Seminar Internet & Internetdienste

SS 2004

Bernd Öchsler

Spam

1. Was ist Spam?

1.1 Herkunft & Geschichte

Spam, eigentlich die Abkürzung für **Sp**iced H**am** (bzw. **S**piced **P**ork **A**nd **M**eat / Ha**m**), also Dosenfleisch der Firma Hormel Foods (s. Abb. 01), ist mittlerweile eher als Bezeichnung für unverlangt zugestellte, meist Werbe-E–Mails, die in grossen Mengen verschickt werden, bekannt , eine mögliche Interpretation ist **S**tupid **P**erson **A**dvertise**m**ent oder **S**ending **P**ersonally **A**nnoying E-**M**ails.

Abb. 01 SPAM

Der Zusammenhang zum Dosenfleisch entstand durch einen Sketch der englischen Komikergruppe „Monty-Python“: In einem Restaurant besteht die Speisekarte ausschliesslich aus Gerichten, die Spam enthalten. Ein Kunde fragt nach einem Gericht ohne Spam, die Besitzerin wiederholt jedoch immer nur die Liste mit den Spamgerichten, woraufhin jedesmal ein Wikingerchor anfängt ein Loblied auf Spam (s. Abb. 02)zu singen, bis das Lärm unerträglich wird und sämtliche Kommunikation unmöglich macht.

Lovely Spam, Wonderful Spa-a-m,
Lovely Spam, Wonderful Spam,
Spa-a-a-a-a-a-a-am,
Spa-a-a-a-a-a-a-am,
SPA-A-A-A-A-A-A-AM,
SPA-A-A-A-A-A-A-AM,
LOVELY SPAM, LOVELY SPAM,
LOVELY SPAM, LOVELY SPAM,
LOVELY SPA-A-A-A-AM . . .
SPA-AM,
SPA-AM,
SPA-AM,
SPA-A-AM!

Abb. 02 Das „Spam“-Lied

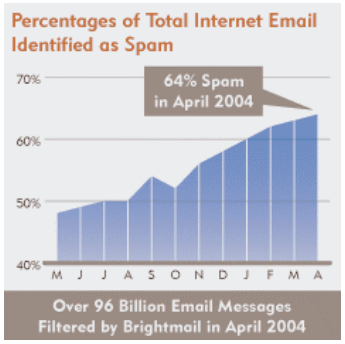
Im April 1994 plazierte nun die amerikanische Anwaltskanzlei Canter & Siegel Werbung für eine Greencard – Lotterie mit Hilfe eines kleines Programms in allen Diskussionsforen des Usenet. Die Forenuser waren entsprechend aufgebracht und ein Nutzer soll in Anlehnung an den Sketch geschrieben haben: ‚Schickt Canter Dosen mit Spam!“
Ob die Canter-Werbung tatsächlich der erste Spam war, wird gern diskutiert, manche Nutzer nennen einen Unbekannten mit dem Kürzel JJ, der sich 1988 in diversen Foren als Student ausgab und um Geld für sein letztes Studienjahr bat, als ersten Spammer, andere einen Mitarbeiter an einem US-College, der im Januar 1994 in über 5000 Diskussionsforen die Botschaft ‚Jesus lebt“ platziert haben soll. [1]

In der Internet - Community ist das Wort Spam auch allgemeiner für sämtliche unnötigen Kommentare gebräuchlich, z.B. Antworten in Foren, die nichts mit dem Thema zu tun haben (off – topic). Hier werden wir hauptsächlich den ‚klassischen“ Spam per E-Mail betrachten., auch wenn sich in letzter Zeit durch die verstärkte Abwehr von E-Mail-Spam neue Formen z.B. in den Instant-Messenger-Programmen (ICQ, Windows Messenger, sog. „Spim“) oder auch per SMS auf Handys ausbreiten (beinahe 90% in Japan! [2]).

1.2 Ziel, Zweck & Zusammensetzung

Eine mögliche Unterscheidung von Spam ist in UBE (**U**nsolicited **B**ulk **E**-Mail) und UCE (**U**nsolicited **C**ommercial **E**-Mail):
UBE ist unverlangte Massen-Email, die also an eine grosse Anzahl von Empfängern gesendet wird, ohne dass diese sie bestellt hatten. Meist sind dies eher zweifelhafte Angebote, wie Medikamente zur Gewichtsreduzierung oder Potenzmittel oder auch Websites mit erwachsenen-orientiertem Inhalt. Häufig sind diese noch mit einem Link versehen, der den Download eines Dialers startet. (sog. „Dialer-Spam“). Für eine genauere Einteilung von Spam siehe Abb. 04 und [3].
UCE ist unverlangte kommerzielle E-Mail. Im Unterschied zur UBE steht hier die komerzielle Absicht des Absenders und nicht der Massenversand im Vordergrund. Also gilt auch eine einzelne Mail, die mit der Absicht, einen Geschäftsabschluss zu erreichen versandt wurde als UCE. [2]

Es gibt allerdings auch noch Spam-Mails, die z.B. als Träger von Viren oder Trojanern versendet werden, die sich nach Öffnen der Mail im Computer festsetzen und z.B. ein Dialer-Programm installieren oder dem Versender erlauben, die Adresse des Opfers als weiteren Spam-Versender zu verwenden (siehe Abschnitt 2).



