

Daniel A. Rehbein
Hörder Semerteichstraße 192
44263 Dortmund

<http://www.daniel-rehbein.de>

Dortmund, 07. Juli 2003

Pressemitteilung

Versender von illegaler Massen-E-Mail („SPAM“) will Gegner mundtot machen.

Zum Zweck der einfacheren Weiterverwendung kann der Text dieser Pressemitteilung als Microsoft-Word- und als PDF-Dokument online unter der Adresse <http://rehbein.net/teleinfo.html> abgerufen werden.

Genau wie die Menge an unerwünschter Werbepost, so wird auch die Zahl ihrer aktiven Gegner immer größer. In verschiedenen Foren im Internet tauschen sie ihre Erkenntnisse über die Versender illegaler Massenmails aus, analysieren die technischen Daten dieser Mails und geben sich Tipps über Gegenmaßnahmen. Ein Versender von Bulk-Mail, die Firma Teleinfo in Garbsen bei Hannover, will nun mit einem juristisch klingenden Schreiben einzelne Spam-Gegner gezielt einschüchtern.

Fast jedem, der das Internet zur Kommunikation via E-Mail nutzt, sind sie bekannt: Unerwünschte Werbemails, die von Tag zu Tag in größerer Zahl im Postfach aufschlagen. Nach einem Sketch der Comedy-Gruppe Monty Phyton werden solche Mails als „SPAM“, eigentlich eine englische Hackfleisch-Marke, bezeichnet. Die korrekte Bezeichnung ist UCE (Unsolicited Commercial E-Mail) oder UBE (Unsolicited Bulk E-Mail).

Der Inhalt von Spam bewegt sich meist im zwielichtigen Milieu. Häufig werben diese E-Mails für Penisverlängerungen, Pornoseiten, gefälschte Hochschuldiplome oder mit ihnen werden 0190er-Dialer an arglose Internet-Nutzer verschickt. Entsprechend unerwünschter Werbung per Telefax oder Telephon ist auch die unerwünschte Werbung per E-Mail nach geltender Rechtsprechung verboten. Gerade am Arbeitsplatz ist der Aufwand, den jeder E-Mail-Nutzer zum Aussortieren der unerwünschten Massenpost braucht, ein erheblicher Kostenfaktor.

Zahlreiche Gerichtsurteile sprechen deshalb den Empfängern von Spam-Mails einen zivilrechtlichen Unterlassungsanspruch gegenüber dem Absender zu. Doch an die ist bei den meisten Mails schwer heranzukommen. Meistens werden Spam-Mails mit gefälschten Absendern über offene Server in Lateinamerika oder Fernost versendet. Und auch der Inhalt der Mails gibt häufig nur wenig Ansatzpunkte. 0190er-Nummern werden in einem komplizierten Geflecht von Subunternehmern verschoben, gefälschte Hochschuldiplome oder ähnliches sollen meist per Kreditkarte in Übersee geordert werden.

Spam-Versender bereits beim Adressensammeln aufspüren

Findige Spam-Gegner kamen deshalb auf die Idee, nicht nur die empfangenen Mails zu analysieren, sondern bereits an der Stelle einzugreifen, wo der Versender sich die Mailadressen seiner späteren Opfer beschafft.

Für das Sammeln von E-Mail-Adressen werden meistens sogenannte Harvester eingesetzt. Der Begriff „harvest“ ist englisch und bedeutet „ernten“. Ein Harvester ist eine Software, die in möglichst kurzer Zeit möglichst viele Webseiten besucht und sämtliche darin enthaltenen E-Mail-Adressen speichert, quasi die E-Mail-Adressen auf den Webseiten „erntet“. Genauso wie der Crawler einer Suchmaschine verfolgt ein Harvester sämtliche Links, aber er merkt sich nicht den Inhalt der besuchten Webseiten, sondern nur die darin enthaltenen E-Mail-Adressen. Besonders abgesehen hat es ein Harvester natürlich auf Homepages mit Gästebüchern oder Diskussionsforen, wo viele User mit ihrer E-Mail-Adresse eingetragen sind.

