

Aktuelle Entwicklungen bei der Spam-Bekämpfung

von Jochen Topf

jochen.topf@jtic.de

1 Einführung

Nachdem das Spamproblem jahrelang immer größer wurde, gibt es die ersten guten Nachrichten: Ende 2004 erklärte die Firma AOL in einer Pressemeldung¹, dass sie deutlich weniger Spam erhält. Andere können das nicht bestätigen, viele sehen immernoch einen Anstieg, einige immerhin eine Stagnation.² WEB.DE gibt Anfang Februar 2005 eine Zahl von ca. 16 Millionen Spams pro Tag an, vor einem Jahr war die Zahl noch halb so hoch, aber seit Oktober 2004 hat sich keine dauerhafte Erhöhung mehr ergeben.

2 Recht und Gesetz

In Deutschland (und der ganzen EU) ist das kommerzielle Spammen eindeutig verboten. Wohl auch deswegen bekommt man in Deutschland kaum Spam aus dem Inland. Der meiste Spam wird nach wie vor von den USA aus verbreitet.³ Dort gibt es seit Anfang 2004 den CAN-SPAM Act, ein Gesetz, das bestimmte Formen des Spam verbietet. Die Statistiken zeigen, dass das Gesetz bisher keinen Erfolg gebracht hat, allenfalls eine Umstellung der Methoden der Spammer, um sich innerhalb des Gesetzes zu bewegen.

In den letzten Monaten setzen große Firmen wie AOL und Microsoft verstärkt auf den Arm des Gesetzes.⁴ Einige Spammer wurden von Gerichten zu hohen Geldstrafen und teilweise auch zu langen Haftstrafen verurteilt.⁵ Damit soll natürlich eine abschreckende Wirkung erreicht werden. Und da nach Schätzungen des Spamhaus-Projektes⁶ der überwiegende Teil des Spam von nur ungefähr 200 Spammern⁷ verschickt wird, wäre mit einigen wenigen Verurteilungen auch durchaus eine Besserung zu erwarten.

Solange den Spammern nicht ausreichend mit juristischen Mitteln beizukommen ist, müssen Anwender und Firmen sich durch Filtermaßnahmen selbst schützen. Dabei ist aber wiederum zu beachten, dass die Gesetze eingehalten werden: Das OLG Karlsruhe hat erst kürzlich entschieden, dass das Unterdrücken von E-Mail strafbar sein kann.⁸ Wenn man die E-Mail Dritter filtert, ist also darauf zu achten, dass man eine Erlaubnis⁹ dazu hat, z. B. durch entsprechende Klauseln in einer Betriebsvereinbarung oder in den AGB.

3 Die Spammer

Vor ein paar Jahren noch waren viele Spammer Hobbyisten, die das Medium E-Mail neu entdeckt hatten. Inzwischen sind die Spammer professioneller geworden. Die

1 http://media.aoltime Warner.com/media/newmedia/cb_press_view.cfm?release_num=55254331

2 <http://www.eweek.com/article2/0,1759,1756981,00.asp>

3 <http://www.sophos.com/spaminfo/articles/dirtydozen.html>

4 <http://legal.web.aol.com/decisions/dljunk/>, <http://www.microsoft.com/presspass/press/2004/mar04/03-10CANSPAMpr.asp>

5 <http://www.spamhaus.org/news.lasso?article=155>

6 <http://www.spamhaus.org/>

7 <http://www.spamhaus.org/rokso/index.lasso>

8 <http://www.heise.de/newsticker/meldung/55201>

9 <http://www.heise.de/ct/03/26/186/>

Software, die sie benutzen, wird professionell entwickelt und vertrieben, hat eine einfach zu bedienende GUI und ist flexibel konfigurierbar.¹⁰ Spammer haben viele Tricks gelernt, die ihnen helfen, die Antispam-Filter zu umgehen.¹¹ Die einfachen Filter „fangen“ heute viele Spam-Mails nicht mehr.

