damit 12 Millionen Dollar und wurde so zum Vorbild für eine ganze Branche.
Über 80 Prozent der unerwünschten digitalen Werbung, die in Nordamerika und Europa

generiert wird, gehen auf das Konto von rund 100 Banden professioneller Spammer, von denen das nicht-kommerzielle Spamhaus Project sogar monatliche Steckbriefe im Internet veröffentlicht. Mehrere US-amerikanische Spammer wurden schon zu Strafen in dreistelliger Millionenhöhe und zu Haftstrafen verurteilt. James McCalla zum Beispiel wurde vor vier Jahren zur Zahlung der eher symbolisch gemeinten Summe von 11,2 Milliarden US-Dollar verurteilt. Das scheint jedoch nicht abzuschrecken. Unerwünschte Werbung per E-Mail nimmt nicht ab, sondern zu.
Neben Indien, China und Russland ist Brasilien der größte Produzent von Spam, Vietnam schließt immer mehr zu den vier Großen auf. Früher benutzten Spammer schlecht konfigurierte Rechner, die für den Versand von E-Mails zuständig waren, die sogenannten offenen Relays, um unbemerkt massenhaft digitale Werbung zu verschicken. Heute wird das in der Regel durch Bot-Netze erreicht, also gekaperte Rechner, auch um die Herkunft des Spam zu verschleiern. Mittlerweile tauschen die meisten Provider »schwarze Listen« mit Rechneradressen aus, die für massenhaften Werbemüll berüchtigt sind. Das hilft aber nicht immer, zumal die Blockade eines Rechners auch oft Unschuldige trifft, deren harmlose E-Mails dann nicht mehr zum Ziel gelangen.
Gefährliche »aktive Inhalte« wie etwa Trojanische Pferde, die per E-Mail auf einen Rechner gelangen, können zwar nichts erreichen, falls der Eigentümer des Computers sie nicht aktiv installiert, aber viele Nutzer insbesondere des Betriebssystem Windows laden sich diese Malware zusammen mit scheinbar harmlosen Programmen herunter. Aber auch hier gilt: Ohne Softwarefehler und ohne aktives Mittun der Anwender passiert gar nichts.

Spam macht mittlerweile 97 Prozent des gesamten E-Mail-Volumens aus. Die Großen unter den Spammern sind jedoch nicht nur lästig und verursachen Kosten. Hinter den russischen Gruppen steht ein verzweigtes Netz von konspirativ arbeitenden Firmen und Organisationen wie etwa das berüchtigte Russian Business Network (RBN). Dieser Internet-Provider mit Sitz in St. Petersburg hat Tochterunternehmen in Panama, auf den Seychellen, in der Türkei, in China und in Großbritannien. Eine der Geschäftsideen ist, kriminellen Kunden zu garantieren, dass deren Daten nicht weitergegeben und diese vor dem Zugriff durch die Justiz geschützt werden. Vor zwei Jahren gab es ernstzunehmende Hinweise darauf, dass während des Konflikts zwischen Georgien und Russland das RBN die Kontrolle über »feindliche« Rechner übernommen hatte. Daher tauchen immer wieder Gerüchte auf, dass die russische Regierung – und nicht nur sie – sich der illegalen Strukturen der Spammer-Gruppen bediente und diese beschützte, um einen Cyberwar führen zu können. Beweisen kann man das jedoch nicht.
Es wird nicht lange dauern, bis die Websites des untergetauchten Igor Gusev und seiner Kumpane durch andere ersetzt werden. Solange der Aufwand gering und der Gewinn hoch ist und solange Internet-Nutzer meinen, Pillen jedweder Art online kaufen zu müssen, wird sich gar nichts ändern. Man muss befürchten, dass sich das Nutzerverhalten erst dann ändern wird, wenn jede unverschlüsselte E-Mail den Rechner lahmlegen könnte und naives Herumsurfen, ohne sich um die Sicherheit des eigenen Rechners zu kümmern, schwerwiegende Folgen hat. Mit jemandem, der auf Spam oder auf Phishing hereinfällt, sollte man kein Mitleid haben. Insofern ist auch der russische Unternehmer Grusev ein Teil von jener Kraft, die stets das Böse will und doch indirekt das Gute schafft.