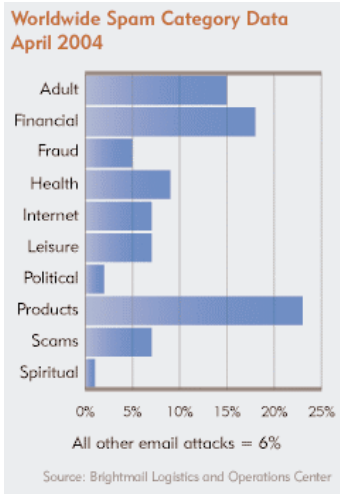


Abb.03 & 04 : Spam-Anteil und –Zusammensetzung im April2004

2. Wie verbreitet sich Spam?

Grundsätzlich lassen sich Massen-E-Mails ohne grossen Aufwand mit einfachen Programmen versenden. Da im SMTP-Protokoll ohne entsprechende Vorsichtsmassnahmen des Providers jede richtig formatierte E-Mail-Adresse (also *@*) akzeptiert wird (Beispiele dazu siehe [4]), liegt die eigentliche Aufgabe darin, ausreichend viele E-Mail-Adressen sowohl als Absender als auch als Empfänger zu besitzen. Daher wird in diesem Abschnitt hauptsächlich auf die Tricks und Vorgehensweisen der Adressensammler eingegangen.

2.1 Crawler & Harvester

E-Mail-Adressen sind überall im Internet zu finden. Sei es bei den Diskussionsforen im Usenet, bei den Instant-Messengern oder auf verschiedensten Seiten im WWW. Da viele Internet-Nutzer nicht im Usenet vertreten sind und die meisten Anwender von Messengern für die Masse anonym bleiben wollen, ist die ergiebigste Quelle für Adressensammler das World Wide Web, wo sich mittlerweile unzählige Privatpersonen, Firmen und Vereine eigene Homepages eingerichtet haben. Dort findet sich meistens dann nicht nur die E-Mail-Adresse des jeweiligen Autors oder Administrators der Seite, sondern auch in Gästebüchern, Mitgliederlisten, etc... weitere Adressen. Diese können leicht durch geeignete Software herausgefiltert und in eine Datenbank aufgenommen werden. Diese Software nennt man **„Harvester“** (engl. „Ernter“), wobei die Progammierer solcher Programme andere Bezeichnungen wie „Online Marketing Tool“bevorzugen. Harvester sind eine Spezialform von sogenannten **„Crawlern“** („Krabbler“) oder **„Spidern“** („Spinnen“), die auch von den gängigen Suchdiensten genutzt werden. Diese Programme gehen von bereits bekannten Seiten über dort aufgeführte Links zu neuen Seiten, um von dort aus wiederum nach verlinkten Seiten zu suchen. Da Crawler von Suchdiensten vom Webmaster einer Seite „ausgesperrt“werden können, wenn sie nicht erwünscht sind, tarnen sich die Harvester, indem sie eine Kennung eines gültigen Browsers aussenden.
Da Harvester in möglichst kurzer Zeit möglichst viele Webseiten „abgrasen“sollen, arbeiten die meisten Programme nicht sehr gründlich und zeichnen alles auf, das dem gängigen E-Mail-Adressenformat (*@*) entspricht. Dass dabei auch sehr viel nutzlose Daten gesammelt werden, stört die Adressenhändler nicht besonders, da es gewisse Wege und Methoden gibt herauszufinden, ob die gefundene Adresse gültig und im Gebrauch ist oder nicht. Mehr dazu in Abschnitt 2.3.

2.2 andere Adressenquellen

Neben dem Sammeln von Adressen durch Harvester gibt es auch noch andere Möglichkeiten, wie Sammler an neue Adressen kommen.
Firmen erhalten Adressen, indem sie z.B. Gewinnspiele auf ihren Homepages anbieten, bei denen es kleine Preise zu gewinnen gibt. Natürlich muss man um teilzunehmen eine E-Mail-Adresse angeben. Die meisten seriösen Firmen versichern mittlerweile, dass die angegebene Adresse nur firmenintern verwendet (wobei man dann nicht von firmeninternen Werbung verschont wird oder - falls in den AGB angegeben - auch Werbung von Werbepartnern) und nicht an Dritte weitergegeben wird, dennoch gibt es Firmen und Privatpersonen, meistens selbst Spammer, die ihre selbst gesammelten Adressen weiterverkaufen.
Viele Spammer bedienen sich auch der Brute-Force-Methode: Da zur heutigen Zeit die Versandkosten auch von sehr vielen Mails verschwindend gering ist, gehen sie dazu über, einfach gängige Adresskombinationen (z.B. webmaster@.. info@.... oder häufige Vorname.Name – Kombinationen) durchzuprobieren oder sogar durch einen Generator erzeugen zu lassen. Dazu gehört auch das sogenannte SMTP-Harvesting. Dabei nutzt man o.g. Schwäche des SMTP-Protokolls sämtliche *@* Kombinationen zunächst einmal als E-Mail-Adresse anzusehen. Gemäß den SMTP-Standards liefert ein empfangender Server eine Fehlermeldung, wenn er eine Mail nicht ausliefern kann, weil die Adresse nicht existiert. So erkennt ein Spammer nun je nach Antwort des Servers, ob die Adresse existiert oder nicht. [5]

2.3 „Lockvögel“

Wenn ein Adressensammler nun eine E-Mail-Adresse über einen Harvester, eine gekaufte Liste oder durch ein Generierungsprogramm erhalten hat, kann er diese sofort in seinen Spamverteiler mit aufnehmen oder er will zunächst herausfinden ob sie für seine Zwecke zu gebrauchen ist. Um festzustellen ob diese Adresse existiert und auch in Gebrauch ist, bedient er sich verschiedener Methoden, von denen hier die zwei gebräuchlichsten vorgestellt werden sollen:

2.3.1 Abmelde-Trick

Bei vielen Spam-E-Mails wird der Eindruck erweckt, diese Mail wurde empfangen, weil die Empfängeradresse in ein Verteilerverzeichnis eingetragen wurde. Nun wird freundlicherweise dem Empfänger angeboten, dass er sich wieder aus diesem Verteiler abmelden kann, indem er einfach nur auf den in der Mail enthaltenen Link (der oft die eigene Adresse beinhaltet) clickt. Gerade dadurch wird allerdings dem Spammer gezeigt, dass diese Mail existiert und in Gebrauch ist. Meistens wird die Adresse dann auch noch gleich in weitere Verteiler eingetragen.