Und die Spammer sind krimineller geworden. Schon lange wird der Spam nicht mehr direkt von eigenen Maschinen des Spammers verschickt. Stattdessen werden fremde Mailrelays und Open Proxies verwendet, um den Spam abzusetzen, ohne dass der Empfänger den eigentlichen Urheber erkennen kann. Mehr und mehr werden dazu auch viren- oder wurmverseuchte Rechner – Zombies – verwendet, die in sogenannten Botnets zusammengefasst und zentral kontrolliert werden. Spammer arbeiten heute Hand in Hand mit Hackern und Betreibern von solchen Botnets zusammen.¹² In einer regelrechten Untergrundwirtschaft werden Kreditkartennummern, E-Mailadressen und infizierte Rechner gehandelt. Ein Zombie-Rechner ist beispielsweise für schlappe 3 US\$ im Monat zu mieten.¹³

Einzelne Botnets umfassen heute nicht selten mehrere 10.000 Rechner, und viele solcher Botnets operieren gleichzeitig im Internet. Manche Botnet-Software kann schon dynamisch aktualisiert werden und ist damit hochflexibel. Botnets können für das Verteilen von Spam, für DDoS-Angriffe, zum Infizieren weiterer Rechner oder zum Ausspionieren der Anwender verwendet werden. Solange einzelne Personen die Möglichkeit haben, auf solche gigantischen Ressourcen zurückzugreifen, muss jede Maßnahme, die dieses Problem nicht berücksichtigt, ins Leere laufen.

Auch gegen Botnets gibt es Mittel. Aus der Erfahrung der letzten Jahre sehen wir, dass die Erziehung der Anwender und die Sicherung der benutzten Anwendungen und Betriebssysteme nicht ausreicht. Selbst wenn 90 % der Anwender Security-Patches installieren (was sicher eine unerreichbar hohe Zahl ist), bleiben immer noch viele Millionen Rechner übrig, die unsicher sind. Stattdessen muss hier von Seiten der Internet-Provider eingegriffen werden.

Über eine Trafficanalyse oder sogar Portscans können ISPs infizierte Rechner ihrer Kunden erkennen und diese vom Netz abhängen. In der Praxis ist das allerdings nicht ganz einfach und vor allem sehr support-intensiv. Ein anderer Ansatz wendet sich deswegen an die Kontroll-Rechner, von denen aus das Botnet gesteuert wird. So muss nur der kritische Rechner im System gefunden und ausgeschaltet werden.

4 Antispam-Maßnahmen

In den letzten Jahren ist eine unglaubliche Vielfalt an Antispam-Maßnahmen entwickelt worden, so dass es schwierig ist, den Überblick zu bewahren. Die Verfahren unterscheiden sich unter anderem danach, auf welche Merkmale (IP-Adresse, Absenderadresse, Inhalt, Menge/Frequenz) von Spam sie sich beziehen und an welchem Ort sie angewendet werden (Server oder Client, vor oder nach Annahme der E-Mail).

In der Regel werden sequentielle Kombinationen mehrerer Verfahren verwendet, die sich auf vielfältige Weise gegenseitig ergänzen können. Dabei werden oftmals billige, weniger ressourcenintensive Verfahren (wie DNSBLs) zuerst verwendet, um eine Vorfilterung durchzuführen und der Spam, der dann noch durchkommt, in weiteren, aufwändigeren Filterstufen (z. B. mit dem Bayes-Verfahren) geblockt. Alternativ kann man mehrere Verfahren parallel anwenden und die Ergebnisse aller in einem Scoring-

10 siehe z.B. <http://www.dark-mailer.com/>, <http://www.send-safe.com/>, <http://www.bestextractor.com/>

11 <http://www.rickconner.net/spamweb/tricks.html>

12 Ferngesteuerte Spam-Armeen. Nachgewiesen: Virenschreiber lieferten Spam-Infrastruktur. c't 5/2004, S. 18 ff.

13 <http://research.microsoft.com/~joshuago/tutorialOnJunkMailFilteringjune4.pdf>

Verfahren „zusammenrechnen“, um so eine höhere Zuverlässigkeit zu erreichen.

