ARGUS Medienbeobachtung

NZZ FOLIO
Beilage der NZZ
8021 Zürich
Auflage 12x jährlich 224394

026.028 / 134578 mm2 / Farben: 3 Seite 25 02.02.2004

Green.ch

EPIDEMIE IM PARADIES

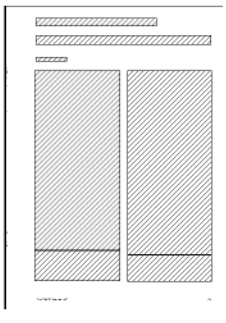
Viren, Würmer und Spam bedrohen den Internetverkehr, die Methoden der Wegelagerer werden immer dreister. Und es kommt noch schlimmer.

Von Claude Settele

Die Informationsfreiheit hat ihren Preis. Dem einst als Kommunikationsparadies gelobten Information Highway droht der Verkehrskollaps, sein feinverästeltes Netz ist voll von Ungeziefer, und überall türmt sich der Abfall. Der arglose Internetwanderer liest hinterhältige Programme auf, stolpert über Lockangebote und wird mit Schmutz beworfen. Viren, Würmer und die als Spam bezeichneten Werbewurfsendungen haben sich im letzten Jahr zu einer Plage mit epidemischem Ausmass entwickelt. Und es gibt keine Aussicht auf Besserung. Die Informationsgesellschaft droht zur Müllgesellschaft zu verkommen.

Spam gibt es schon länger, zum Problem geworden ist er erst durch die schiere Masse. Woher das Wort stammt, ist nicht ganz klar, in der inoffiziellen Geschichtsschreibung des Internets taucht meist die englische Komikertruppe Monty Python als Urheberin auf. Diese Version kolportiert auch die auf Dosenfleisch spezialisierte US-Firma Spam. Demnach geht der Begriff auf einen Sketch von Monty Python zurück, in dem eine Gruppe singender Wikinger in einem Restaurant, in dem nur Spamprodukte auf der Speisekarte stehen, immer lauter «Spam, Spam, Spam» grölt, bis jede Konversation unmöglich wird.

Auch im Internet ist die Konversation massiv gestört. Kreditangebote, Rezepte zur Vergrösserung gewisser Körperteile, pornographische Lockangebote, Gewinnversprechen nach dem Schneeballprinzip oder dubiose Rundschreiben verstopfen die elektronischen Postfächer. Laut der US-Firma Brightmail war 2003 weltweit mehr als jede zweite E-Mail eine Spambotschaft. Das auf Spambekämpfung spezialisierte Unternehmen behauptet, dass der Anteil der Werbe-E-Mails von 40 Prozent im Jahr 2002 auf 56 Prozent im letzten Jahr explodiert sei. Skepsis gegenüber solchen Statistiken ist berechtigt, doch Brightmails Zahlen alarmieren. Sie basieren nicht auf Schätzungen, sondern auf der Analyse von 300 Millionen E-Mail-Konten, für welche die Firma im Auftrag von Unternehmen und Internetprovidern, darunter auch der Swisscom-Tochter Bluewin, E-Mails filtert. Nicht weniger als 800 Milliarden E-Mails hat Brightmail



2003 geprüft, was 15 Prozent des weltweiten E-Mail-Verkehrs entsprechen soll.

Rechnet man diesen Marktanteil hoch, so sind letztes Jahr weltweit 5,3 Billiarden elektronische Mitteilungen versandt worden, mehr als die Hälfte davon – nämlich 3 000 000 000 000 E-Mails – waren demnach Müll. Auch die Brightmail-Konkurrentin MessageLabs beziffert den Müllanteil im E-Mail-Verkehr mit rund 55 Prozent. Übersetzt auf die Wasserversorgung ist die Lage etwa so, wie wenn Frischwasser und Abwasser gemischt aus demselben Hahn flössen.

Ein grosser Teil dieser Schmutzwelle erreicht die Anwender nicht, weil die Provider vorher den Riegel schieben. Sunrise etwa filtert täglich 70000 Werbe-E-Mails aus. Mehrere Provider schätzen, dass der Anteil von Spam auch hierzulande gut die Hälfte ausmacht. Für Optimismus gibt es wenig Anlass. Experten warnen im Gegenteil davor, dass die Quote in den nächsten Jahren 65 bis 75 Prozent erreichen könnte, pessimistische Propheten verkünden gar den Kollaps des E-Mail-Systems.