2.3.2 HTML-Mails

Sehr viele E-Mails werden auch im HTML-Format versendet, d.h. es können Bilder, Musik, Hintergrundfarben, Smilies etc. eingebunden werden. Das Problem ist nur, dass diese Extras zuerst vom eigenen Rechner bei einem externen Server abgeholt werden müssen. Durch den Aufbau dieser Verbindung erhält natürlich dann der Spammer wiederum den Beweis, dass die E-Mail-Adresse genutzt wird und kann nun erst recht mit dem Versand von Spam-Mails beginnen.

2.4 Spam von der eigenen Adresse

Es kann vorkommen, dass man anscheinend eine E-Mail „von sich selbst“bekommt, also mit der eigenen Mail-Adresse als Absender. Häufig ist eine Fehlermeldung eines Mail-Demons der Inhalt. In diesem Fall wurde die eigene E-Mail-Adresse als falscher Absender angegeben, wobei die Mail jedoch nicht zugestellt werden konnte. Dass die Adresse nur gefälscht wurde und nicht tatsächlich vom eigenen E-Mail-Account abgeschickt wurde, kann man daran erkennen, dass die E-Mail von einer anderen IP-Adresse als der eigenen abgesandt wurde.

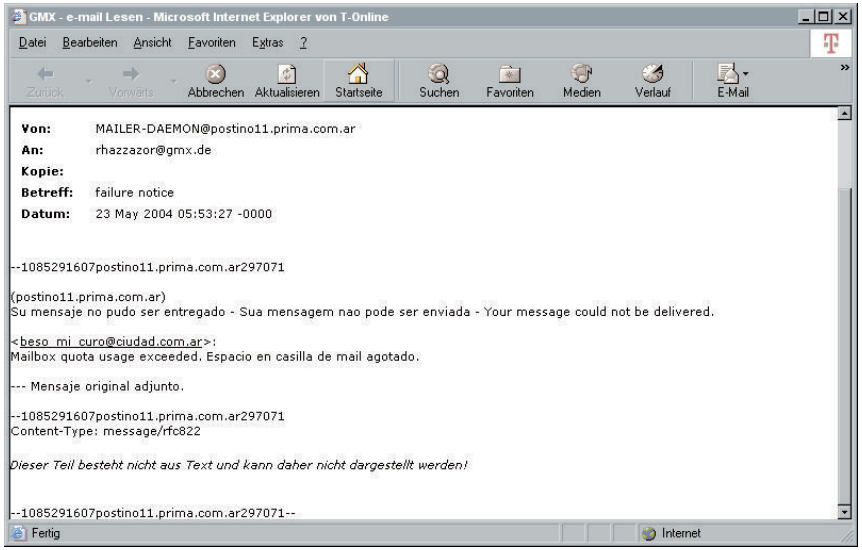


Abb. 05: fehlgeschlagene Spam-Mail mit eigener Absenderadresse

3. Welche Probleme verursacht Spam?

3.1 Privatpersonen

Spam verursacht für Privatpersonen auf verschiedenste Weise Probleme: Zuallererst belegen die ungewollten Massenmails Speicherplatz, der gerade bei kostenlosen E-Mail-Anbietern nicht unbegrenzt zur Verfügung gestellt wird, so dass bei einem beinahe vollen Postfach sehr leicht wichtige Mails nicht mehr zugestellt werden können. Sollten die Spam-Mails nicht automatisch gelöscht werden, so kostet dieser Vorgang zusammen mit dem Kennzeichnen und Verschieben von Spam, der durch die Filter ‚geschlüpft" ist, ausserdem Rechenzeit und verursacht so unnötige Verbindungskosten. Sollten die Spam-Mails automatisch gelöscht werden, so kann es passieren, dass auch Nicht-Spam-Mails diesem Vorgang zum Opfer fallen, z.B. weil der Absender eine Adresse besitzt, die vom E-Mail-Anbieter bzw. Spamfilter des Empfängers als unsicher eingestuft wird (Anbieter, ausländische Adresse, ‚kryptische" Adresse,...)
Des weiteren kann es passieren, dass man als vermeintlicher Spam-Versender (siehe 2.4) plötzlich mit Drohungen, Beschimpfungen, ja sogar Klagen konfrontiert wird, deren Klärung wiederum mit zusätzlichem Aufwand und evtl. Kosten verbunden ist.
Dies alles führt dazu, dass mittlerweile viele Internetnutzer ihre E-Mail-Adresse sehr häufig wechseln oder gar nicht mehr herausgeben, was eine Kommunikation natürlich extrem erschwert bzw. unmöglich macht.