Im folgenden soll eine (unvollständige) Aufzählung einiger Verfahren einen Einblick in die derzeitigen Möglichkeiten geben:

Billig: DNSBLs

Von den meisten IP-Adressen kommt entweder nur Ham (Nicht-Spam-Mail) oder nur Spam. Deswegen ist es durchaus sinnvoll, eine Filterung nach der IP-Adresse des einliefernden Rechners vorzunehmen. Zu diesem Zweck existieren im Internet jede Menge¹⁴ sogenannter DNSBLs (DNS Blacklists), die deswegen so heißen, weil das Domain Name System (DNS) zur Abfrage benutzt wird, ob ein IP-Adresse aufgeführt ist.

Es gibt viele Varianten von DNSBLs, die jeweils andere Policies haben. Manche sammeln IP-Adressen, von denen erwiesenermaßen Spam verschickt wurde, manche testen IP-Adressen automatisch auf Open Relays oder Open Proxies, manche listen einfach alle bekannten dynamischen IP-Adressbereiche, hinter denen z. B. DSL-Kunden mit (wahrscheinlich) schlecht gesicherten Rechnern sitzen. Bei der Auswahl der benutzten DNSBLs sollte auf jeden Fall berücksichtigt werden, dass die Betreiber und damit die Listen nicht immer wirklich zuverlässig sind. Empfehlenswert sind zum Beispiel die Listen des Spamhaus-Projektes.¹⁵

DNSBLs haben ihre Kritiker¹⁶, werden aber doch vielfach benutzt, weil sie vor allem einen Vorteil haben: Sie sind konkurrenzlos billig und einfach zu benutzen. Der Overhead pro E-Mail ist im Gegensatz zu fast allen anderen Verfahren vernachlässigbar. Deshalb sind sie auch weiterhin ein gutes Element im Maßnahmenmix.

Effektiv: Bayes-Filter

Statistische Filter werden durch Vorlage von Spam und Ham trainiert und extrahieren selbständig aussagekräftige Merkmale in der E-Mail, die sie dann zur Filterung verwenden. Das ursprünglich 2002 von Paul Graham¹⁷ zur Filterung von Spam vorgeschlagene Bayes-Verfahren erfreut sich nach wie vor einer großen Beliebtheit und ist in verschiedenen Varianten in zahlreichen Produkten eingebaut. Daneben gibt es inzwischen aber auch einige andere Algorithmen mit ähnlicher Funktionsweise. Trotz aller Versuche von Spammern, solche Verfahren zu überlisten, sind sie weiterhin sehr effektiv. Bei entsprechendem Training können Erkennungsraten von 98 bis über 99 % erreicht werden, bei False-Positiv-Raten von kleiner als 0,1 %. Damit sind sie besser als ein Mensch, der bei der Filterung vieler E-Mails auch Fehler machen wird.

Die Effektivität des Verfahrens wird durch einen erheblichen Rechenaufwand erkauft. Dieser rührt zum einen von den aufwändigen mathematischen Algorithmen her, zum anderen hat er seine Ursache aber auch in der notwendigen „Vorbehandlung“ der E-Mails, um den Tricks der Spammer entgegenzuwirken. Diese „Vorbehandlung“ muss MIME-kodierte Texte auspacken, HTML-Mails erkennen und behandeln, zufällig ausgewählte Füllworte entfernen usw. In diesem Bereich wird viel geforscht, um die Verfahren zu verbessern. Da die statistischen Verfahren so viel Rechenzeit erfordern, ist ihr Einsatz in Mailsystemen mit sehr hohem Durchsatz nicht oder nur sehr eingeschränkt möglich.