Blenden wir zurück in die gar noch nicht so ferne Zeit Mitte der neunziger Jahre, als sich das World Wide Web zu entfalten begann. Da war die Internetwelt noch in Ordnung. Die neuen Siedler auf dem elektronischen Planeten setzten auf moralische Werte und definierten mit der «Netiquette» einen Verhaltenskodex. Dieser untersagte etwa die Beschimpfung von Teilnehmern in Diskussionsforen und das Versenden unverlangter E-Mails. Wer gegen die Regeln verstiess, wurde an den Pranger gestellt.

Doch inzwischen ist der Planet dicht bevölkert, und die selbsternannten Wächter über die Anstandsregeln haben kapituliert. Heute haben Virenautoren und die Spam-Industrie das Internet fest im Griff. Sind Virenprogrammierer meist von nichtmateriellen Motiven wie Geltungsdrang oder destruktiver Machtdemonstration beflügelt, agieren Spammer aus rein kommerziellen Absichten. Sie streuen die Werbebotschaften im Auftrag von Firmen und verdienen dabei je nach Schätzung pro Million versandter E-Mails zwischen 250 und 1000 Dollar. Im Vergleich zum gedruckten Werbeversand sind die Vertriebskosten beim E-Mail-Versand praktisch zu vernachlässigen. Dafür sind die Streuverluste gross, da immer mehr Spam direkt im Müllordner landet. Deshalb erhöhen Spammer laufend die Menge und die Kadenz ihrer Mailings.

Die Agitatoren auf der dunklen Seite des Netzes ziehen hierzu alle Register und zwingen Provider und

Internetnutzer zu Gegenmassnahmen. Es tobt ein technisch geführter Abnützungskrieg. Die Angreifer sind im Vorteil, denn sie wechseln wie Guerrillakämpfer schnell die Taktik und nutzen Sicherheitslücken im Internet. Microsoft muss im Wochenrhythmus mit immer neuen Flicken Löcher stopfen. Der Kampf gegen Spam schürt bei vielen Opfern Aggressionen. Im November 2003 wurde ein kalifornischer Programmierer verhaftet, nachdem er einem Spammer gedroht hatte, ihn ausfindig zu machen, zu erschiessen und zum Abschluss mit Bohrer und Eispickel sein Hirn zu bearbeiten. Der nach eigenen Angaben sonst friedfertige Mann rastete aus, weil er, an Hodenkrebs erkrankt, von Spam-E-Mails bombardiert wurde, die ihm ein Mittel zur Penisverlängerung andrehen wollten. Nun droht ihm eine Freiheitsstrafe von bis zu fünf Jahren. Doch auch den Spammern ist jedes Mittel recht. Gefälschte Absender und irreführende Betreffzeilen gehören zum Grundhandwerk. Ein neues Täuschungsmanöver besteht darin, Spam als offizielle Mitteilung bekannter Unternehmen zu tarnen.

So versandten im Dezember 2003 Betrüger mit einer scheinbar der Firma Visa gehörenden E-Mail-Adresse Spams, die die Empfänger aufforderten, ihre Kreditkartendaten zu aktualisieren. Ein Link führte zu einer angeblichen Website von Visa, die inclusive Domainadresse gefälscht war. Dieses Spoofing (Manipulation, Verschleierung) oder auch Phishing genannte Verfahren, das den Anwendern eine vertrauenswürdige Website vorgaukelt, ist aufgrund eines Fehlers in den gängigen Browsern möglich, der in der Adresszeile die Umleitung auf die wirkliche Adresse unterschlägt. Phishing hat sich in den USA so schnell verbreitet, dass sich das FBI letztes Jahr besorgt an die Öffentlichkeit wandte. Opfer ähnlicher Aktionen waren auch das Internet-Auktionshaus eBay, die Citibank und AOL geworden. Die Betrüger wollen dabei meist persönliche Kreditkartendaten und Kontoinformationen ausspionieren.

Mit Phishing arbeiten auch zweifelhafte Witzbolde, die mit Scherz-E-Mails (Hoax) für Verunsicherung sorgen. In Grossbritannien zirkulierten E-Mails, in denen der angebliche Kauf eines iPods von Apple mit dem Hinweis bestätigt wurde, dass der Betrag der Kreditkarte des Empfängers belastet worden sei. Für allfällige Fragen war eine Telefonnummer aufgeführt. Sie gehörte der Polizeistation in Cambridgeshire, deren Zentrale in der Folge von Anrufen überschwemmt wurde.