3.2 Unternehmen

Das meiste, was bei Privatpersonen geschrieben wurde, lässt sich auch auf Unternehmen übertragen: Auch hier belegt Spam unnötigen Speicherplatz und seine Beseitigung kostet wertvolle Rechen- und viel wichtiger, Arbeitszeit.
Ausserdem kann es auch hier passieren, dass die Firmendomain, also @firma, als angebliche Absenderadresse von Spam-Mails angegeben wird, was natürlich für das entsprechende Unternehmen zu grossem Imageschaden führen kann.
Zusätzlich entstehen weitere Kosten, wenn das Unternehmen Spamfilter installieren muss, die meisten im Internet für Privatpersonen frei erhältlichen Spamfilter und Antivirenprogramme sind für Unternehmen kostenpflichtig. Dann kann es allerdings auch wie oben schon beschrieben, passieren, dass eigentlich erwünschte Mails durch den Filter aufgehalten werden, was natürlich bei Unternehmen noch grösseren Schaden anrichten kann als bei Privatpersonen.
Schliesslich kann es passieren, dass manche Internet-Angebote des Unternehmens, wie z.B. Newsletter, gar nicht erst von den Kunden wahrgenommen werden, aus Misstrauen, dass sie bei Angabe ihrer E-Mail-Adresse auch noch weitere Spam-Mails erhalten.

3.2.1 Internet-Unternehmen

Reine Internet-Unternehmen, vor allem E-Mail-Provider sind natürlich besonders von Spam betroffen. Neben den Problemen, die auch ein ‚normales" Unternehmen als Empfänger von Spam-Mails hat, kommen noch speziellere Probleme hinzu, da die Server der E-Mail-Provider quasi die unfreiwilligen „Versender" von Spam-Mails sind.
Da zum Versand anstehende Mails beim Mailserver in einer Warteschleife stehen und es genügt zu einer Spam-Mail nur eine Liste mit Empfängern anzugeben, die dann vom Mailserver abgearbeitet wird, kann es zu merkbaren Verzögerungen beim Versand von normalen Mails kommen, wenn der Server erst einmal 100.000 bis 1 Million Spam-Mails abarbeiten muss. [5] Daneben müssen die Mail-Provider nun auch in verstärkten Spamschutz investieren, also extra Personal und Mittel bereitstellen, was natürlich zusätzliche Kosten verursacht, die dann auch an den Nutzer weitergegeben werden, sei es durch Gebühren, um vom Spamschutz profitieren zu können, oder auch einfach nur durch erhöhte Werbung, z.B. durch Pop-Ups oder Mails. Dies stösst beim Kunden nicht unbedingt auf Verständnis, denn immerhin erhält er weiterhin unverlangte Werbemails, und muss sich mit dauernd auftauchenden Werbefenstern herumärgern.
Ausserdem können meist nur die Provider zur Verantwortung gezogen werden, wenn es darum geht, einen Spammer auszuschalten, was natürlich weiteren Aufwand und Imageschaden bedeutet. Wollen sie verhindern, dass Spammer sich ihrer Server bedienen, wäre eine Möglichkeit den Erwerb von E-Mail-Adressen zu erschweren (z.B. Adressüberprüfung, Gebühren), was wiederum bei den normalen Nutzern zu Verärgerung führen kann.

4. Was kann man gegen Spam tun?

In diesem Abschnitt werden einige Möglichkeiten vorgestellt, wie Spam vermieden und abgeblockt werden kann, sowohl von Seiten der Privatnutzer als auch der E-Mail-Provider, ebenso wie verschiedene Spamfiltersoftware, Lösungsansätze von Seiten der grossen Firmen und abschliessend einige Gesetzesregelungen gegen Spam. Grundsätzlich muss man zu den meisten Verfahren aber anmerken, dass natürlich auch die Spamversender versuchen, diese Massnahmen zu umgehen, mehr dazu bei den einzelnen Verfahren.

4.1 Prävention

Private Nutzer haben bereits schon ohne Installation von Spamfilter-Software einige Möglichkeiten, sowohl ihr E-Mail-Postfach als auch das anderer Nutzer vor Spam zu schützen, insbesondere werden hier einige Verfahren vorgestellt, mit denen man die Harvester der Adressensammler austricksen kann. Natürlich werden diese auch laufend weiter verbessert, so dass auch die hier vorgestellten Tricks kein absolutes Gegenmittel darstellen.

Zunächst einmal sollte man sich eine E-Mail-Adresse speziell für Gewinnspiele, Newsletter und ähnliche Internetangebote anlegen. Manche E-Mail-Provider bieten für diesen Zweck spezielle Wegwerf-Adressen an, die man bei Gewinnspielen o.ä. angeben kann, und die empfangenen E-Mails an die eigentliche Adresse weiterleiten. Sollte dann irgendwann Spam über diese Adresse empfangen werden, kann man sie einfach wieder löschen. Mehr zu diesem Thema siehe z.B. [6].
Auch für seine reguläre Adresse empfiehlt es sich, sie nicht nur aus seinem Vornamen oder ähnlichen gängigen Ausdrücken zu erstellen, da diese häufig von Spammern auf Verdacht hin angemailt werden. Auch drei- oder vierstellige Buchstabenkombinationen sind weniger sinnvoll, da gerade diese sehr leicht von Adressgeneratoren erzeugt werden. Allerdings sei an dieser Stelle angemerkt, dass mittlerweile auch eine vollständige Adresse vom Format vorname.name@example.com durchaus auch von Generatoren erzeugt werden kann.
Wenn man dennoch einmal eine Spam-Mail erhalten hat, sollte man auf keinen Fall anders darauf reagieren als sie ohne weiter Umstände zu löschen (ggf. höchstens erst in den entsprechenden Spamordner verschieben – siehe dazu auch 4.2.1). Auch wenn sie anscheinend einen Link angibt, an dem man sich ab sofort aus einem Verteiler austragen lassen könnte, sollte man darauf nicht eingehen, da man sonst nur bestätigt, dass diese E-Mail-Adresse in Benutzung ist (siehe 2.3.1).
Wenn möglich sollte man auch keine E-Mails ohne vorherige Überprüfung herunterladen und öffnen (wie es z.B. Outlook Express tut), da sonst die Gefahr besteht, dass eine Spam.Mail im HTML-Format dabei ist. (siehe 2.3.2)
Wenn man im Besitz einer eigenen Homepage ist, ist es empfehlenswert, sämtliche E-Mail-Adressen nicht als direkte Links im gänigen Format anzuzeigen, da gerade danach die Harvester suchen. Es gibt verschiedene andere Möglichkeiten Adressen anzuzeigen:

- Einfach „**ausgeschrieben**", z.B. vorname punkt name at anbieter punkt de. Diese Möglichkeit bietet sich auch an, wenn man seine Adresse in einer öffentlich zugänglichen Mailinglist oder einem Forum anzeigen möchte. Der Nachteil ist, dass so eine Kombination theoretisch auch sehr einfach in ein Harvester Programm integriert werden kann (z.B. mit regulären Ausdrücken) und zum anderen muss man auch noch mit dem DAU rechnen – dem Dümmsten Anzunehmenden User, d.h. es könnte sein, dass manche Besucher der Website vielleicht nicht verstehen, dass diese Wortkombination eine E-Mail-Adresse darstellen soll. Zusätzlich ist diese ‚Adresse" nicht direkt anklickbar, muss also erst noch in ein Empfängerfeld übertragen werden, was zwar nicht viel Aufwand ist, aber dennoch Aufwand, der unnötig erscheinen mag.
- als **Grafik**: Da die Harvester im HTML-Code der Seiten nach E-Mail-Adressen suchen, bietet es sich an, diese dort gar nicht aufzuführen sondern als Grafik einzubinden. Da fast jedes Grafikprogramm auch das Darstellen von Text ermöglicht, ist dies nicht allzu schwer zu bewerkstelligen. Gibt man dem Text dort auch noch keine allzu geradlinige Form, können auch versiertere Sammler die Grafik nicht so schnell als Adresse erkennen. Der Nachteil dieser Methode ist wiederum, dass die Adresse eigentlich nicht direkt angeklickt werden kann und wieder ‚umständlich" abgeschrieben werden muss. Dies kann aber auch durch ein kleines Programm gelöst werden, siehe Abb. 06.
- in **Unicode**: Bisher (!) können die meisten Harvester noch nicht Unicode lesen und beschränken sich darauf, den HTML-Code zu durchforsten. Also könnte man seine E-Mail-Adresse in Unicode darstellen und über ein kleines Java-Script übersetzen lassen, so dass die reguläre Darstellung gewahrt bleibt. Mehr dazu siehe [7]
- **Tags ergänzen**: Eine weitere einfache Möglichkeit seine Adresse vor den meisten Harvestern zu verstecken ist um das „@" – Zeichen Tags zu plazieren die in HTML nicht definiert sind und somit nicht übersetzt werden können. So wird die Adresse im Browser korrekt angezeigt und der Nutzer muss sie nur kopieren.

```
<script language="JavaScript">
        <script language="javascript">
        <!--
          function MailHref(joman) {
            var TheColonel  = "<a href='mailto:" + joman + "@webs" + "ite." + "de'>"  ;
            document.write(TheColonel);
          }
        // -->
        </script>

        <script language='javascript'> MailHref('administrator'); </script>
<img src='Pictures/email.jpg' width='247' height='32' border='0'></a>
        </script>
```

Abb. 06: Javaskript für versteckten Adresslink

Soweit zu den Massnahmen um die eigene E-Mail-Adresse vor zuviel Spam zu bewahren. Nun kann man aber auch noch gewisse Vorsichtsmassnahmen treffen, damit Adressen von anderen Nutzern auch nicht von Harvestern eingesammelt werden können. So ist es empfehlenswert und auch im Sinne der Privatsphäre, Massenmails nur über Verteiler oder mit Hilfe der BCC-Funktion zu versenden, so dass beim jeweiligen Empfänger nur die eigene Adresse angezeigt wird. Natürlich kann man auch wie in 4.1 beschrieben die Adressen „tarnen“, wenn man sie auf einer Website anzeigen möchte.
Ausserdem sollte man bei Darstellung von Beispieladressen auf einer Website die Bezeichnungen gem. RFC-Dokument 2606 verwenden. Bei Verwendung anderer Adressen besteht die Gefahr das diese Adresse tatsächlich existiert und von einem Harvester registriert wird. Mehr dazu siehe [8]

4.2 Software – Spamfilter

4.2.1 GMX-Spamfilter

Der Spamfilter des E-Mail-Providers GMX zeichnet sich durch insgesamt 7 Filtermethoden aus, die ein Spam durchdringen müsste, bevor er im Posteingang landet (genaueres siehe [9]) :