Das notwendige Training dieser Verfahren dagegen, das anfangs noch recht umständlich

14 <http://www.moensted.dk/spam/>

15 <http://www.spamhaus.org/>

16 <http://theory.whirlycott.com/%7Ephil/antispam/rbl-bad/rbl-bad.html>

17 Graham, Paul: A Plan for Spam. <http://www.paulgraham.com/spam.html>

war, ist heute einfacher geworden, da Mailclients entsprechende Funktionen eingebaut haben. Unter Umständen reicht es sogar, auf ein manuelles Training zu verzichten und stattdessen ein automatisches Verfahren zu benutzen, das selbständig sicher als Spam erkannte E-Mails zum Training benutzt.

Im Kommen: Greylisting

Beim Greylisting-Verfahren¹⁸ werden alle E-Mails vom Mailserver beim ersten Auslieferungsversuch mit einem temporären Fehler abgelehnt. Da die meisten Spammer spezielle Software zum Versand ihrer E-Mail benutzen, die auf hohen Durchsatz getrimmt ist und keinen zweiten Zustellungsversuch unternimmt, wird der Spam effektiv blockiert. Ham dagegen wird von Mailservern versandt, die gemäß den Mailstandards nach einiger Zeit eine erneute Zustellung versuchen.

Das Verfahren ist zur Zeit sehr effektiv und wird von mehr und mehr Organisationen eingesetzt. Einige Nachteile sollten aber nicht verschwiegen werden: Zunächst einmal wird jede E-Mail von einem unbekanntem Empfänger um einige Minuten oder Stunden verzögert. Zudem ist mit False Positives zu rechnen, wenn MTAs sich nicht an die Standards halten, was bei einiger älterer Software der Fall ist. Solche Fälle muss man durch Whitelisting der entsprechende Rechner umgehen. Das Greylisting greift auch nicht mehr, wenn Spammer dazu übergehen, ihre Mails auf normalem Weg über Mailserver zu versenden, ein Weg, der in der letzten Zeit wieder häufiger von Spammern genommen wird.¹⁹

Vielversprechend: Frequenzanalyse

Durch die zunehmende und effektivere Filterung bei vielen Empfängern müssen die Spammer immer mehr E-Mail versenden, um überhaupt noch ausreichend viel Spam durch die Filter zu bekommen. Aber genau diese Menge wird ihnen auch wieder zum Verhängnis. Jemand, der plötzlich viele E-Mails verschickt, fällt auf.

Große Mailsysteme, die eine entsprechend breite Datenbasis haben, können eine Frequenzanalyse durchführen und damit Anomalien erkennen. Kommt regelmäßig viel E-Mail von einem Absender, so ist das wahrscheinlich normal; es kann sich zum Beispiel um eine Mailingliste handeln. Wenn aber ein bisher inaktiver Rechner plötzlich viel E-Mail versendet, so ist das verdächtig.

Verfahren zur Frequenzanalyse sind relativ aufwändig zu implementieren und zu kalibrieren. Eine manuelle Intervention durch Admins, die z. B. legitime Newsletter in Whitelisten eintragen, ist in der Regel noch notwendig. Um so mehr wir über solche Verfahren lernen und sie weiterentwickeln, um so einfacher werden sie aber auch zu bedienen sein.

Die Frequenzanalyse eignet sich auch zur Filterung ausgehender E-Mail (siehe unten) und damit zur Erkennung infizierter Rechner im eigenen Netz bzw. unter den Kunden eines ISPs.

Noch unentschieden: SPF, SenderID und DomainKeys

Wenn man die Presseberichte im letzten Jahr verfolgt hat, könnte man glauben, die perfekte Maßnahme gegen Spam sei bereits entwickelt worden: SPF²⁰ (Sender Policy Framework) und SenderID²¹ (eine Kombination von SPF mit dem von Microsoft

¹⁸ <http://projects.puremagic.com/greylisting/>

¹⁹ http://news.com.com/2100-7349_3-5560664.html

²⁰ <http://spf.pobox.com/>

²¹ <http://www.microsoft.com/senderid/>

propagierten CallerID-Verfahren). Die MARID-Arbeitsgruppe der IETF, die diese und andere Vorschläge zur Absenderauthentifizierung sichten sollte, um einen gemeinsamen Standard auszuarbeiten, ist jedoch gescheitert.²² Das lag einerseits an der nicht zu erzielenden Einigung über technische Details, andererseits aber auch an den Patentansprüchen, die Microsoft auf ihr Verfahren angemeldet hat.