Die Entwicklung im vergangenen Jahr nährt den Verdacht, dass sich Spammer und Virenautoren indirekt befruchten, indem sie gegenseitig die Tricks und Programmiertechniken abkupfern, um ihre gefährliche und lästige Fracht effektiv unter die Leute zu bringen. So setzten Spammer laut Angaben des Antispamprojekts Spamhaus den Wurm W32.Mimail.E in Umlauf, der einzig das Ziel hatte, die Website von Spamhaus mit einem Anfragebombardement auszuschalten.

Ein weiteres Beispiel für die unheilige Allianz ist das Faktum, dass jetzt auch Virenautoren Spoofing als Taktik einsetzen. Laut der auf Virenbekämpfung spezialisierten Firma Trend Micro tauchte der Ende 2003 hyperaktive Wurm Sven.A als scheinbar offizielle Mitteilung von Microsoft mit gefälschtem Logo und Absender in den Postfächern auf und verleitete die Empfänger dazu, den Anhang zu öffnen.

Diese Taktik hat Erfolg, weil der Mensch als offenbar schwächstes Glied in der Kette der Abwehrmassnahmen leicht zu täuschen ist. In der Szene spricht man deshalb bereits von Viren und Würmern des Typs «Social Engineering». In diese Kategorie gehört das letzten Dezember in Deutschland zirkulierende E-Mail, das sich als Mitteilung der Kripo Düsseldorf ausgab und dem Empfänger mitteilte, dass gegen ihn ein Verfahren wegen illegalen Herunterladens von MP3-Songs und Filmen eingeleitet worden sei. Der Inhalt der Klage – so stand in der E-Mail – sei im Anhang enthalten. Wer diesen öffnete, aktivierte eine Variante des Sobig-Wurms. Dieser Wurm kopiert die E-Mail-Adressen eines Rechners und sendet sich gleich an diese weiter.

Mit solchen Programmiertricks verbreitet sich das Ungeziefer rasend schnell. Den Rekord schaffte im vergangenen Sommer der Wurm Sobig.F, der laut MessageLabs am 19. August 2003 innerhalb von 24 Stunden eine Million Rechner infizierte. Die Infektionsrate bei Bluewin – durchschnittlich 0,5 Prozent der E-Mails – schnellte an einzelnen Tagen im August und September hoch auf 15 bis 25 Prozent.

Zu den bestehenden Viren und Würmern gesellen sich neue Schädlingstypen wie Retroviren, deren Ziel es ist, Antivirensoftware auszuschalten. Perfid sind auch Troianer und verwandte Typen, die sich auf befallenen Computern «Hintertüren» einrichten, über die der Rechner ferngesteuert werden kann. Dieses Hijacking kann benutzt werden, um vom gekaperten Rechner ei-

nes ahnungslosen Computerbenutzers aus Hunderttausende von Spam-E-Mails zu versenden.

Die Spammer umgehen so Filter und sogenannte Blacklists von Mailservern, die als notorische Spammer bekannt sind. Auch den grossen Schweizer Providern sind solche Vorfälle bekannt. Betroffen sind vor allem ADSL-Kunden mit einer festen IP-Adresse, die ihre Sicherheitseinstellungen nicht optimal konfiguriert haben. Eine Bluewin-Sprecherin sagt, dass die Kunden selber dafür verantwortlich seien, dass ihre PC sicher und frei von Viren blieben. Kunden, von deren Rechnern aus Massen-E-Mails versandt worden sind, erhalten von Bluewin eine Verwarnung und bei ausbleibender Reaktion die Kündigung. Da viele Anwender bei der Wahl der passenden Abwehrmassnahmen überfordert sind, bieten die Provider einfach konfigurierbare Viren- und Spamlösungen sowie Firewalls an.

Für Internetnutzer, die sich per Modem ins Netz einloggen, lauert eine weitere Gefahr in Form von sogenannten Dialer-Programmen. Beim Besuch gewisser Websites nisten sich solche PC-Dialer oft unbemerkt auf dem PC eines Anwenders ein, unterbrechen die Verbindung zum Standardprovider und wählen eine eigene Verbindung über eine teure Leitung an. Diese läuft über 090x-Mehrwertdienstnummern, bei denen horrende Minutenpreise anfallen. In der Schweiz gibt es für Abzockernummern keine Preislimite. Als Schutz gegen Dialer-Programme lassen sich solche Mehrwertdienstnummern jetzt immerhin kostenlos sperren.