- **Textmuster-Profiler** : Dieses Programm arbeitet auf Basis der sogenannten „Bayes-Klassifizierung“: D.h. er ‚erlernt“ mit Hilfe statistischer Methoden, welche Mails vom Nutzer als Spam betrachtet werden und welche nicht. Jedes Mal, wenn eine Mail vom Posteingang in den Spamverdachtsordner verschoben wird, aktiviert sich der Profiler, analysiert und speichert den Inhalt der Mail und ordnet einzelnen Textmuster je nach Häufigkeit in erwünschten bzw. unerwünschten Mails einen bestimmten Wert zu. Bei jeder neu eingehenden E-Mail ermittelt der Profiler dann aufgrund dieser Werte die Wahrscheinlichkeit, dass es sich bei der neuen Mail um Spam handelt. Überschreitet das Ergebnis einen gewissen Schwellenwert, wird die Mail aussortiert.
  Momentan ist dieser Filter kostenpflichtig und nicht für die kostenlosen Adressen bei GMX verfügbar. Ausserdem haben viele Spammer auf solche Textmusteranalysen reagiert und fügen ihrer Mail eine Sammlung von Worten hinzu, die in vielen Mails verwendet werden, so dass der Profiler falsche Häufigkeitswerte erhält.
- **Briefkopf-Analyzer** : Ähnlich wie der Textmuster-Profiler, errechnet der Briefkopf-Analyzer eine Wahrscheinlichkeit, dass die eingehende Mail Spam sein könnte. Anstatt des Inhaltes wird hier jedoch der sog. „Header“ einer Mail, also Absender, Empfänger, Betreff, E-Mail-Client des Absenders, etc. analysiert. Mehr zur Headeranalyse siehe [10].
- **Spamserver-Blocker** : Hier wird die IP-Adresse der E-Mail analysiert, da viele Spamabsender zum Schein von einer Adresse eines bekannten Providers abgesandt werden. Durch Analyse der IP-Adresse kann nun festgestellt werden, ob sie tatsächlich diesem Anbieter gehört oder nicht.
- **Persönliche Blacklist / Whitelist** : Hier kann der Nutzer persönlich unerwünschte E-Mail-Adressen (ganz oder auch nur Teile, siehe Abb. 07) eingeben. Mails von dieser Adresse werden ab sofort als Spam eingestuft und auf Wunsch gar nicht mehr zugestellt, wobei dann der Absender gleichzeitig eine Meldung erhält, dass die Mail-Adresse nicht existiert und den Nutzer dann möglicherweise aus seinem Verteiler nimmt. Gleichzeitig besteht auch die Möglichkeit, Adressen in eine Whitelist einzutragen: Mails aus dieser Liste werden ohne weitere Kontrolle sofort zugestellt.
- **GMX-Team Antispam – Liste** : GMX beschäftigt ein spezielles Team, das sich eigens mit der Analyse und dem Erkennen von Spam beschäftigt. Auch hier wird eine Blacklist geführt.

- **Globale Antispam – Liste** : Diese Liste enthält die IP-Adressen sogenannter „Open-Relay-Server“; d.h. Server, über die Mails versandt werden können, ohne dass der Absender sich zuvor authentifizieren musste. Diese Server werden gerne von Spammern genutzt, da sie Kosten sparen und eigene Ressourcen schonen. Mails von solchen IP-Adressen werden ebenfalls als Spam behandelt.
- **Per Filterregel verschoben** : Hier werden sämtliche Mails, die nicht von einer Adresse aus dem Adressbuch des Nutzers stammen als Spam eingestuft. Der Einsatz dieses Filters bedarf also stetiger Pflege des Adressbuches.

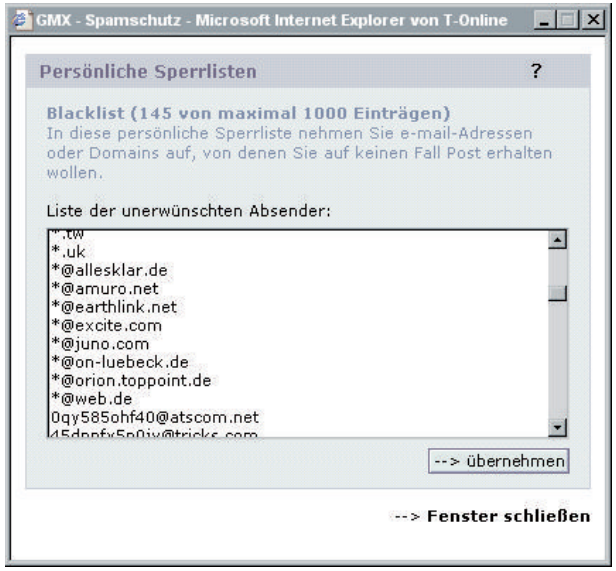


Abb. 07: persönliche Blacklist

Des weiteren blockiert GMX auch erst einmal die vollständige Darstellung von HTML-Mails, so dass der Nutzer bei jeder Mail selbst entscheiden kann, ob er dies wünscht.

4.2.2 Filter zum Download

In diesem Abschnitt werden einige Spamfilter vorgestellt, die kostenlos aus dem Internet heruntergeladen werden können. Solche Programme sind speziell für Nutzer sinnvoll, die ihre Mails mit E-Mail-Programmen aus ihrem Postfach auf ihre Festplatte speichern (z.B. Outlook Express).
Grundsätzlich sei noch darauf hingewiesen, vor dem Download und der Installation von Filterprogrammen die Hilfestellungen und Hinweise auf den angegeben Websites genau durchzulesen.