Auch ohne eine offizielle Standardisierung werden SPF und SenderID in der Praxis eingesetzt. Die breitere Basis hat dabei zur Zeit SPF.

Keines dieser Verfahren kann jedoch die Hoffnungen erfüllen, die viele in sie gesetzt haben. Viele Probleme, wie das der Weiterleitung, sind weiterhin nicht zufriedenstellend gelöst, die Kritik ist nicht verstummt.²³

Vielfach wurde auch die einfache Tatsache übersehen, dass alle diese Verfahren nur dazu dienen, die Absenderdomain zu authentifizieren. Im besten Fall kann der Empfänger also einigermaßen sicher sein, dass eine E-Mail vom Inhaber einer Domain oder mit dessen Einverständnis versandt wurde. Das sagt aber erstmal noch nichts über den Spam- oder Hamgehalt einer E-Mail aus. Sicher kann dadurch der Spam, der angeblich von AOL oder Hotmail kommt, verringert werden, aber dem Spammer steht es ja frei, selbst eine Domain zu registrieren und dann Absenderadressen aus dieser Domain zu verwenden, der er die passenden SPF-Einträge gegeben hat. Und genau dies ist bereits geschehen: Spammer sind schneller auf den Zug aufgesprungen als die Betreiber von Mailsystemen.²⁴

Lösen läßt sich dieses Problem nur durch Einsatz eines Reputationssystems, d. h. einer Datenbank, die zu jeder Domain speichert, ob aus ihr eher Spam oder eher Ham zu erwarten ist. Mit dem DNSBLs haben wir für das Merkmal „IP-Adresse“ bereits solche Verfahren, für das Merkmal „Absenderdomain“ steckt die Entwicklung erst in den Kinderschuhen. Ohnehin zeigt die Erfahrung mit DNSBLs, wie schwierig es ist, verlässliche Reputationssysteme zu betreiben.

Als Alternative zu den MARID-Methoden werden die sogenannten MASS-Verfahren (Message Authentication Signature Service) vorgeschlagen. Dabei wird jede ausgehende E-Mail mit einer Signatur im Header versehen, über die der Empfänger prüfen kann, ob die E-Mail von einem für diese Domain autorisierten Mailserver verschickt wurde. Das am weitesten verbreitete Verfahren, das unter anderem von Google Mail eingesetzt wird, heißt DomainKeys²⁵, Cisco hat das ähnliche IIM²⁶ vorgeschlagen. Aber genauso wie bei den MARID-Verfahren kommen wir ohne ein Reputationssystem nicht viel weiter. Zusätzlich wirft eine kürzlich vorgestellte Sicherheitsanalyse²⁷ einige Fragen zur Sicherheit der Vorschläge auf.

Die Firma Sendmail hat Empfehlungen zum Umgang mit den MARID- und MASS-Verfahren herausgegeben.²⁸ Absenderseitig empfehlen sie den Eintrag von SPF-Records im DNS und die Nutzung von DomainKeys, empfängerseitig nur eine vorsichtige Nutzung zur Filterung. Die Nutzung von SRS²⁹, also das Umschreiben des Envelope-Froms bei der Weiterleitung von E-Mails, lehnen sie explizit ab.