Die volkswirtschaftlichen Kosten der Viren- und Spamplage sind enorm. Die Provider, die Netzwerkbetreiber, die Firmen- und Privatkunden müssen in Hard-, Software und Dienstleistungen investieren, um ihre Rechner sauberzuhalten. Freuen kann dies nur die Hersteller von Antivirensoftware, Spamfiltern und Firewalls. Gewaltig sind aber auch die Kosten der verpufften Arbeitszeit, die für die Sichtung und Löschung von Spam benötigt wird – und für die Wiederherstellung von verlorenen Daten.

Die Beratungs- und Marktforschungsfirma Radicati Group veranschlagt die von Spam verursachten Kosten für Firmen im letzten Jahr auf 20,5 Milliarden Dollar. Bis im Jahr 2007 sollen sie sich auf 198 Milliarden Dollar vervielfachen. Dabei sind die Folgen von Virenschäden nicht einmal mitgerechnet. Die Spamplage frisst über den überflüssigen Datenverkehr zunehmend auch Bandbreite, die die Provider für teures Geld bereitstellen. Der Schweizer Provider Green.ch schätzt, dass

bereits 20 Prozent seiner Bandbreite durch Spamverkehr ausgelastet sind, die Kosten betragen rund 250 000 Franken pro Jahr.

Hinzu kommt der gestiegene Supportaufwand, für den die Provider zusätzlich Personal einstellen mussten. Auch der Informationsbedarf der Kunden ist nämlich explodiert. Bei Bluewin hat sich die Zahl der täglichen Anfragen letztes Jahr im Vergleich zum Vorjahr auf 50 bis 100 verzehnfacht. Bluewin beziffert den gesamten Aufwand im Kampf gegen Viren und Spam auf mehrere Millionen Franken jährlich. Und obwohl Experten schätzen, dass vier Fünftel der Werbe-E-Mails von nur rund 200 professionellen Spammern stammen, ist der Misere schwer beizukommen.

Für die Bekämpfung des Übels setzt man auf verschiedene Strategien. An erster Stelle steht die technische Abwehr über Filter, die vor Spam schützen sollen wie der Damm vor Hochwasser. Provider setzen dabei auf die Dienste professioneller Anbieter wie Brightmail, die die Filterdefinitionen pro Stunde bis zu zehnmal aktualisieren. Bluewin schätzt, dass rund 70 Prozent Spam in diesem Filter hängen bleiben. Für die vom Provider nicht gefilterten Werbesendungen bieten die neusten E-Mail-Programme Spamfunktionen, die zum Teil «lernfähig» sind.

Eine weitere Strategie setzt auf die Macht der Justiz. Während die Europäische Union bereits eine Regelung gegen Spam eingeführt hat, gibt es in der Schweiz kein entsprechendes Gesetz. Der Artikel 13 der EU-Datenschutzrichtlinie erlaubt das Versenden von Werbe-E-Mails nur mit Einwilligung des Empfängers. Ausserdem muss die Botschaft einen korrekten Absender sowie eine Option zur Abbestellung enthalten. Die gleiche Regelung ist im Rahmen der geplanten Revision des schweizerischen Fernmeldegesetzes vorgesehen, zu der der Bundesrat seine Botschaft im November 2003 verabschiedet hat. Dazu wird das Bundesgesetz gegen den unlauteren Wettbewerb durch einen Artikel ergänzt.

Kritiker dieser sogenannten Opt-in-Lösung weisen darauf hin, dass damit Firmen von sich aus keinen E-Mail-Kontakt zu Kunden aufbauen können. Dies ist mit dem in den USA kürzlich eingeführten Can Spam Act noch möglich. Dieses als Opt-out-Variante bezeichnete Gesetz erlaubt den Versand von Werbe-E-Mails mit korrekten Absendern, die Empfänger müssen sich selber aus einer Versandliste austragen.

Kritiker der Opt-out-Lösung bezeichnen das Gesetz

als Freipass für Spammer, denn es lädt zu Missbrauch geradezu ein. Wie reagiert ein Richter beispielsweise, wenn ein Spammer bei jeder Werbewelle einen anderen korrekten Absender benutzt, um Kunden, die diese Botschaft abbestellten, ins Leere laufen zu lassen? Zur Diskussion steht in den USA auch die Einführung einer Art Robinsonliste von Leuten, die keine Werbe-E-Mails erhalten wollen, analog zur bereits bestehenden Liste für Telefonmarketing.