SpamPal : Dieses Programm, entwickelt von James Farmer, positioniert sich zwischen den POP3-Server und das E-Mail-Programm (siehe Abb.08), überprüft alle eingehenden E-Mails mit Hilfe von sog. DNSBL-Listen (d.h. Listen mit Verweisen auf Spammer) und markiert entsprechende Mails mit speziellen Headern oder einer Erweiterung im Betreff, so dass diese im E-Mail-Programm gelöscht werden können. Mit verschiedenen Plug-Ins kann die Markierung noch erweitert werden, so dass z.B. auch HTML-Mails nicht ausgeführt werden oder Spam mit Hilfe der Bayes-Methode erkannt wird.
Momentan ist SpamPal nur für Windows-PCs verfügbar und funktioniert auch nur bei Mailanbietern, die ein POP3 oder IMAP4-Postfach besitzen; bei manchen Anbietern (Yahoo, Hotmail) ist deshalb eine kleine Modifikation von Nöten. Für unternehmensweite Mail-Server ist SpamPal nicht empfehlenswert, da keine Administrator- und Sicherheitsfunktionen vorhanden sind. [11]

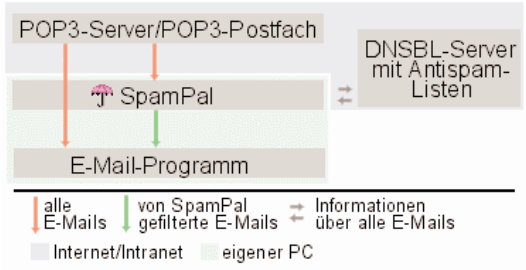


Abb.08 : So funktioniert SpamPal

Spamihilator : Auch dieses Programm schaltet sich zwischen Mail-Server und Mail-Programm, überprüft die eingehenden Mails mit Hilfe der Bayes-Methode, der Suche nach bestimmten Schlüsselwörtern und einer persönlichen Blacklist. Als Spam erkannte Mails landen dann in einem speziellen Papierkorb, wo sie noch einmal überprüft und gelöscht werden können, was auch nach einiger Zeit automatisch geschieht. Zur Zeit unterstützt Spamihilator keine IMAP-Protokolle, kann also nicht mit E-Mail-Adressen von Hotmail und AOL genutzt werden. [12]

Expurgate : Dieses Programm ist sowohl für Unternehmen als auch für Privatkunden verfügbar, wobei die Nutzung für Unternehmen kostenpflichtig ist. Um das Programm nutzen zu können wird eine zweite E-Mail-Adresse benötigt (nicht bei GMX-Nutzern). Man erhält bei Expurgate einen Account, an den alle eingehenden Mails weitergeleitet werden. Dort werden sie dann auf Spam untersucht und erhalten wiederum zusätzliche Headerinformationen, die das Ergebnis beinhalten (sauber / verdächtig / eindeutig Spam). Danach werden die Mails an die zweite E-Mail-Adresse weitergeleitet, wo sie dann vom Nutzer abgeholt und vom Programm je nach Headerinformation entsprechend behandelt werden können. [13]

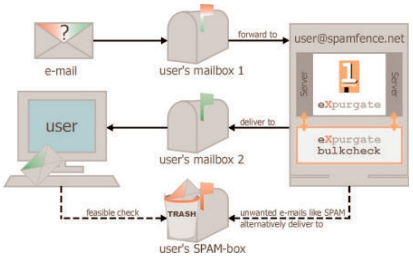


Abb.09 : So funktioniert Expurgate

K9 : Dieses Programm arbeitet ebenfalls mit der Bayes-Methode, um Spam zu erkennen. Ausserdem kann eine sehr flexible Blacklist (inkl. regulärer Ausdrücke) geführt werden. Es ist ebenfalls lernfähig und kann schon zu Beginn auf Spam trainiert werden. Jedoch funktioniert es bislang auch nur bei POP3-Servern. [14]

4.3 andere Lösungen

Hier werden verschiedene Lösungsvorschläge vorgestellt, die zum Teil von den grossen Unternehmen (AOL, Microsoft,...) geplant werden.

SPF : Dieses Projekt wurde vom Gründer des E-Mail-Dienstleisters Pobox initialisiert und bereits von AOL getestet. SPF steht für ‚Sender Permitted Form"und ist vom technischen Aspekt her ein simples Verfahren: Hierzu publiziert jeder legitimierer Mail-Benutzer, der über eine eigene Domain verfügt, über das „Domain Name System"(DNS) die Adresse seines Rechners. So können eingehende Mails vom Mailserver des Empfängers ob die Absenderadresse wirklich von dem Server kommt, mit dem diese Domain im DNS

eingetragen ist. Andernfalls kann SPF nicht genutzt werden. Natürlich können sich auch Spammer in DNS eintragen, würden aber dann durch ein Reputationssystem schnell als ‚böse"Absender erfasst. [15]

Caller ID : Dieses Verfahren, das von Microsoft-Chef Bill Gates vorgeschlagen wurde, funktioniert ähnlich wie SPF: Auch hier wird der Eintrag in DNS um ein weiteres Feld erweitert, in dem z.B. angegeben wird, von welcher IP-Adresse aus Mails mit entsprechender Absenderadresse versandt werden dürfen. [16]