Um Harvester in die Irre zu locken, gibt es CGI-Skripte, die dynamisch per Zufallsgenerator Webseiten aus sinnlosem Text (quasi einem dynamisch generierten Blindtext) mit Links erzeugen. Jeder dieser Links führt

wieder zum selben CGI-Skript mit zufällig generierten Parametern. Da die Parameterliste immer wieder anders ist, geht die Harvester-Software davon aus, daß es sich immer wieder um eine neue Webseite handelt und verfolgt beharrlich sämtliche Links. Da es kein Mensch ist, der die Webseiten abrufen, sondern nur eine Software, kann diese natürlich auch nicht erkennen, daß der Seiteninhalt völlig sinnlos ist. Stehen nun zusätzlich noch E-Mail-Adressen zwischen den sinnlos aneinandergereihten Wörtern, so kann man aufgrund von deren späterer Adressierung in Spam-Mails die Massenmail-Aussendung dem Harvester-Besuch zuordnen.

Die Webseiten von Daniel Rehbein

Daniel Rehbein aus Dortmund hat sich eine etwas andere Variante ausgedacht: Er hat ohnehin bereits eine ganze Sammlung von Webseiten, die dynamisch über CGI-Skripte in der Sprache PHP erzeugt werden. Mal wird der Besucher mit einer tageszeitabhängigen Grußformel begrüßt, mal kann er ein Gedächtnisspiel spielen und mal Rechenaufgaben ausführen lassen. Wenn ohnehin bereits ein PHP-Interpreter läuft, dann kann dieser auch gleich noch einen pro Seitenaufruf eindeutigen E-Mail-Link einfügen.

So ist in jeder dynamisch generierten Webseiten von Daniel Rehbein eine Mailadresse eingebaut, in der Datum, Uhrzeit und IP-Adresse des Seitenaufrufs codiert sind. Für einen normalen Besucher ist dies unsichtbar. Ein Harvester jedoch findet diese Adressen im HTML-Quelltext und liest diese aus. Kommt an diese Mailadressen dann Spam an, so ist ersichtlich, auf welchem Rechner (anhand der IP-Adresse) der Harvester gelaufen ist, wer also die Adressen gesammelt hat.

Übertragen auf die klassische Briefpost sähe dies so aus: Stellen Sie sich vor, ich hätte eine eigene Postleitzahl. Egal, welcher Name auf dem Brief steht, alle Briefe mit dieser Postleitzahl kommen bei mir an. Nun teile ich jedem, der mich besucht, einen anderen (fiktiven) Namen von mir mit, am einfachsten seinen eigenen. Wenn also Hans Meier mir einen Brief schreibt, so schreibt er an Hans Meier mit meiner Postleitzahl. Und wenn Lieschen Müller mir einen Brief schreibt, schreibt sie an Lieschen Müller mit meiner Postleitzahl. Wenn dann bei mir unerwünschte Werbung ankommt, wo als Empfänger Peter Schulte mit meiner Postleitzahl steht, so weiß ich sofort, daß es Peter Schulte war, der meine Adresse ohne mein Einverständnis weitergegeben hat. Alle Namen in diesem Beispiel sind natürlich frei erfunden.

Die Verfahrensweise, die sich Daniel Rehbein überlegt hat, ist in einer kleinen Demo auf der Webseite <http://spamfang.rehbein.net> dargestellt. In den dynamisch generierten E-Mail-Adressen ist sekundengenau der Zeitstempel des Seitenaufrufs und die aufrufende IP-Adresse enthalten. Kommen dann Spam-Mails bei ihm an, so weiß er sofort, zu welchem Zeitpunkt und von welchem Server der Harvester seine Seiten besucht hat. Eine Auswertung von Logfiles des Webservers ist dazu nicht notwendig.

Das Gewinnspiel der Firma Teleinfo

Im Juni 2003 berichteten diverse Diskussionsteilnehmer im Usenet-Forum de.admin.net-abuse.mail über E-Mails mit Werbung für das Gewinnspiel „map-scout“ der Firma Teleinfo in Garbsen bei Hannover. Mit Betreffzeilen wie „Bingo! Bonus für die Urlaubskasse!“ oder „Bar-Kohle mit MapScout!“ berichtete in diesem Mails ein angeblicher Gewinnspiel-Teilnehmer über das Gewinnspiel und forderte den Empfänger auf, ebenfalls teilzunehmen.