Viele erhoffen sich von den neuen Gesetzen Prozesse mit abschreckender Wirkung. In Kalifornien, wo ein schärferes Antispam-Gesetz gilt, wurden im Oktober erstmals zwei Spammer zu einer Busse von zwei Millionen Dollar verurteilt. Der Staat New York und Microsoft haben einen der bekanntesten amerikanischen Spammer mit dem erklärten Ziel angeklagt, dessen Unternehmen mit einer Maximalbusse von 20 Millionen Dollar in den Ruin zu treiben. Microsoft ist mit der Gründung eines Fonds auch in der Bekämpfung von Virenprogrammierern aktiv geworden. Für die Ergreifung der Autoren von Lovesan/Blaster und Sobig hat der Fonds ein Kopfgeld von 250 000 Dollar ausgeschrieben.

Einige Vorschläge zur Bekämpfung der Misere basieren schliesslich auf Änderungen der Standards für Mailprotokolle, um das Versenden von E-Mails mit gefälschten Adressen zu verunmöglichen. Doch viele Experten zweifeln, dass das Übel mit Gesetzen und technischen Lösungen eingedämmt werden kann. Eine ökonomisch ausgerichtete Gegenstrategie will deshalb das Businessmodell der Spammer attackieren. Die Kosten des Spamming sollen demnach statt den Internetnutzern den Urhebern aufgebürdet werden.

So ist beispielsweise das Marktforschungs- und Beratungsinstitut Forrester Research überzeugt, dass das Problem nur in den Griff zu bekommen ist, wenn man sich vom kostenlosen E-Mail-Service verabschiedet. Schon eine Gebühr von einem Viertelcent pro E-Mail würde die Geschäftsidee der Spammer zunichte machen. Der Vorschlag leuchtet ein – und doch hat er kaum Chancen. Denn dieser Pfeil wird aus demselben Grund sein Ziel verfehlen wie jener aus dem gesetzlichen Köcher: Das Internet kennt keine Landesgrenzen. Erste Spammer benutzen bereits Offshore-Destinationen für den Massenversand. Selbst bei einer breit abgestützten Initiative für kostenpflichtige E-Mails dürfte es immer ein paar Länder ohne Gesetze gegen Spam und E-Mail-Gebühren geben.

Bleibt also nur die betrübliche Perspektive des Duells Richter gegen Spammer beziehungsweise Filter gegen Müll? Es macht ganz den Eindruck. Und es wird noch schlimmer kommen. Schaut man über den Horizont der Computertastatur hinaus, zeichnet sich ab, dass die zunehmend vernetzte Welt in vielen Bereichen des täglichen Lebens verwundbar geworden ist.

Der virusbedingte Zusammenbruch des Informatiksystems der Schweizer Post im Oktober 2003 oder der vor Jahresfrist vom Wurm SQL-Slammer verursachte Ausfall von 13 000 Geldautomaten in den USA sind Vorboten einer möglicherweise fatalen Entwicklung. Durch maliziöse softwarebedingte Computerabstürze können eines Tages auch die Fahrplansteuerung von Verkehrsbetrieben, die Reservationssysteme von Fluggesellschaften oder das delikate Gleichgewicht der Stromversorgung gestört werden. Auch kann die steigende Spamflut die Infrastruktur der als Knoten im Netz agierenden Provider blockieren und deren Funktionsfähigkeit einschränken.

Die Plage wird auch nicht auf den PC beschränkt bleiben. SMS-Spam auf Handys ist bereits im Vormarsch. Viren könnten bald folgen, da Smartphones neben Java demnächst auch das Internetprotokoll TCP/IP nutzen werden. Gefahr droht überall, wo Computer im Einsatz sind. Zum Beispiel in Multimedia-Servern für die Steuerung von TV, DVD und Musik. Oder in Autos, wo heute bereits mehrere Prozessoren für die Fahrzeugsteuerung und Bordunterhaltung arbeiten. Sollte eines Tages die Müll- und Virenwelle auch Handys, Stereoanlagen und Autos lahmlegen, dürften die Emotionen bei den Opfern hochgehen und Rachgelüste geweckt werden.

Doch die gerechte Strafe müsste die Spammer und Cracker ja nicht gleich in Form eines Eispickels treffen. Eine lange Haftstrafe mit einem auf Dosenfleisch reduzierten Menuplan würde reichen. Für die pädagogisch wertvolle Unterhaltung könnte allenfalls ein Wikingerchor sorgen.

Claude Settele ist Redaktor für Medien und Informatik bei der NZZ.