DomainKeys : Dieser Vorschlag wurde von Yahoo eingebracht. Hierbei wird die Mail asymmetrisch verschlüsselt: Jeder Domainbesitzer erstellt einen privaten und einen öffentlichen Schlüssel. Der öffentliche Schlüssel wird in DNS veröffentlicht, den privaten Schlüssel erhalten die Server, die für das Absenden zuständig sind. Mit Hilfe dieses privaten Schlüssels kann der Server des Absenders den Header einer Mail mit einer digitalen Signatur versehen, diese kann der Server des Empfängers dann mit Hilfe des über DNS zugänglichen Schlüssels überprüfen, ob sie auch vom zugehörigen privaten Schlüssel erzeugt wurde. Nur dann wird sie angenommen. Zusätzlich zum Vermeiden von Spam kann so auch das sogenannte „Phishing", also Vortäuschen von offiziellen E-Mails um damit an PIN-Codes o.ä. zu kommen, bekämpft werden. [17], [18]

virtuelle Briefmarke : Die kürzlich von Bill Gates vorgetragene Idee, Spam über eine Art E-Mail-Porto in den Griff zu bekommen, ist nicht neu, so dass es mittlerweile auch verschiedenste Ansätze gibt, wie diese ‚Briefmarke"aussehen könnte. Zum einen die klassische bezahlte Briefmarke, für die allerdings ein Art von Micropayment-System eingeführt werden müsste, was im Moment aufgrund des globalen Einsatzgebietes noch ein zu enormer Aufwand ist (Infrastruktur, Befugnisse, Rechtslage,...).
Eine andere Art wären sogenannte „Arbeitsbeweis"-Briefmarken, bei denen vom Absender kein Geld, sondern Rechenleistung fordert; z.B. indem vor dem Absenden ein einfaches mathematisches Problem gelöst werden muss. Für den privaten Nutzer ist die Rechenzeit kaum spürbar, für einen Massenversender dagegen schon. Ein Beispiel für eine sog. „Proof of Work Stamp"ist das „ Camram"-System, bei dem gewisse Eingangsdaten (Datum , Adresse, Zufallszahl) in eine Hash-Funktion eingesetzt werden, und damit eine iterative Berechnung durchgeführt wird, bis ein als ‚Briefmarke"gekennzeichnetes Ergebnis erreicht wird (z.B. die ersten n Bits sind alle 0). [19]

4.4 rechtliche Schritte

Rechtlich gesehen fällt Spam unter den Begriff „unerwünschte Werbung", deren Versand nach einem BGH-Urteil wettbewerbswidrig ist. Mittlerweile wurde auch das Gesetz gegen den unlauteren Wettbewerb (UWG) dahingehend reformiert, so dass belästigende Werbung, zu der Spam gehört, verboten ist. Ausserdem verletzt das unerlaubte Sammeln von Adressen das Bundesdatenschutzgesetz.
Direkte Klagen gegen Spamer sind allerdings in den meisten Fällen sehr schwer durchzuführen, da dazu der richtige Absender bzw. Verantwortliche zweifelsfrei festgestellt werden muss. Meistens sind diese jedoch nur schwer herauszufinden oder haben ihren Sitz gar nicht in Deutschland. [20]
Eine ähnliche Rechtslage findet sich in Österreich und der Schweiz. In den USA wurde erst kürzlich ein Spammer wegen „Indentitätsdiebstahls"zu sieben Jahren Haft verurteilt, zusätzlich zu einer Schadensersatzzahlung in Höhe von 16,4 Mio. US-Dollar an den Internet-Provider Earthlink. Ob dies wie bei den Klagen gegenüber Raubkopieren die erwünschte abschreckende Wirkung hat, wird sich noch zeigen. [21]

Abbildungsverzeichnis

Quellenverzeichnis

[1]: espace.ch – 10 Jahre lang Werbemüll (http://www.espace.ch/boulevard/artikel/42921/artikel.html)
[2]: Wikipedia – Die freie Enzyklopädie (http://de.wikipedia.org/wiki/Spam)
[3]: Brightmail (http://www.brightmail.com)
[4]: Daniel Rehbein – Über Spam und die Sammler von Mailadressen (http://www.rehbein-dortmund.de/spamtrap.html)
[5]: Informationen zum Thema Spam (http://spam.trash.net/)
[6]: Yahoo-Mail (http://www.yahoo.de)
[7]: Alles über Spam (http://www.hierkriegstdualles.de/spam.htm)
[8]: Daniel Rehbein – Domainnamen für Beispiele – RFC 2606 (http://www.daniel-rehbein.de/rfc2606.html)
[9]: GMX – Stop Spam! (http://www.gmx.de/)
[10]: Spamassassin (http://www.spamassassin.org/tests.html)
[11]: Deutsche Hilfeseite für SpamPal für Windows (http://www.spampal.spxs.net)
[12]: Spamihilator (http://www.spamihilator.com)
[13]: eleven's Expurgate spam-filter (http://www.eleven.de/products/expurgate/)
[14]: Robin Keir's Homepage – Software – k9 (http://www.keir.net/k9.html)
[15]: Technology Review – Neue Anti-Spam-Technik auf dem Vormarsch (http://www.heise.de/tr/aktuell/meldung/44259)
[16]: Heise Online-News vom 24.05.2004 (http://www.heise.de/newsticker/meldung/47589)
[17]: Heise Online-News vom 19.05.2004 (http://www.heise.de/newsticker/meldung/47508)
[18]: Yahoo! Anti-Spam Ressource Center (http://antispam.yahoo.com/domainkeys)
[19]: Technology Review (http://www.heise.de/tr/aktuell/meldung/46152)
[20]: Rechtsanwalt Dr.Stephan Ackermann, Rostock: Spam/Spamming (http://www.dr-ackermann.de/spam/)
[21]: Heise Online-News vom 28.05.2004 (http://www.heise.de/newsticker/meldung/47764)

Stand: 29. 06. 2004