Eine Analyse der technischen Daten dieser E-Mails ergab, daß diese in Lateinamerika abgeschickt worden waren, an den wahren Absender war also nicht heranzukommen. Auf entsprechende Beschwerden wusch die Firma Teleinfo ihre Hände in Unschuld. Sie veranstaltete zwar das Gewinnspiel, bei dem es ein Ziel sei, möglichst viele weitere Mitspieler anzuwerben. Wie die Teilnehmer dies täten, läge außerdem des Einflussesbereichs von Teleinfo. Die Firma Teleinfo sicherte zu, die Namen der so aufgefallenen Teilnehmer aus den Gewinnerlisten zu streichen.

Doch anhand der Empfängeradresse der E-Mails, die Daniel Rehbein in dieser Angelegenheit erhalten hatte, kam dieser zu dem Schluß, das Teleinfo kaltschnäuzig gelogen hat. Aus den E-Mail-Adressen ging die IP-Nummer 62.48.74.61 hervor. Dies ist der Proxy-Server der Firma Teleinfo.

Die Verteilerliste für die Massenmails, die angeblich ein unbekannter Gewinnspiel-Teilnehmer versendet haben soll, ist also in Wirklichkeit von einem Harvester, der im Unternehmensnetz von Teleinfo lief, zusammengestellt worden!

Daniel Rehbein veröffentlichte seine Erkenntnisse im Usenet-Forum de.admin.net-abuse.mail und machte damit öffentlich, wie Teleinfo die Beschwerdeführer durch dreiste Lügen an der Nase herumgeführt hatte. Die Lawine von Diskussionsbeiträgen und Empörung, die diese Darlegung hervorrief, wurde offensichtlich auch von der Firma Teleinfo sehr aufmerksam verfolgt.

Denn nur wenige Tage später erhielt Daniel Rehbein ein Einschreiben von der Rechtsabteilung der Firma Teleinfo. In diesem wird ihm vorgeworfen, in erheblichem Maße gegen Rechtsvorschriften im Bereich des Datenschutzes zu verstoßen.

Unter Ignoranz des tatsächlichen und öffentlich dargelegten Sachverhalts wirft Teleinfo Daniel Rehbein vor, Verbindungsdaten unrechtmäßig gespeichert und an Dritte übermittelt zu haben. So schreibt Teleinfo beispielsweise „Sie werfen uns nebulös eine Verwicklung in sogenannten Spam vor und scheuen dabei nicht vor Gesetzesüberschreitungen zurück“. Mit einer Auflistung diverser Paragraphen und der Androhung weiterer „rechtlicher Maßnahmen und Schritte“ versucht Teleinfo, den Spam-Jäger einzuschüchtern und weitere kritische Veröffentlichungen zu unterbinden.

Eine absurde Situation, wie der Einbrecher, der den Hausherrn wegen Diebstahl anzeigt, weil dieser ihn auf frischer Tat ertappt und ihm sein Brecheisen weggenommen hat. Die Firma Teleinfo, die von Webseiten personenbezogene Daten, nämlich E-Mail-Adressen, in erheblichem Umfang und ohne legalen Zweck abgefragt und gespeichert hat, schießt nun mit Datenschutz-Argumenten gegen denjenigen, der mit Hilfe von Kontrolladressen diese Tat nachweisen konnte und die Beweisführung öffentlich dargelegt hat.

Offen bleibt, ob Teleinfo diesen mißlungenen Einschüchterungsversuch weiter fortsetzen wird. „Wenn Teleinfo gegen mich Klage erheben sollte, wird das bestimmt eine interessante Verhandlung“ blickt Daniel Rehbein optimistisch in die Zukunft. Anderen, denen ähnliches wiederfahren sollte, rät er: „Bangemachen gilt nicht!“.