22 http://www.circleid.com/article/765_0_1_0_C/

23 <http://www.advogato.org/article/816.html>

24 http://www.ciphertrust.com/company/press_and_events/article.php?id=0000362

25 <http://antispam.yahoo.com/domainkeys>

26 Identified Internet Mail: <http://www.identifiedmail.com/>

27 Housley, R: Security Review of Two MASS Proposals. draft-housley-mass-sec-review

28 http://www.sendmail.net/tools/Sendmail_Auth_Reco_wp.pdf

29 <http://spf.pobox.com/srs/>

Mehr Erfahrungen nötig: Sender Verify

Spammer benutzen meist zufällige Absenderadressen; viele davon existieren gar nicht. Durch eine DNS-Abfrage läßt sich schnell ermitteln, ob die Absenderdomain existiert. Etwas aufwändiger ist die Rückfrage beim MX der Absenderdomain, ob die Mailadresse existiert. Das geschieht durch den Aufbau einer SMTP-Verbindung quasi in Rückrichtung und dem Versuch, dort eine E-Mail abzusetzen.

Zwar ist dieses Verfahren nicht perfekt, weil manche Mailserver E-Mail auch für Adressen annehmen, die nicht existieren (und sie dann später bouncen), aber wenn der MTA die Annahme ablehnt, dann kann man sich sicher sein, dass die Adresse nicht existiert, und das ist es, worauf es hier ankommt. Das Verfahren erzeugt auch keine False Positives, solange der Absender sein System richtig konfiguriert hat und eine gültige Absenderadresse angibt.

Selbstgebastelt: BATV gegen fehlgeleitete Bounces

Etwas aus dem Rahmen fällt das BATV-Verfahren³⁰ (Bounce Address Tag Validation). Es dient nicht der Erkennung von Spam, sondern wird benutzt, um Bounces, die durch eigene E-Mails ausgelöst wurden, von solchen zu unterscheiden, die durch fremde E-Mails mit gefälschter Absenderadresse hervorgerufen wurden.

Vereinfacht gesagt, wird für jede ausgehenden E-Mail eine spezielle Absenderadresse im Envelope verwendet, die nicht nur die eigentliche Absenderadresse enthält, sondern auch eine Signatur. Erreicht nun eine Bounce den Absender der E-Mail, so kann er die Signatur überprüfen und feststellen, ob er auch die ursprüngliche E-Mail versandt hat. Dann wird er den Bounce annehmen und sonst ablehnen.

Ablehnen statt Spam-Ordner

Jede E-Mail, die nicht angenommen wurde, muss auch nicht weiterverarbeitet werden und braucht keine Ressourcen mehr. Grundsätzlich spart man sich also einiges an Aufwand, wenn man eine Spam-Mail noch im SMTP-Dialog ablehnt, statt sie anzunehmen und dann in einem Spam-Ordner zuzustellen. Während die ersten Antispam-Programme noch in Procmail-Skripte oder ähnliches eingebunden wurden und deswegen die E-Mail erst zu sehen bekamen, nachdem sie angenommen wurde, bieten heute fast alle MTAs selber Antispam-Maßnahmen an oder sie haben passende Plugin-Schnittstellen, an denen man die Antispam-Software einbinden kann. Über diese Schnittstellen kann dann schon während des SMTP-Dialogs ein Spam- und Virencheck stattfinden.

Der Vorteil dieser Art der Filterung ist auch, dass der Absender von Ham im Falle eines False Positives eine Fehlermeldung bekommt und daran erkennt, dass seine E-Mail nicht zugestellt wurde.

Auf keinen Fall sollte man jedoch für erkannten Spam oder Viren Bounces generieren, da diese meist Unschuldigen zugestellt werden, deren Mailadresse vom Spammer missbraucht wurde.

Ausgehenden Spam bekämpfen

Fast alle Antispam-Maßnahmen greifen nur bei eingehender E-Mail. Jeder schützt sich eben selbst so gut er kann. Klar ist aber, dass es viel sinnvoller wäre, das Problem an der Wurzel zu packen und schon auf der Seite des Versenders den Spam zu stoppen.³¹ Dazu

³⁰ <http://mipassoc.org/batv/>

³¹ <http://www.taugh.com/weblog/2005/01/11>

gibt es mehrere Ansätze: Einmal kann eine Firma bzw. ein Provider den SMTP-Port ausgangsseitig für alle Rechner im eigenen Netz sperren, die nicht als Mailserver bekannt sind. Damit wird schonmal jede Mail durch das Nadelöhr des eigenen Mailserver gezwungen, wo weitere Maßnahmen ansetzen können. Spätestens wenn sich Verfahren wie SPF und DomainKeys durchsetzen, wird es sowieso notwendig, alle ausgehende E-Mail durch einen zentralen Server zu leiten, weil nur der die entsprechenden SPF-DNS-Einträge hat bzw. die DomainKeys-Signatur in den Header einfügen kann.

Auf dem Mailserver kann dann die Menge und Häufigkeit des Mailversands von einer IP-Adresse (bzw. einem Kunden) überwacht werden. Sendet ein Rechner, der sonst eher inaktiv ist, plötzlich sehr viele E-Mails oder geht ein hoher Prozentsatz ausgehender E-Mail an nicht-existierende Adressen, so sollten die Alarmglocken schrillen. Zusätzlich kann man im eigenen Netz nach Open Relays, Open Proxies und anderen Hinweisen auf infizierte Rechner fahnden. Manche Provider haben angefangen, solche Systeme zu entwickeln, und es ist zu erwarten, dass mehr und mehr nachziehen werden, um zu verhindern, dass ihre eigenen Mailserver als Spamschleudern auf schwarze Listen geraten.

Eine Alternative zur Sperre des SMTP-Ports ist MTA-Mark.³² Dabei markiert der „Besitzer“ einer IP-Adresse im DNS, ob auf diesem Rechner ein Mailserver läuft. Der Eintrag sieht dabei ähnlich aus wie ein Reverse-DNS-Eintrag. Der empfangende Mailserver kann dieses Flag nun abfragen und selbst entscheiden, ob er E-Mails von einem Rechner annehmen will, der explizit als „Nicht-Mailserver“ gekennzeichnet ist. Im Moment ist das MTA-Mark-Verfahren allerdings noch recht neu und nicht weit verbreitet.

5 Ausblick

Anfang 2004 hat Bill Gates versprochen, dass Spam in zwei Jahren besiegt sei. Damals, wie auch heute – ein Jahr später –, wirkt diese Vorhersage etwas zu optimistisch. Den Spam ganz besiegen werden wir weder in einem Jahr noch in zehn Jahren.

Andererseits gibt es aber auch durchaus Grund, nicht zu verzweifeln: Vor nicht allzulanger Zeit noch sah es so aus, als ob uns das Spamproblem über den Kopf wachsen würde. Heute verfügen wir über eine erstaunlich große und vielfältige Anzahl von Maßnahmen gegen Spam, die zusammengenommen einer Lösung sehr nahe kommen. Mailsysteme, die dem Stand der Technik entsprechen, können heute das Spamproblem auf eine Größenordnung zurückschneiden, die für den Endanwender problemlos zu ertragen ist. Sicher kosten solche Systeme viel Geld, aber mit der Zeit werden wir uns daran gewöhnen und aufhören, darüber zu lamentieren. Schließlich beschweren wir uns auch nicht täglich darüber, dass wir unser Auto abschließen müssen, weil es sonst geklaut wird.

Es ist nur eine Frage der Zeit, bis die Systeme allgemein eingesetzt werden und genug operationelle Erfahrung vorliegt, dass sie einfach, sicher und ohne viele False Positives betrieben werden können. Die kommerziellen Lösungen haben sich in den letzten Monaten deutlich verbessert.³³

Ganz ohne Spam jedoch wird die Welt nie wieder sein. Dafür sorgen schon die Anwender, die wieder und wieder durch Spam beworbene Webseiten und Produkte anschauen und kaufen. Nach einer Umfrage von Forrester Data im Auftrag der Business

32 Stumpf, M.; Hoehne, S.: Marking Mail Transfer Agents in Reverse DNS with TXT Rrs. draft-stumpf-dns-ntamark

33 <http://www.nwfusion.com/reviews/2004/122004spampkg.html>

Software Alliance (BSA) lesen Anwender in Deutschland 25 % der Spam-Mail, die sie erhalten, und 43 % der Befragten haben als Folge einer Spam-Werbung schon Produkte gekauft.³⁴ Dabei ist es nicht nur der Spam im Posteingang, der erfolgreich ist. Manche Anwender machen sich sogar die „Mühe“, ihren Spam-Ordner anzuschauen und bereits klar als Spam markierte E-Mails zu lesen und die beworbenen Webseiten aufzurufen.³⁵

Nicht nur E-Mail ist betroffen

Wie eigentlich zu erwarten war, nimmt Spam auch in anderen Medien (SMS, Instant Messaging (IM), Wikis, Blogs, ...) zu. Während IM-Spam („Spim“) und SMS-Spam ähnlich wie bei E-Mail-Spam dem Benutzer etwas verkaufen oder ihn zum Anruf einer teuren Telefonnummer animieren wollen, ist die Situation bei Wiki-Spam und dem Comment-Spam in Blogs und Newsforen etwas anders. Dort geht es meist darum, den Webseiten des Spammers ein besseres Ranking in Suchmaschinen wie Google einzubringen. Google hat dazu kürzlich zusammen mit anderen Suchmaschinen ein Gegenmittel angekündigt.³⁶

Und weiterhin werden neue Dienste und Protokolle eingeführt, ohne geringste Überlegungen dazu, wie die Spammer sie ausnutzen werden und wie man bereits im Design Vorkehrungen dagegen treffen könnte. Mit Voice-over-IP ist schon der nächste Dienst in den Startlöchern, der Spammern und Antispammern neue Herausforderungen bescheren wird.

Dabei hat die E-Mail-Community in den letzten Jahren vieles über das Spamproblem und seine Bekämpfung gelernt, das auch in anderen Bereichen nützlich sein kann. Beispielsweise verstecken sich Comment-Spammer genauso gerne hinter Open Proxies wie es E-Mail-Spammer tun. Damit kann hier das gleiche Konzept der Blacklisten zum Einsatz kommen, es können sogar teilweise dieselben DNSBLs verwendet werden.³⁷

6 Weitere Information

Wer sich weiter zum Thema Spam informieren will, findet im Web Unmengen an Informationen, die allerdings nicht immer leicht zu erschließen sind. Neben der guten Übersicht in der Wikipedia³⁸ will ich hier nur eine sehr umfangreichen Linksammlung ("everything you didn't want to have to know about spam") erwähnen:
<http://spamlinks.net/>

Nachdem es im Buchsektor lange Zeit ruhig war, sind im letzten Jahr mehrere Bücher zum Thema Spam herausgekommen. Hervorzuheben ist hier das spannend geschriebene „Spam Kings“ von Brian McWilliams (O'Reilly Media, 2004) mit vielen Geschichten von Spammern und Anti-Spammern. Eine Liste mit Büchern zum Thema Spam (und allgemein E-Mail) gibt es unter <http://ref.allthingsemail.org/books/index.html>.

34 Consumer Attitudes Toward Spam in Six Countries, December 2004:

<http://www.bsa.org/usa/events/loader.cfm?url=/commonspot/security/getfile.cfm&pageid=20654&hitboxdone=yes>

35 <http://www.oreilynet.com/pub/a/network/2005/01/20/spamfolder.html>

36 <http://www.google.com/googleblog/2005/01/preventing-comment-spam.html>

37 Auch für Internet Relay Chat (IRC) Server wird das schon lange verwendet:
<http://wiki.blitzed.org/BOPM>

38 <http://en.wikipedia.org/wiki/Spamming>